Law Commission
Reforming the law

Search warrants

HC 852

Law Com No 396

Law Commission
Reforming the law

Law Com No 396

Search warrants

Presented to Parliament pursuant to section 3(2) of the Law Commissions Act 1965.

Ordered by the House of Commons to be printed on 7 October 2020.

HC 852

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at search_warrants@lawcommission.gov.uk .

ISBN 978-1-5286-2169-4

CCS0920279116 10/20

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the APS Group on behalf of the Controller of Her Majesty's Stationery Office

The Law Commission

The Law Commission was set up by the Law Commissions Act 1965 for the purpose of promoting the reform of the law.

The Law Commissioners are:

The Right Honourable Lord Justice Green, Chairman

Professor Sarah Green

Professor Nick Hopkins

Professor Penney Lewis

Nicholas Paines QC

The Chief Executive of the Law Commission is Phil Golding.

The Law Commission is located at 1st Floor, Tower, 52 Queen Anne's Gate, London SW1H 9AG.

The terms of this Report were agreed on 29 July 2020.

The text of this Report is available on the Law Commission's website at http://www.lawcom.gov.uk.

Contents

Glossary

Access conditions

The statutory conditions that must be met for the issue of a search warrant. Depending on the search warrant provision, these may include that there are reasonable grounds for believing that an offence has been committed and that there is relevant material on the premises. The term is used in this sense in schedule 1 to the Police and Criminal Evidence Act 1984 ("PACE").

Accessibility conditions

The term we use to describe a particular subset of access conditions that relate to the impracticability of gaining access to the premises or materials without a search warrant.

All premises warrant

A search warrant that allows for the entry and search of all premises associated with a particular person.

Associated powers

The term we use to refer to powers other than search powers that are authorised under a search warrant. For example, a search warrant may have an associated power to use reasonable force, to search persons found on the premises and to seize material.

Applicant

The term we use occasionally to refer to an individual officer or investigator who applies for a search warrant.

Code B of PACE

The PACE Code of Practice which governs the search of premises by police officers and the seizure of property found by police officers on persons or premises.

Criminal Practice Directions

The Criminal Practice Directions ("CrimPD") are made by the Lord Chief Justice and relate to the practice and procedure of the criminal courts. CrimPD Division XI (47A and 47B) relates to search warrants.

Criminal Procedure Rules

The Criminal Procedure Rules ("CrimPR") govern the way criminal cases are managed and set out the processes of the criminal courts. Part 47 of the CrimPR governs search warrant applications. There are search warrant application forms which accompany Part 47 of the CrimPR.

Duty of candour

This describes the duty owed by any person making an application for a search warrant to provide full and frank disclosure to the court of all relevant information including that which might militate against the granting of the search warrant.

Electronic data

The term we use to refer to data stored in electronic form.

Electronic device

The term we use to refer to all devices that control and direct electric currents.

Electronic material

The term we use to refer to both devices themselves ("electronic devices") and data stored in electronic form ("electronic data").

Entry warrant

A warrant issued by a judge that authorises entry onto premises.

Ex parte

A hearing in which an interested party is absent and, in the context of search warrant hearings, unnotified. In the search warrants context, the occupier of the premises will be absent and unnotified when an investigator makes an application for a search warrant, as the presence of the occupier would frustrate the purpose of the search warrant.

Excluded material

Material that is partially exempt from searches under a search warrant. Excluded material is defined in section 11 of PACE. It broadly covers material in the following categories, which is held in confidence: medical records acquired or created in the course of an occupation; human tissue; and confidential journalistic material. It can be searched for under the second set of access conditions under schedule 1 to PACE.

Imaging

Imaging an electronic device involves capturing and storing a copy of the data on a device for later inspection away from the premises.

Independent lawyer

The term we use to refer to a lawyer who is not connected to the case, whose role is to advise the investigator on what may and may not be seized. This person is referred to in practice as "independent counsel".

Iniquitous material

The term we use to refer to protected material that has lost its protected status, or is to be regarded as never having been afforded confidential status, because it is tainted by "iniquity". Under the iniquity or "crime-fraud" exception, the protection afforded to special categories of material is lost when, broadly speaking, it is created, acquired or held for an iniquitous purpose.

Information

The technical name for the document sworn in support of the application for a search warrant. The CrimPR provide application forms that constitute the information.

Inspection warrant

A warrant issued by a judge that authorises entry onto, and the inspection of, premises.

Inter partes

A hearing in which all interested parties are present.

Issuing authority

The term we use to describe the person or court empowered to grant the search warrant application and issue a search warrant.

Legally privileged material

Legally privileged material is defined in section 10 of PACE and broadly covers communications made in connection with the giving of legal advice or in contemplation, and for the purpose, of legal proceedings between: a professional legal adviser and their client; and a professional legal adviser and any third party representing their client. It is absolutely exempt from searches under a search warrant.

Metadata

A set of data that describes and gives information about other data. An example is communications data, which is data on the who, where, when and how of a communication but not its content. Communications data is defined in section 261(5) of the Investigatory Powers Act 2016.

Multiple entry warrant

A search warrant that allows for the entry of premises on more than one occasion, either up to a stated maximum number of times or an unlimited number.

Occupier

The term we occasionally use for a person in possession or control of the premises to be searched under a search warrant. We also use the terms “suspect” and “person affected by the warrant” depending on the nature of the discussion.

Off-site

The term we use to refer to activity, such as the sifting of material, that takes place once an investigator has left premises following the execution of a search warrant.

On-site

The term we use to refer to activity, such as the imaging of devices, that takes place while an investigator is on premises following the execution of a search warrant.

Premises

The place to be entered and searched under a warrant. Premises is defined in section 23 of PACE. Other statutes may provide their own definitions of premises.

Production order

A court order compelling a party to produce a particular category of material as specified under the order.

Protected material

The term we use to refer to material which is legally privileged, excluded material or special procedure material, and other categories of material that cannot be searched for or seized when searching premises. In our consultation paper we used the term “exempted material” to refer to these categories of material. All three of these categories have varying degrees of restriction in relation to search and seizure.

Public interest immunity

A determination made by an issuing authority that the public interest demands that some of the material relied upon to satisfy the issuing authority to issue a search warrant should not be disclosed.

Remotely stored electronic data

The term we use, along with “remotely stored data”, to refer to electronic data which is physically stored on a different electronic device from the device which is accessing the electronic data. Remotely stored data can be accessed by connecting to an online account or remote storage account.

Search warrant

A warrant issued by a judge that authorises entry onto, and the search of, premises.

Seize and sift

Powers of seizure under Part 2 of the Criminal Justice and Police Act 2001, which provides the power to seize indeterminable or inseparable material and to sift off the premises that which an investigator was entitled to seize from that which they were not.

Sensitive material

Any information relied on in support of an application for a warrant which the applicant regards would be damaging to the public interest were it to be disclosed. An investigator may later assert public interest immunity over the sensitive material on the grounds that there would be a real risk of serious prejudice to an important public interest were it to be disclosed.

Special procedure material

Material that is partially exempt from searches under a search warrant. It can be searched for under the first set of access conditions under schedule 1 to PACE. Special procedure material is defined in section 14 of PACE. It broadly covers material other than excluded material, which was acquired or created in the course of an occupation and which is held in confidence, and also non-confidential journalistic material.

Specific premises warrant

A search warrant that allows for the entry and search only of premises specified in the warrant; these may be either one or more sets of premises.

Search Warrants

To the Right Honourable Robert Buckland QC MP, Lord Chancellor and Secretary of State for Justice

Chapter 1: Introduction

BACKGROUND TO THE PROJECT

1.1 A search warrant is a document issued by a magistrate or judge ("the issuing authority") to a police officer or other investigator, granting legal authority to enter premises and search for specified items. There are approximately 176 different search warrant provisions across 138 different pieces of legislation. Most search warrants are obtained in order to search premises for evidence of a criminal offence.[1] Around 40,000 search warrants are issued in England and Wales every year.[2]

1.2 The importance of the law and procedure governing search warrants operating efficiently and fairly is clear. Search warrants are a vital tool for the effective investigation of all forms of crime – including murder, terrorism, fraud, rape and child sexual abuse – and the protection of the public from harm. At the same time, search warrants are one of the most intrusive powers of the state, the execution of which not only amounts to an interference with an individual's privacy rights, but may significantly adversely impact on an individual's life and lead to the collection of large volumes of personal material.

1.3 The consequences of search warrants law and procedure failing to operate properly can be severe. Where there are deficiencies in the law, law enforcement agencies will not have the means to obtain evidence and effectively investigate, detect, prevent and prosecute serious criminality. This creates a heightened risk of harm to members of the public. Where there are procedural errors, the search warrant and any entry, search and seizure may be declared unlawful. In recent years, dozens of search warrants have been declared unlawful by the courts. Inappropriately obtained search warrants can lead to entire criminal investigations collapsing and millions of pounds incurred by public bodies on legal fees and damages. This can also erode public trust and confidence in law enforcement agencies. Significant reputational damage and stress may also be caused to innocent individuals who are the subject of a search. The impact on a person's social life, academic studies or the running of their business can also be particularly acute where electronic devices are seized and retained.

THE PURPOSE OF THE PROJECT

1.4 We undertook this project at the request of the Home Office, starting work in January 2017. This request followed from comments made by senior members of the judiciary suggesting that the law governing search warrants was in need of reform, due to its complexity and following a series of high-profile cases in which search warrants were declared unlawful.

---

1 For an overview of the law of search warrants, see Search Warrants (2018) Law Commission Consultation Paper No 235, ch 2.

2 Data collated and provided to us by HMCTS.

1.5 The purpose of this project is therefore to recommend ways in which the law of search warrants can be simplified, rationalised, modernised and made fairer. Our recommendations would equip law enforcement agencies with the means to investigate crime effectively while ensuring that enforcement powers are exercised appropriately, in a proportionate manner and subject to proper safeguards.

1.6 This is the most extensive independent review of the law governing search warrants ever carried out in this jurisdiction. In this project we review the law and practice governing search warrants. We examine the law and procedure when applying for, issuing, and challenging a search warrant, and carrying out a search under warrant. We also examine the law governing the treatment of sensitive material, electronic material and categories of material that are exempt from being the subject of a warrant. Finally, we consider the extent to which the wider landscape of search warrant provisions should be consolidated.

1.7 This report sets out our 64 recommendations for reform.[3] A full list of our recommendations can be found in Chapter 20 of this report. A full list of those who submitted a consultation response can be found at appendix 1. Extracts from the most frequently cited statutory provisions in this report can be found at appendix 2.

THE SCOPE OF THE PROJECT

1.8 The complete terms of reference for the project, as agreed in a memorandum of understanding between the Law Commission and the Home Office signed on 11 January 2017, are as follows:

> The law reform objectives of the review encompass elements of rationalisation and streamlining of the current law, as well as identifying and addressing pressing problems.
>
> The focus of this review is on making search warrants legislation more transparent and accessible, thus reducing the scope for errors, which in turn can lead to substantive injustice and wasted costs.
>
> The review will include consideration of reform by legislative change, as well as non-statutory guidance, Criminal Procedure Rules and other initiatives.

1.9 In the course of working on the project it became clear that the application of search warrant powers to electronic material was an area of considerable uncertainty and one which causes significant difficulties in practice. We therefore extended the project timeline and terms of reference to include the following paragraph:

> The review will include consideration of how the existing search warrants legislation deals with electronic material. For the avoidance of doubt, any revisions to the Investigatory Powers Act 2016, and the Regulation of Investigatory Powers Act 2000 are outside scope. Furthermore, questions relating to encryption are beyond the scope of this review.

1.10 The law and procedure governing search warrants is vast and complex. We identified 176 distinct search warrant provision on the statute book in our consultation paper.[4] This list does not include warrants to enter premises ("entry warrants") and warrants to enter and

---

3 The report is available online at https://www.lawcom.gov.uk/project/search-warrants/.

4 See Search Warrants (2018) Law Commission Consultation Paper No 235, appendix 1.

inspect premises ("inspection warrants"). Statutory provisions that are exercised in conjunction with a warrant and govern the treatment of seized material are also contained in the Police and Criminal Evidence Act 1984 ("PACE") and Part 2 of the Criminal Justice and Police Act 2001 ("CJPA").

1.11 Beyond the primary legislation, there are supplementary provisions in Code B of PACE, the Criminal Procedure Rules 2020 ("CrimPR") and the Criminal Practice Directions ("CrimPD"). There are a number of other guidance documents and codes of practice pertaining to criminal investigations that may involve the execution of a search warrant.

1.12 This project only concerns search warrant provisions relating to a criminal investigation. It does not concern powers of stop and search or police powers more generally; however, we discuss these powers to the extent that they inevitably overlap with search warrants law and procedure.

THE HISTORY OF THE PROJECT

1.13 This report represents the conclusion of our search warrants project. As noted above, work began on the project in January 2017. We met with a diverse range of stakeholders to gather evidence of the problems with the current law and set about producing provisional proposals in a consultation paper. In preparing the consultation paper, we conducted an extensive literature review and discussed the law with academics, lawyers, judges, court organisations, law enforcement agencies, Government departments and special interest groups. This iterative discussion process was invaluable in helping us to understand how the current law operates, its deficiencies and potential avenues for reform.

1.14 Our consultation paper was published on 5 June 2018, which marked the beginning of a three-month open public consultation period, ending on 5 September 2018. During the consultation period, we invited responses to the 64 consultation questions contained in our consultation paper. We received 47 consultation responses in total.[5]

1.15 To encourage discussion and foster ideas for reform, we held an operational roundtable event on 23 July 2018 and a practitioners' roundtable event on 24 July 2018.[6] We also held a roundtable at the Royal Courts of Justice on 21 November 2018 with senior Circuit judges,[7] High Court judges and judges of the Court of Appeal.[8] In addition, we gave a number of presentations on the project to human rights organisations, special interest groups and members of the legal and medical professions.

1.16 With the kind assistance of several stakeholders, we undertook several activities to assist in understanding the practical side of search warrants. We spent time with Staffordshire Police, who gave us operational insight into applying for and executing search warrants. This included accompanying constables during the execution of a search warrant.[9] We attended the offices of Privacy International, who demonstrated to us first-hand the capability of

---

5 We list those individuals and organisations who submitted a consultation response at appendix 1 to this report.

6 We are grateful to Northumbria Law School for organising a regional public roundtable, which informed their consultation response.

7 A senior Circuit judge (resident judge) carries out leadership and management duties in running the court centre at which they are based.

8 We refer to this in our report as a roundtable with the senior judiciary.

9 We would like to thank DC Anthony David in particular for all of his assistance.

mobile phone extraction tools and the quantity of data that they can extract. We also attended a number of court hearings that concerned the treatment of material seized following the execution of a search warrant.

1.17 An analysis of consultation responses followed our consultation exercise which, along with the other events discussed above, has shaped the formulation of our policy and informed the 64 recommendations contained in this report.

THE PROBLEMS WITH THE CURRENT LAW

1.18 This section provides an overview of the problems with the current law and procedure that govern search warrants. There are three principal ways in which these problems manifest themselves. First, errors are often made. Operation Midland is a high-profile case in point, in which six search warrants were obtained following false allegations made relating to historic child sexual abuse. A report by Sir Richard Henriques into Operation Midland found serious errors in the search warrant applications.[10] The consequences of errors such as these – which include millions of pounds incurred by public bodies, the erosion of public trust and confidence in law enforcement agencies and significant reputational damage to innocent individuals – have already been set out at paragraph 1.3 above.

1.19 Secondly, the problems that we have identified lead to procedural inefficiency and unfairness. In some cases, it can take police forces three weeks to obtain a search warrant due to a lack of available hearing slots. The longer it takes to obtain and execute a search warrant, the higher the risk of evidence being lost and the longer the period of potential offending and therefore harm being caused to members of the public. When a search warrant has been executed, and material seized, logistical challenges may arise when material is subsequently examined. This can lead to excessive cost and delay, thereby impeding law enforcement agencies from investigating crime effectively. The significant backlog of electronic devices awaiting examination – in some cases up to a year – also means that individuals whose electronic devices are seized may be left without material that is integral to their social lives, academic studies or the running of their business.

1.20 Thirdly, law enforcement agencies lack the powers to investigate, detect, prevent and prosecute crime effectively. Nowhere is this issue more acute than in the area of electronic material. By way of example, relevant evidence may be stored remotely in a cloud account protected by two-factor authentication. The law has failed to keep pace with the modern digital landscape and the ways in which criminality now occurs. As a result, law enforcement agencies may fail to obtain electronic evidence which is vital for the successful investigation and prosecution of serious criminal offences.

Complexity

1.21 The complexity of provisions regulating search warrants leads to a confusing legislative landscape. Search warrants legislation has repeatedly been acknowledged to be an

[10] Sir Richard Henriques, *Independent Review of the Metropolitan Police Service's handling of non-recent sexual offence investigations alleged against persons of public prominence* (4 October 2019) para 2.4.64. Available at https://www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/henriques-report/.

"unfortunate jumble of legislative provisions",[11] with a former Lord Chief Justice also commenting that associated legislation "could have been more felicitously drafted".[12]

1.22 Accordingly, there is a heightened risk that errors will occur when applying for and executing a search warrant, which may lead to inordinate cost, delay and investigations collapsing. Investigators also often spend time and money deciphering the law to ascertain precisely what conduct is legally permissible.

1.23 For individuals, the complexity of the law means that it is difficult to understand the extent of the state's powers, the safeguards that protect them, and what means of redress they have. The combined effect of these problems is that the law is in a highly unsatisfactory state.

Inconsistency

1.24 There are numerous statutes providing search warrant powers. There are differences across these statutes as to who may apply for a search warrant and carry out a search, and the powers that are available. Some of these inconsistencies cause gaps in investigative capabilities. Certain law enforcement agencies may therefore be left with insufficient powers to effectively investigate crime. These inconsistencies also mean that the safeguards and protections that apply vary considerably based on how powers are exercised. As a consequence, some individuals have fewer statutory protections than they might otherwise have.

1.25 There are also regional inconsistencies in the procedure for obtaining a search warrant, with a potential under-utilisation of technology, leading to procedural inefficiency. This means that, for example, depending on where an application is made, there will be differences in the time it takes to hear an application and the way in which the application is heard.

1.26 Inconsistency can also be found in the quality of search warrant applications, some of which have serious errors. A review undertaken by the National Crime Agency in 2016 into 268 separate operations in which search warrants were obtained revealed potentially significant deficiencies in 22 operations and minor deficiencies in an additional 189 operations.[13] This means that 78.73% of investigations had defective warrants, 8.2% of which had potentially significant deficiencies in the warrants obtained. Part of the reason for errors stems from inconsistencies in the level of training undertaken by those who apply for a warrant. As we have highlighted, errors may lead to lead to criminal investigations collapsing, large sums of money being incurred by public bodies and significant reputational damage and stress to innocent individuals who are the subject of a search.

1.27 Law enforcement agencies have differing views on what is legally permissible, primarily because it is unclear how the law of search warrants applies to electronic material. As a consequence, some law enforcement agencies may be performing coercive acts which are a serious infringement of an individual's liberty without lawful basis. Other law enforcement agencies adopt a cautious approach, which may potentially lead to investigators not

---

11 *Gittins v Central Criminal Court* [2011] EWHC 131 (Admin), [2011] Lloyd's Rep FC 219 at [36(1)] per Gross LJ; *R (A) v Central Criminal Court and another* [2017] EWHC 70 (Admin) at [38], [2017] 1 WLR 3567 at [11]; and *Business Energy Solutions Ltd v The Crown Court at Preston* [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [15].

12 *R (Panesar) v Central Criminal Court* [2014] EWHC 2821 (Admin), [2015] 1 WLR 2577 at [44].

13 National Crime Agency, *Warrant Review Closing Report* (31 March 2016) p 15.

obtaining the evidence needed for the successful prosecution of serious criminal offences. In both cases criminal investigations are being jeopardised.

Outdated

1.28 We live in an age where terabytes of material can be stored electronically, in some cases on remote servers in an unknowable jurisdiction. A large proportion of the provisions governing search warrants, in particular those contained in PACE, predate the advent of electronic material and modern computing methods. This means that the current law fails to appreciate the unique features of electronic material and digital investigations. As a consequence, search warrants legislation is therefore failing to deal with emerging digital technology and the ways in which criminal activity now takes place.

1.29 Dramatic technological change has also created legal uncertainty in respect of search warrant regimes. As a result, the current law both inhibits criminal investigations and has significant privacy implications for those whose electronic devices are searched and seized.

Costly

1.30 There are several aspects of the law and procedure governing search warrants that lead to unnecessary cost. The procedure when applying for and issuing a search warrant also does not always operate efficiently. This can lead to wasted time and money, and significant delays in obtaining a search warrant.

1.31 The complexity of the law causes additional expense due to the time spent resolving disputes and ascertaining the scope of powers. Inconsistencies in the powers available to law enforcement agencies also result in excessive cost and delay. For example, certain agencies must enlist the help of the police to obtain and execute warrants. Certain law enforcement agencies also lack powers exercisable by others that would otherwise provide for a more efficient means of executing a search warrant, thereby generating additional cost.

1.32 The failure of the current law to keep pace with modern computing methods and the digital landscape also causes unnecessary expense as law enforcement agencies must examine electronic devices within a legal framework that is not fit for purpose.

THE AIMS OF OUR PROJECT

1.33 Search warrants are vital to criminal investigations; they also raise important constitutional issues concerning the rule of law and the proper balance between the powers of the state and the rights and freedoms of individuals. The tension between these competing public interests was described by Lord Justice Bingham, as he then was, as follows:

> There is an obvious tension between these two public interests because crime could be most effectively investigated and prosecuted if the personal and property rights of citizens could be freely overridden and total protection of the personal and property rights of citizens would make investigation and prosecution of many crimes impossible or virtually so.[14]

1.34 The overarching aim of the recommendations in this report has therefore been to strike a fair and appropriate balance between these competing public interests. The specific aims of our

[14] *R v Lewes Crown Court ex parte Hill* (1991) 93 Cr App R 60, 66.

recommendations are set out below. In turn, these aims should reduce the risk of errors, render search warrants procedure fairer and more efficient and equip law enforcement agencies with the powers to investigate serious crime effectively.

Simplify the law

1.35 Our recommendations aim to simplify the law by rendering it more rational and comprehensible. Law enforcement agencies would therefore better understand what powers they have and the conditions to which they are subject. This would make the law more efficient and reduce the scope for errors, thereby reducing the risk of search warrants being declared unlawful and investigations collapsing.

1.36 Our recommendations would also make it easier for individuals to understand the extent of the state's powers, the safeguards that protect them, and what means of redress they have.

Make the law fairer

1.37 Our recommendations would make the law fairer by extending protections and making their application more consistent, making it easier for individuals to obtain redress where their property is seized, making the law and the actions taken by law enforcement agencies more transparent, and making law enforcement agencies more accountable for their actions.

1.38 Our recommendations seek to ensure that human rights are protected and that a search under a warrant is necessary and proportionate to the outcome sought. In particular, our recommendations would better protect the property and privacy rights of those whose property is seized.

Modernise the law

1.39 Our recommendations aim to support the wider public interest in providing law enforcement agencies with the tools to protect the public by detecting and prosecuting crime. In particular, our recommendations aim to modernise procedures, by ensuring that technology is best utilised, and modernise the law, by ensuring that it reflects the changing nature of investigations and is equipped to deal with digital investigations.

1.40 Our recommendations would therefore ensure that investigative agencies can respond quickly to crime and tackle criminal conduct as it is carried out in a digital world, whilst maintaining robust and effective safeguards that account for the nature of electronic material.

Make the law more cost-efficient

1.41 Our recommendations aim to make the law more cost-efficient by rationalising the powers available to law enforcement agencies, introducing more streamlined methods to obtain a search warrant which utilises technology, reducing the risk of errors occurring and providing swift and effective means to resolve disputes.

1.42 In redesigning the search warrants regime, we have been alive to the fact that unrealistic or disproportionate demands must not be imposed on law enforcement agencies. The law should also facilitate and permit law enforcement agencies to carry out criminal investigations expeditiously.

SUMMARY OF THE REPORT CHAPTERS AND OUR RECOMMENDATIONS

1.43 This section describes the content of each chapter of this report and explains the recommendations that we make. As indicated, we make 64 recommendations in this report. Some of our recommendations would require implementation through primary legislation. Other recommendations would require amending Code B of PACE, the CrimPR or the CrimPD. We direct our recommendations which concern Code B of PACE to the Home Office PACE Strategy Board, which is an advisory body to the Home Secretary who has the power to amend the PACE Codes of Practice.[15] Our recommendations regarding the CrimPR, the CrimPD and accompanying application forms are directed to the Criminal Procedure Rule Committee ("CPRC"), an advisory non-departmental public body, sponsored by the Ministry of Justice. Some recommendations would require implementation by means other than those discussed above.

Chapter 2: The operation of the statutory safeguards

1.44 In Chapter 2 of this report, we examine the safeguards that must be followed when applying for and executing a search warrant.

1.45 We start by considering when the statutory safeguards under sections 15 and 16 of PACE should apply to search warrants. We observe that the safeguards may not afford adequate protection because they only apply when a search warrant is issued to a constable. Further, the safeguards may not have been adequately extended to other agencies.

1.46 We do not consider it appropriate to extend sections 15 and 16 of PACE to all search warrant regimes for the reasons set out at paragraph 2.48 below. We conclude, however, that, as a matter of policy, the safeguards should apply to all search warrants relating to a criminal investigation. That being said, we do not consider it practical to have an all-encompassing test which seeks to apply the safeguards to all search warrants that relate to a criminal investigation. This is because such an extension may have unintended consequences. It is therefore desirable to consider and craft the most appropriate safeguards for each search warrants regime.

1.47 Turning to consider individual search warrant regimes, we recommend that statutory safeguards, modelled on sections 15 and 16 of PACE, are inserted into the Criminal Justice Act 1987 ("CJA"), which enables a member of the Serious Fraud Office ("SFO") to apply for a search warrant. This is because it is unclear at present whether sections 15 and 16 of PACE apply to the regime. Making it clear that safeguards apply would provide clarity and enforceable standards of conduct.

1.48 We turn to consider whether sections 15 and 16 of PACE should be extended to warrants relating to a criminal investigation that permit entry or inspection only, rather than search. We observe that such warrants will often still enable an investigator to search premises, and therefore safeguards should apply. However, once again we conclude that an extension or modification of the statutory safeguards should be considered on a case-by-case basis. For the reasons set out at paragraph 2.72 below, there are no specific regimes in which we are able to conclude that the safeguards are inadequate, and so we do not make a recommendation for reform.

1.49 Next, we consider when regard should be had to Code B of PACE by non-police investigators. Code B of PACE is a Code of Practice which governs the exercise of police

[15] Police and Criminal Evidence Act 1984, s 67(2).

powers to search premises; it restates many of the safeguards found in sections 15 and 16 of PACE and supplements them with further guidance. Persons other than police officers must have regard to any relevant provision of Code B of PACE.

1.50 We observe that it is unclear to what extent regard to Code B of PACE should be had by non-police investigators. We conclude that the burgeoning number of law enforcement agencies that can now apply for and execute warrants for the purpose of a criminal investigation justifies Code B of PACE providing more detail than it currently does. Accordingly, we recommend that the PACE Strategy Board consider amending Code B of PACE to provide guidance for non-police investigators in complying with the provisions of the Code.

1.51 The remainder of the chapter discusses section 15(1) of PACE, which provides that an entry on or search of premises under a warrant is unlawful unless "it" complies with sections 15 and 16 of PACE. We examine first the activities to which the "it" in section 15(1) of PACE refers. We conclude that "it" refers to the warrant, entry and search and recommend that section 15(1) of PACE is amended to make this clear.

1.52 We then discuss the elements of the search rendered unlawful following a breach of sections 15 and 16 of PACE. We observe that the Divisional Court has on a number of occasions expressed the view that non-compliance with section 15(1) of PACE also renders seizure unlawful, in addition to entry and search. We again recommend that section 15(1) of PACE is amended to make this clear.

1.53 Finally, we discuss whether breaches of all the provisions in sections 15 and 16 of PACE should render entry, search and seizure unlawful, and what the consequence of a finding of unlawfulness should be. There is no consistent approach regarding the circumstances in which a failure to comply with sections 15 and 16 of PACE will lead to a breach of section 15(1) of PACE. However, we conclude that this is an area of law in which a wide margin of judicial discretion should be afforded to both the question of when a breach will result in a finding of unlawfulness and the relief granted in respect of a breach.

Chapter 3: Agencies empowered to apply for and execute search warrants

1.54 In Chapter 3 of this report, we consider whether some agencies which are not at present entitled independently to apply for and execute search warrants should be given the power to do so.

1.55 We begin by discussing the agencies entitled to apply for a search warrant. We explain that a large number of law enforcement agencies are empowered to apply for a search warrant. However, NHS Counter Fraud Authority ("NHSCFA") and NHS Counter Fraud Service Wales ("NHSCFSW") do not have the power to apply for a search warrant, and the Insolvency Service only has the power to apply for a warrant in respect of confidential categories of material.

1.56 In respect of the NHSCFA and NHSCFSW, we conclude that other avenues to obtain medical records, namely seeking police assistance to arrest individuals or apply for search warrants itself, are unsatisfactory. We conclude that it would be desirable for the NHSCFA and NHSCFSW to be empowered to apply for a search warrant where there has been non-compliance with, or it is impracticable to issue, a production notice under the NHS Act 2006 and make a recommendation accordingly. In respect of the Insolvency Service, we conclude that it would be desirable to empower the agency to apply for a search warrant itself in

respect of ordinary material that is not confidential and, again, make a recommendation accordingly.

1.57 We turn next to discuss which agencies are entitled to execute a search warrant. We observe that some search warrant provisions empower the agency applying for a warrant to execute the warrant, whereas other provisions permit an agency to accompany a constable who executes the warrant. We conclude that these differences are justified based on the particular agency concerned. We recommend that a search warrant applied for by the NHSCFA or NHSCFSW permit either that agency or a constable to execute the warrant, and that neither agency be required to exercise powers of search and seizure in the presence of a constable. We also recommend that the Insolvency Service be empowered to execute search warrants without the presence of a constable, and that sections 19 to 22 of PACE, which provide powers of seizure and retention, be extended to the Insolvency Service, with necessary modifications.

1.58 We end the chapter by discussing the requirement under certain search warrant regimes that investigators can only exercise their powers of search and seizure in the presence of a constable. We conclude that there are several reasons why it would be desirable for members of the SFO and Financial Conduct Authority ("FCA"), under their respective regimes, to be permitted to remain on premises and exercise powers without a constable's ongoing presence once lawful entry has been effected, and make a recommendation accordingly. To ensure the appropriate powers and safeguards apply, we also recommend the application and modification of section 16 of PACE and the creation of a new offence of obstructing a person who is carrying out functions under a search warrant.

Chapter 4: Search warrant application documents

1.59 In Chapter 4 of this report, we consider reform to the documents used to apply for a search warrant.

1.60 We begin by discussing the need for bespoke warrant applications. We explain that there are specially designed application forms for a small number of the most commonly sought search warrant provisions, and a generic form for the majority of others. We conclude that, while it would be disproportionate to create application forms for every search warrant provision, there would be real benefit in the creation of *entry* warrant application forms. We therefore recommend the creation of a specific entry warrant application form for applications under the Consumer Rights Act 2015, and a generic entry warrant application form that can be modified.

1.61 We turn next to consider the content of warrant application forms. We note that the failure to observe the duty of candour is one of the most frequent challenges to search warrants. Given that there are countless matters that may be relevant to discharging the duty of candour, we recommend that the CPRC consider amending search warrant application forms to include within the guidance notes an extensive (but non-exhaustive) list of factors which could be relevant to discharging the duty, along with specific questions as appropriate. We then discuss a number of other amendments to the application forms that may be desirable.

1.62 We then discuss the need for draft warrant templates. While a standard search warrant template exists, we note that there is no standard entry warrant template. To obviate the need to modify search warrant templates, we recommend the creation of a standard entry warrant template.

1.63 We end the chapter by discussing the desirability of an online application portal. At present, search warrant application forms are typically downloaded, completed on a computer, and then emailed to the relevant court centre. We conclude that an online search warrants application portal would bring a host of benefits, and therefore recommend that Her Majesty's Courts and Tribunals Service ("HMCTS") consider the practicability of designing and implementing an interactive online search warrants application portal.

Chapter 5: Applying for a search warrant

1.64 In Chapter 5 of this report, we consider reform to the wider framework governing the application process.

1.65 We begin by discussing the scope of the duty of candour outside of application forms. We conclude that steps ought to be taken to make the common law duty of candour more accessible and comprehensible, given that failure to discharge the duty remains one of the most frequent grounds of challenge to a search warrant. Given the importance of the duty, we recommend that the duty of candour be codified in section 15 of PACE. We also recommend that the duty of candour is set out in greater detail in the Criminal Practice Directions and Code B of PACE.

1.66 We then discuss the process of arranging a search warrant application hearing. We explain that there is no standard procedure for arranging a search warrant application hearing and proceed to discuss the different methods. Comments from consultees lead us to make two recommendations. First, we recommend that all law enforcement agencies take steps to ensure that sufficient training is provided to officers involved in applying for and executing search warrants to ensure that applications are consistently completed to a high standard. Secondly, we recommend that HMCTS consider the practicability of making more search warrant application hearing slots available, or pursuing other measures which would decrease both the length of time it takes to obtain a search warrant and the disruption to other court business.

1.67 We turn next to discuss the level of knowledge required of an applicant when appearing at a search warrant hearing. Consultees' responses revealed that there is a tendency for junior officers with very limited knowledge of the investigation to be tasked with seeking search warrants, causing wasted time and expense. We therefore recommend that Code B of PACE be amended to include the requirement that a person applying for a search warrant has adequate knowledge to answer questions asked by the issuing authority.

1.68 We end the chapter by discussing the interaction between search warrants and the powers to search premises following arrest. The issue with which we are concerned is whether the police, or other officers who have powers of arrest, should be allowed to arrest an individual solely to activate the power to search premises in preference to securing a search warrant. We conclude that any amendments to powers of arrest would have a wide-ranging impact on police powers and that further evidence would be necessary before reform was made.

Chapter 6: Issuing a search warrant

1.69 In Chapter 6 of this report, we consider reform to the procedure for issuing a search warrant.

1.70 We begin by considering the circumstances in which a search warrant application ought to be heard by a judge as opposed to a magistrate. We make clear that properly advised magistrates are clearly capable of dealing with search warrant applications, and so restricting the ability to issue a warrant to judges would be inappropriate. We conclude that

there is no appetite for a more formal set of rules concerning the allocation of complex search warrant applications.

1.71 We then consider whether magistrates should have specialist training to hear search warrant applications. Given the clear support from consultees, we recommend that only those magistrates who have undergone specialist training should have the power to issue a search warrant. However, we do not seek to prescribe the exact form any such training should take, as this would be a matter for other organisations to consider.

1.72 Next, we consider whether the practice of magistrates being advised by a legal adviser should be formalised. At present there is no legal requirement that a magistrate deciding a warrant application should be advised by a legal adviser (a justices' clerk). Every consultee agreed that a magistrate should be advised by a legal adviser. We conclude that the requirement should be formalised, and recommend that it be so in the CrimPR.

1.73 We consider next whether more than one magistrate ought to be required to hear a search warrant application. We agree with the overwhelming majority of consultees that this would not be desirable.

1.74 We then consider the procedure governing out of hours search warrant applications. Applications for search warrants can be made to a magistrate out of hours at the magistrate's home address. We agree with the weight of consultees that a rota system of legally qualified judges is both unnecessary and impractical. We do, however, see merit in formalising a nationwide procedure where applications are submitted and heard remotely. We therefore recommend that HMCTS review the current magistrates' courts' out of hours search warrant application procedures across all regions to ensure, amongst other things, that proper use is being made of technology.

1.75 We then turn to consider formalising the application procedure in court hours. There are varying practices across different regions. We conclude that, to the maximum extent possible, there should be regional consistency in relation to the procedure for applying for search warrants. We also consider that there ought to be a greater utilisation of technology as a means for making and hearing applications. We therefore recommend that an application system for court hours applications be formalised nationwide to provide for these matters, along with the screening of applications by a legal adviser where practicable to do so.

1.76 We then consider the filtering of search warrant applications made to the Crown Court by a legal adviser. For a number of reasons, we conclude that search warrant applications made to the Crown Court should not be screened by a magistrates' court legal adviser.

1.77 Next, we consider the recording of additional material provided during search warrant hearings. Additional information provided by the applicant during the hearing of a search warrant application should be recorded. However, search warrant applications in the magistrates' courts are not recorded, meaning that a handwritten or typed note must be made. We conclude that it would be desirable to introduce a standard audio recording procedure and recommend that the Ministry of Justice examines the practicability of audio recording search warrants hearings in the magistrates' court and out of hours.

1.78 We then consider the position concerning the provision of written reasons for issuing a search warrant. We agree with the present position: a failure to give reasons should not necessarily invalidate a search warrant if it is clear that the court was presented with evidence of sufficient grounds to issue the warrant. For this reason, amongst others, we

consider reform to the current position, whereby search warrant application forms invite the issuing authority to give reasons, to be unnecessary.

1.79 We end the chapter by considering record keeping and statistics concerning search warrants. There have been many complaints about the lack of statistical information on search warrants. We conclude that record keeping and statistics would provide a number of benefits, and therefore recommend that certain categories of data concerning warrants be collected and published by HMCTS, with the assistance of law enforcement agencies where possible.

Chapter 7: The conduct of a search under warrant

1.80 In Chapter 7 of this report, we consider reform to various aspects of the execution of a search warrant.

1.81 We begin by considering the requirement to specify who may accompany the person conducting a search under a warrant. There is ambiguity in respect of certain regimes over whether the person accompanying a constable must be a named individual, or whether it is sufficient to refer to the role that person will perform in the course of the execution of the warrant. We conclude that search warrants should only be required to state the agency or role of the individual who is to accompany the person executing the warrant. Reflecting on the current law, we conclude that certain regimes do permit an individual's role, rather than their name, to be specified by the warrant or an investigator. We conclude that there is strong justification for clarifying this position in several statutes and make a recommendation accordingly.

1.82 We consider next the length of time for which a search warrant should remain valid. We do not consider that uniformity across all search warrant provisions should be pursued for its own sake. Nor do we consider that the period of validity provided for under any particular search warrant provision ought to be amended given that we did not receive evidence that problems arise in practice.

1.83 We turn next to examine the number of visits to premises that may be authorised under a single search warrant. A number of search warrant provisions include a power to apply for a warrant authorising multiple entries. We conclude that it would be desirable to extend this power to search warrants under section 2 of the CJA, section 352 of the Proceeds of Crime Act 2002 ("POCA"), and section 176 of the Financial Services and Markets Act 2000 ("FSMA"), with appropriate safeguards, and make a recommendation accordingly.

1.84 We then consider the power to access all premises occupied or controlled by an individual. As with multiple entry warrants, a number of search warrant provisions include a power to apply for a warrant authorising the entry of all premises occupied or controlled by a person. We conclude that it would also be desirable to extend this power to search warrants under section 2 of the CJA, section 352 of POCA, and section 176 of FSMA, with appropriate safeguards, and make a recommendation accordingly.

1.85 Next, we consider the search of persons on premises during the execution of a warrant. While a person may be searched on premises in several circumstances, there is nothing in section 8 of, or schedule 1 to, PACE to allow warrants issued under those provisions to permit the police to search persons who are on the premises subject to the search. We conclude that such a power would be desirable and recommend that it be introduced, subject to stringent safeguards.

1.86 We consider next the time at which a search under warrant is conducted. Under the majority of search warrant provisions, a search warrant must be executed at a reasonable hour unless to do so would frustrate the purpose of the investigation. We conclude that the latitude afforded under this test should be retained for operational reasons. However, to ensure that entry and search under warrant is proportionate, we recommend, first, that application forms invite the issuing authority to record their reasons for granting a warrant which may be executed outside usual hours and, second, that the PACE Strategy Board consider amending Code B of PACE to provide guidance as to what constitutes a reasonable hour.

1.87 We then consider the information provided to the occupier during the search. Section 16 of PACE lists several pieces of information which must be provided to occupiers. Given the heavy qualifications to these provisions provided in case law, and to ensure consistency in practice, we recommend that the PACE Strategy Board consider amending Code B of PACE to reflect these developments.

1.88 Next, we consider the desirability of the provision of an authoritative guide to search warrants for occupiers. If an officer conducts a search to which Code B of PACE applies, Code B of PACE states that the officer shall, unless it is impracticable to do so, provide the occupier with a copy of a "notice of powers and rights". We recommend that the duty to produce a notice of powers and rights be put on statutory footing. We also recommend the introduction of a specific search warrants "your rights and the law" webpage on the Government website.

1.89 We then consider a requirement to inform an occupier how to apply for the underlying information sworn in support of a search warrant application. We conclude for a number of reasons that it would be preferable for the right to be included in the notice of powers and rights rather than on the face of the warrant.

1.90 Finally, we consider the presence of legal representatives during the execution of a search warrant. At present, there is no guidance which sets out the permissible functions of a legal representative who is present during a search, even though it is common for occupiers to ask a legal representative to be present at the search in large-scale financial investigations. We therefore recommend that Code B of PACE should make clear that a legal representative must be allowed to be present and observe a search under warrant to make their own notes, subject to the same qualifier as currently applies in Code B of PACE when a friend or neighbour is requested: the ultimate decision whether to delay a search should remain with the investigator carrying out the search.

Chapter 8: Challenging a search warrant

1.91 In Chapter 8 of this report, we consider how challenges can be made to both the lawfulness of a search warrant and the way in which a search under warrant has been conducted.

1.92 We begin by considering the introduction of a new Crown Court procedure for challenging a search warrant or the conduct of a search. After carefully considering consultation responses, we are no longer of the view that there would be merit in the introduction of an entirely new procedure to challenge search warrants in the Crown Court. We set out in detail why the procedure we proposed in our consultation paper would be an unsatisfactory mechanism for challenging search warrants. We also consider that recommendations made elsewhere in this report would promote access to justice and produce greater efficiency in the system.

1.93 The remainder of the chapter considers possible amendments to section 59 of the CJPA, which allows for applications to be made to the Crown Court for the return or retention of material taken during a search. At present, the Crown Court is unable to make orders for costs in section 59 proceedings. We conclude that it would be desirable to introduce a costs regime and so recommend that a judge hearing an application under section 59 of the CJPA have the power to order costs between parties.

1.94 At present, a High Court judge cannot exercise the powers under section 59 of the CJPA when hearing a claim for judicial review. For example, where a warrant has been quashed and no order, or a conditional order, is made for the material seized to be returned, an investigator must make a separate application under section 59(6) of the CJPA to retain the material. To save cost and promote efficiency, we recommend that a judge hearing a judicial review of a search warrant should have the powers and duties of the Crown Court in relation to the return or retention of material under section 59 of the CJPA.

Chapter 9: Sensitive material and public interest immunity

1.95 In Chapter 9 of this report, we consider the procedure for dealing with sensitive information contained in an application for a search warrant and claims for public interest immunity.

1.96 We begin the chapter by setting out the procedure under the current law when search warrant applications involve sensitive material and public interest immunity claims, in order to contextualise the consultation responses that we received and our analysis of them.

1.97 We look first at how sensitive material is stored. We conclude that more prescriptive rules governing the handling of sensitive material in the CrimPR would be beneficial given the lack of a consistent approach. We consider that sensitive material is likely to be better protected if stored by the investigator, however, discretion must ultimately reside with the court. We provide a suggestion of what more prescriptive rules might look like and then recommend that the Criminal Procedure Rules are amended to include rules governing the storage of sensitive material provided to the court during a search warrant application. We end the section by discussing two related issues concerning the use of a separate sensitive document when applying for a search warrant.

1.98 We turn to discuss the investigator's right to register an objection to an application by a person affected by a warrant for supply of the underlying information, the procedure for which is currently set out in the CrimPR. We recognise the concerns expressed to us that the current procedure carries the risk that an investigator might not have notice of a request for disclosure of an application in time, or at all, resulting in the disclosure of highly sensitive information. We discuss a number of options for reform, by none of which we are entirely persuaded. We therefore recommend that the CPRC consider the desirability of amending the rules governing an investigator's right to issue an objection, with the aim of ensuring that the investigator receives the relevant request.

1.99 We then discuss the desirability of formalising the matters relevant to the court's decision to disclose sensitive material. We recognise the value in elaborating on such matters. Accordingly, we recommend that consideration be given to amending the Criminal Practice Directions to set out matters that should be considered by the court when determining whether sensitive material ought to be withheld on the grounds of public interest immunity.

1.100 Finally, we discuss the consequences of a decision to order disclosure of sensitive material and whether the investigator should have the option to avoid disclosure by returning the material seized. We explain that, for several reasons, we consider that it would be

inappropriate for law enforcement agencies to be able to avoid the disclosure of material where it is ordered by the court.

Chapter 10: Iniquitous material

1.101 In Chapter 10 of this report, we consider the operation of what is known as the "iniquity exception" or "crime-fraud exception" whereby the protection afforded to special categories of material we term "protected material"[16] is lost when, broadly speaking, it is created, acquired or held for an iniquitous purpose.

1.102 We begin the chapter by setting out a detailed discussion of the current law, identifying specific areas of ambiguity. We identify three different formulations of the iniquity exception, two of which are statutory and another which is a common law exception. We then set out comments provided by consultees on the current law and how it ought to be reformed. We note the overwhelming majority of consultees considered that the broad common law iniquity exception should be replaced with a clear statutory test. However, there is a clear divergence of views as to what the test should be.

1.103 We conclude that it as unsatisfactory that there is neither a clear nor coherent approach to the principle of iniquity under the current law. The lack of clarity around the categories of material vulnerable to iniquity, the test to be applied and the effect on the material creates confusion and other problems in practice. For this reason, we recommend that the Government considers whether the law relating to iniquitous material in the context of criminal investigations ought to be reformed. We also provide views on the matters which should be taken into account should such reform be considered desirable.

Chapter 11: The treatment of legally privileged material

1.104 In Chapter 11 of this report, we consider reform to the way in which legally privileged material is treated. We do not propose altering the protection which is currently afforded to legally privileged material. Instead, we consider changes to how legally privileged material is sifted and how disputes regarding its treatment are resolved.

1.105 We begin the chapter by examining the case for introducing a formal procedure by which independent counsel are instructed to assist in identifying legally privileged material and separating it from other material. To retain flexibility, we recommend that the procedure for instructing independent lawyers or other experts to resolve issues associated with legal privilege be set out in a new Code of Practice. We also recommend a Code of Practice governing the acquisition and treatment of electronic material (some of which may be legally privileged) later in Chapter 17 of this report.

1.106 We then turn to examine whether it would be desirable to introduce a new procedure requiring a person who claims that material sought under a warrant contains legally privileged material to assist in identifying that material, so that it can be segregated, returned and deleted more quickly. We do not recommend such a procedure. In Chapter 17 of this report, we recommend that a person with an interest in electronic material be able to apply to the Crown Court for a judge to decide how the investigator should treat electronic material, for example, how legally privileged material should be sifted. This procedure would

---

16 That is typically, depending on the statutory regime: (1) legally privileged material; (2) excluded material (confidential personal records, human tissue, tissue fluid and confidential journalistic material); and (3) special procedure material (confidential business records and non-confidential journalistic material).

also enable a law enforcement agency to seek judicial approval of a protocol which details how they propose to sift material and resolve disputes between the parties. We conclude that this recommendation would satisfactorily address the specific concerns that the original procedure discussed at the start of this paragraph was designed to address.

Chapter 12: The treatment of excluded material

1.107 In Chapter 12 of this report, we consider reform to the way in which "excluded material" (ie confidential personal records, human tissue and fluid and confidential journalistic material) is treated when applying for and executing a search warrant.

1.108 We begin by considering the position in respect of confidential personal records, which include medical and counselling records. We explain how the circumstances in which excluded material can be obtained by investigators in criminal investigations vary. We conclude that a uniform scheme of identical statutory access conditions in respect of confidential personal records is not in itself desirable and that each regime must be carefully considered.

1.109 In respect of PACE, we conclude that the current statutory conditions for a search warrant regarding confidential personal records are too restrictive, thereby impeding serious criminal investigations. There are issues both in respect of how the statutory conditions operate and the underlying policy of the statutory conditions. Further, other mechanisms to obtain confidential personal records are unsatisfactory. We conclude that, for several reasons, it would be desirable for confidential personal records to be subject to the same statutory access conditions as "special procedure material", which are set out in paragraph 2 of schedule 1 to PACE. However, for a number of reasons, we do not make a firm recommendation for reform. Instead, we recommend that the Government considers whether the law governing access to confidential personal records, human tissue and tissue fluid under PACE strikes the right balance between the competing interests at play, and whether the law ought to be reformed.

1.110 We then consider the position of confidential journalistic material. We adopt much the same analysis as we do in respect of confidential personal records. We conclude that a uniform scheme of identical statutory access conditions across all search warrant provisions is not in itself desirable. With the exception of media organisations, consultation responses indicated clear support that confidential journalistic material should remain obtainable under PACE in exceptional circumstances. We reach the view that confidential journalistic material should remain obtainable under PACE in very limited circumstances. As with confidential personal records, human tissue and tissue fluid, we consider that there is an argument that alignment with the first set of access conditions might be desirable; however, we do not recommend reform for the same reasons as for those categories of material. Instead, we again recommend that the Government considers whether the law governing access to confidential journalistic material under PACE strikes the right balance between the competing interests at play, and whether the law ought to be reformed.

1.111 We turn next to consider the second set of access conditions under paragraph 3 of schedule 1 to PACE, which governs applications for production orders and search warrants in respect of excluded material. The second set of access conditions are used extremely rarely. However, we conclude that it would be inappropriate to repeal the second set of access conditions at this time, as it would make it impossible to obtain a production order or search warrant for excluded material under PACE. While the test under the second set of access conditions is highly restrictive, and in our view both impractical and arbitrary, it does allow for

excluded material to be obtained in some limited cases. The second set of access conditions is therefore better than having no access conditions for excluded material and so should not be abolished without a more wholesale restructuring of the regime, for which we consider there are strong arguments.

1.112 We end the chapter by considering the protection afforded to excluded material and special procedure material in cases of seizure not under warrant. Excluded material and special procedure material can only be searched for and seized under a warrant issued under schedule 1 to PACE. However, these categories of material can be searched for and seized under several other provisions of PACE following the arrest of a person or when a constable is lawfully on premises. We acknowledge the argument that excluded material and special procedure material should be exempt from seizure under arrest and other powers that do not require judicial authorisation. However, we conclude that, for several reasons, it would be undesirable to amend these powers, which in any event fall outside of our terms of reference.

Chapter 13: The treatment of special procedure material

1.113 In Chapter 13 of this report, we consider reform to the way in which "special procedure material" (ie non-confidential journalistic material and confidential business records) is treated.

1.114 We consider, first, the desirability of a uniform scheme for the availability of special procedure material under search warrants relating to a criminal investigation. The legislative framework dealing with special procedure material is equally as complex as that for excluded material, with the availability of such material varying across regimes. We conclude that a uniform scheme would be undesirable, as the centrality of special procedure material to different agencies justifies differing statutory access conditions. Nor are there any specific legislative regimes in which we can conclude the rules governing the availability of special procedure material require modification.

1.115 We turn to consider the position where the target material includes both special procedure material and ordinary non-protected material. Consultees reported problems that arise in practice where investigators seek both ordinary and special procedure material. We conclude that a schedule 1 to PACE warrant can in fact be obtained where the target material includes both ordinary material and special procedure material.

1.116 We then consider the position where the target special procedure material is mixed with excluded material which cannot be sought. We observe that the wording of paragraph 2(a)(ii) of schedule 1 to PACE may lead to an individual being able to resist the grant of a production order merely on the grounds that to sift special procedure material from excluded material would impose a burden. We consider that it would be desirable to amend the statutory access conditions so that a production order could only be granted where it would not be reasonably practicable for special procedure material to be sifted. However, we make no formal recommendation for reform as any amendment would fundamentally alter the operation of production orders, on which we did not directly consult.

1.117 We then turn to discuss the disclosure of non-confidential journalistic material. A media consultee expressed concern regarding the protection afforded to non-confidential journalistic material and the risk that the disclosure of such material may nonetheless reveal sources. In our view, the answer to the concern raised lies in the application of the public interest test under paragraph 2(c) of schedule 1 to PACE when deciding whether to grant a production order or search warrant. Additionally, the issuing authority must take into account

the right to freedom of expression protected by article 10 of the European Convention on Human Rights when exercising its discretion.

1.118 Next, we consider the desirability of expanding the definition of special procedure material to include material protected under the General Data Protection Regulation ("GDPR"). The GDPR applies to the processing of personal data, which may include special category data. We conclude that, for a number of reasons, it would not be desirable for personal data and special category data to be absorbed into the definition of special procedure material.

1.119 We end the chapter by considering the desirability of issuing further guidance on the meaning of special procedure material. Consultation responses reveal that investigators find it difficult to ascertain whether material is special procedure material. We conclude that greater clarity is needed to identify when material constitutes special procedure material, in order to better inform law enforcement agencies and reduce the risk of unlawful search and seizures. We recommend that Code B of PACE is revised to provide guidance on when material constitutes special procedure material.

Chapter 14: An introduction to electronic material and the law

1.120 In Chapter 14 of this report, we provide an introduction to the topic of electronic material in order to provide essential context for the issues discussed in the next four chapters. The central question with which these chapters are concerned is: what ought to be the law and procedure when an investigator seeks to obtain electronic data stored on, or accessible from, a device on premises under the authority of a search warrant?

1.121 We begin the chapter by discussing the nature of electronic material, including the key characteristics of electronic devices and electronic data. We explain the different ways in which electronic material can be categorised. We then discuss the features of electronic devices, including how they store data. We also explain the characteristics of electronic data, including how it is shared through network systems and the means by which its accessibility can be affected. We then explain how data can be stored remotely and the features of cloud computing.

1.122 Next, we provide an overview of the relevant legal regimes which govern the acquisition and treatment of electronic material. When electronic material is sought in criminal investigations, there are a number of investigative powers under a range of different legal regimes that may be used both prior to and during, or in the alternative to, the execution of a search warrant. These powers allow investigators to request and compel the production of or access to information, interfere with electronic devices and intercept electronic data.

1.123 We then discuss how searches under warrant for electronic material operate in practice, and in particular the use of digital forensics. We provide an overview of when and how electronic devices are examined, including the types of data extraction and the increasing use of data extraction devices.

1.124 We end the chapter by setting out the problems with the current law concerning the acquisition and treatment of electronic material. We explain that electronic material raises novel, complex and sensitive issues in respect of the law governing not only search warrants, but the acquisition and treatment of material generally. The issues which we have identified with the law fall in essence into one of two categories. First, the lack of clear and effective legal bases to acquire electronic material. Secondly, the lack of sufficient safeguards in respect of the acquisition and treatment electronic material.

Chapter 15: The search for and seizure of locally stored electronic material

1.125 In Chapter 15 of this report, we discuss reform to the law relating to the search for and seizure of electronic devices and electronic data stored locally on those devices.

1.126 We begin the chapter by considering the legislative terminology used to refer to electronic material which is the target of a search warrant. We conclude that all forms of electronic material should be, and under certain regimes are, on their face, capable of being the target of a search warrant. We conclude that there are no search warrant provisions which require reform in this regard.

1.127 We consider next the satisfying of the statutory access condition for the issue of a search warrant when the target of a warrant is an electronic device. We conclude that search warrant provisions should continue to permit electronic devices to be the target of a search warrant where investigators seek relevant information in electronic form. However, we recommend that search warrant provisions are amended to clarify that, when electronic data is sought, electronic devices can be the target of a search warrant so long as the data satisfies the statutory conditions relating to the target material.

1.128 We then turn to consider the procedure for applying for a search warrant where electronic material is the target of a search. We conclude that there are two ways in which application forms ought to be amended to encourage consideration of the necessity and proportionality of the search for and seizure of electronic devices. Accordingly, we recommend that the CPRC consider amending search warrant application forms to require an investigator, when they are seeking to obtain a warrant to search for and seize electronic devices to acquire electronic data, to explain (1) in as much detail as practicable what information on devices is sought; and (2) why they believe that the information is on the device and why the information would satisfy the statutory conditions. However, for several reasons, we conclude that it would not be desirable to require pre-search protocols at the application stage to set out how investigators intend to treat electronic devices.

1.129 We then consider the specifying of electronic material on the face of a search warrant when it is the target of a search warrant. We conclude that electronic devices should be capable of being specified on the face of the warrant as the material to be searched for on premises and seized. However, for several reasons, we recommend that search warrants are required to contain two parts when electronic devices are sought for the purpose of obtaining information in the form of electronic data. The first part should specify the electronic device(s) to be searched for and seized. The second part should specify the information on the electronic device(s) that is sought.

1.130 Next, we consider the seizure of electronic devices when executing a search warrant. We conclude that search warrants should continue to permit the seizure or copying of entire electronic devices where it is necessary to do so and safeguards are adhered to. We also recommend that search warrant provisions are amended to make clear that the power to seize an electronic device includes the power to copy all or some of the electronic data stored on an electronic device while on premises.

1.131 We end the chapter by considering the search of electronic devices on premises and subsequent seizure of electronic data. We conclude that it is unclear whether certain search warrant provisions permit an investigator to search electronic devices while on premises. To encourage proportionality and facilitate dynamic decision-making, we recommend that search warrant provisions should be amended to permit an investigator to apply for authority to conduct a search of electronic devices found during the course of a search where it is

necessary to do so for the purpose for which the warrant is issued. If granted, the warrant should authorise the search for and copying of any electronic data stored on the device that falls within the information specified in the second part of a search warrant, which we recommend earlier in the chapter.

Chapter 16: The search for and seizure of remotely stored electronic data

1.132 In Chapter 16 of this report, we discuss the powers that law enforcement agencies ought to have to search for and seize (ie copy) remotely stored electronic data under a search warrant.

1.133 We begin the chapter by discussing the extraterritoriality of powers of search, seizure and production. We conclude that it is unclear whether powers of search, seizure and production exercised within this jurisdiction in relation to remotely stored data should be classified as extraterritorial: while the powers are exercised within this jurisdiction, the location of data still holds particular significance. However, even if such powers were to be deemed extraterritorial, we consider it unlikely that the presumption against a statute having extraterritorial effect would operate so as to prevent the powers being exercisable in respect of remotely stored data.

1.134 We then turn to consider the circumstances in which the search, seizure and production of remotely stored data is permissible under international law. We conclude that the answer, too, is unclear: state practice indicates certain instances in which the conduct might be deemed acceptable, however, concerns clearly remain in the international community with no clear international consensus. That said, we consider that there will be circumstances in which the search, seizure or production of remotely stored data pursuant to a warrant is unlikely to cause a grievance from another state and that any infringement on the sovereignty of another state would be *de minimis*.

1.135 Next, we discuss the circumstances in which law enforcement agencies ought to be able to search for and copy remotely stored data from an electronic device on premises. We conclude that the current circumstances in which such action is permissible are unclear. We then conclude that law enforcement agencies should be given the powers to enter premises, search for and copy remotely stored data when executing a search warrant. We are unable to reach a definitive conclusion on the appropriate model to be adopted for the search and seizure of remotely stored data in respect of the many search warrant regimes without further technical and cross-sectional input. We therefore recommend that the Government considers the desirability of amending the law to permit law enforcement agencies to obtain authorisation to search for and copy remotely stored data when executing a search warrant.

1.136 We then turn to consider amending the law governing the power to compel the production of passwords and other access information. We accept that without a power to require passwords, any power to search for and copy remotely stored material will be rendered ineffective in certain circumstances given that virtually all electronic data is protected by either a password, encryption or two-factor authentication.[17] We set out the various arguments in favour of reforming the law. For a number of reasons, we do not make a firm recommendation. That said, based on the consultation responses that we did receive, and the analysis that we have undertaken, we consider that it is a matter that would merit further consideration. We therefore recommend that the Government considers the desirability of

[17] We explain what these security features are at paragraph 14.23.

amending the law governing the power to compel the production of passwords and other access information with the aim of making the law clearer and more effective. This should include consideration of an integrated power to form part of search warrant regimes.

1.137 We turn finally to consider introducing a power to modify or alter remotely stored data in order to preserve it and prevent interference. We conclude that there are few, if any, statutory powers that could be relied on as a lawful basis to modify or alter remotely stored data. We then conclude that other methods of seeking preservation are not an effective means of preventing the modification or alteration of remotely stored data to prevent interference. We recognise the rationale of a power to modify or alter data to prevent interference, as well as the valid concerns that would be raised by such an intrusive power. Again, for a number of reasons, we do not make a firm recommendation. We do, however, recommend that the Government considers the desirability of introducing a power to modify or alter remotely stored data exercisable pursuant to a search warrant.

Chapter 17: The treatment of seized electronic material

1.138 In Chapter 17 of this report, we consider the law and procedure which governs the treatment of electronic material once it is in the possession of a law enforcement agency following the execution of a search warrant.

1.139 We recommend in this chapter a new statutory regime to govern the treatment of electronic material seized or copied pursuant to a search warrant. We also recommend that the regime is supplemented by a new Code of Practice which would regulate the acquisition and treatment of electronic material in search warrant cases. Set out together, the recommendations that we make in this chapter are as follows.

(1) We recommend the introduction of a new statutory regime governing the treatment of electronic material. The regime ought to apply whenever a relevant power of seizure or production is exercised in respect of electronic material following the execution of a search warrant.

(2) We recommend that, under this new statutory regime, an investigator be required to provide the following information within a reasonable time from a person with an interest in the electronic material making a request for it:

(a) as specific a description of what was seized as is reasonably practicable;

(b) details of what action was taken in respect of electronic devices on premises in as much detail as practicable; and

(c) protocols setting out how electronic material is to be examined.

(3) We also recommend that an investigator be required to comply with the following statutory duties:

(a) to return electronic devices following seizure on premises as soon as reasonably practicable;

(b) to return and/or delete electronic material as soon as reasonably practicable; and

(c) to return and/or delete non-responsive electronic material so far as is reasonably practicable.

(4) We also recommend that a person with an interest in electronic material be able to apply to the Crown Court for:

(a) a judge to approve of, or adjudicate on disputes regarding, the way in which the investigator intends to examine electronic material; and

(b) the return or deletion of particular electronic data or return of an electronic device on the grounds that:

(i) the electronic material is reasonably required by the person with an interest in it; or

(ii) continued retention by an investigator of the electronic material is not necessary.

(5) Finally, we recommend the creation of a Code of Practice governing the acquisition and treatment of electronic material in criminal investigations involving search warrants.

Chapter 18: A wider review of the law governing electronic material

1.140 In Chapter 18 of this report, we discuss the need for a wider review of the law governing the acquisition and treatment of electronic material in criminal investigations, which is not confined solely to search warrants.

1.141 We begin the chapter by setting out the reasons justifying a wider review of the law governing electronic material. We explain that the problems discussed in our report transcend search warrants. Amendment to search warrants legislation would also not be a viable long-term solution to the problems posed by cloud computing. The interconnectivity of investigative powers also raises questions over where certain powers should be contained. There are also arguments that some of our recommendations should apply beyond the search warrants context. Additionally, consultation responses indicated that there are several other statutory powers that may require reform.

1.142 We then set out those topics which we regard as germane to a wider review. First, consideration should be given to the desirability of powers to search electronic devices not contingent on premises, or to search electronic data directly. Secondly, consideration should be given to the operation of sections 19(4) and 20(1) of PACE. Thirdly, consideration should be given to the regulation of data extraction devices, in addition to the extraction of data from complainants' devices. Accordingly, we recommend a wider review of the operation of powers of search, production and seizure in respect of electronic material when investigating criminal offences not confined to cases where such powers are exercised pursuant to a search warrant or in respect of premises.

Chapter 19: Consolidating search warrants legislation

1.143 In Chapter 19 of this report, we discuss the desirability of consolidating search warrant provisions, as well as repealing unnecessary provisions and standardising certain statutory conditions.

1.144 We begin the chapter by discussing whether there are any unnecessary search warrant provisions which ought to be repealed. We remain of the view expressed in our consultation paper that, in principle, obsolete search warrant provisions should be repealed. However, we did not receive sufficient evidence to enable us to conclude that any particular search warrant provisions are unnecessary and suitable for repeal. Given the potential risk of creating gaps in enforcement regimes, we make no recommendations as to repeal.

1.145 Next, we consider the desirability of consolidating search warrant provisions into a single statute. We explain that there are two potential forms of consolidation. First, bringing search warrant provisions into one statute and codifying the statutory conditions and powers. Secondly, strict consolidation by creating a single statute which contains all of the law on search warrants but does not actually alter the law. We conclude that neither would be desirable. Search warrant provisions form part of wider enforcement regimes and sit better in the statutes that regulate each law enforcement agency more generally, especially given the presence of related investigative powers in those statutes that interact with search warrant provisions. The burden of consolidation, in terms of the Law Commission, Parliamentary Counsel, consultees and Parliament's time, would be unlikely to outweigh any benefit. Other changes, including issuing clearer guidance, would be a more proportionate response to the problems with the current law.

1.146 We turn to consider the desirability of partially consolidating search warrant provisions into related groups of powers. For the reasons in the paragraph above, we reach the same conclusion that it would not be desirable. While some form of very minimal consolidation might avoid the above concerns, the benefits of consolidation on such a small scale, if any, would be nominal.

1.147 We end the chapter by considering the desirability of standardising the accessibility conditions through harmonisation. We use the term "accessibility conditions" to describe the subset of statutory conditions that relate to the impracticability of gaining access to the premises or material without a search warrant. We identified variations across the accessibility conditions. However, based on consultees' responses, we conclude that there would be no value in standardising the accessibility conditions, and it may in fact affect the operation of enforcement regimes in all sorts of undesirable ways.

ACKNOWLEDGMENTS

1.148 First and foremost, we acknowledge and thank Professor David Ormerod QC who was Commissioner of Criminal Law prior to the appointment of Professor Penney Lewis. Without Professor Ormerod's insight and guidance during the pre-consultation, consultation, policy development and early writing stages of this report, this project could never have reached completion. The final recommendations should not be taken to represent Professor Ormerod's views.

1.149 We have held a number of meetings with individuals and organisations while we have been preparing this paper, and we are extremely grateful to them all for giving us their time and expertise so generously. We are also particularly grateful to James Mullen, Micheál Ó Floinn and Karl Laird who acted as consultants on this project.

THE TEAM WHO WORKED ON THIS REPORT

1.150 The following members of the Law Commission worked on this report: Alex Davidson (lawyer); and Samantha Magor (research assistant).

Chapter 2: The operation of the statutory safeguards

INTRODUCTION

2.1 Statutory safeguards which an investigator must follow when applying for and executing a search warrant are contained within sections 15 and 16 of PACE. Section 15 of PACE, titled "search warrants – safeguards", specifies the requirements applicable to the process of obtaining a search warrant and the content of the warrant itself. Section 16 of PACE, titled "execution of warrants", governs how searches under warrant must be carried out and the steps to be taken post-search. Sections 15 and 16 of PACE are supplemented by Code B of PACE, a Code of Practice which governs the exercise of police powers to search premises. Code B of PACE provides further guidance on applying for and executing a search warrant.

2.2 Examples of the safeguards in section 15 of PACE are a requirement to state the grounds on which the warrant is sought and to specify matters about the proposed search, such as the articles sought and the premises to which it applies. Examples of the safeguards in section 16 of PACE are a requirement only to search premises once without special authorisation, to conduct searches at a reasonable hour and to produce identification and a copy of the warrant when lawful entry is effected.

2.3 Sections 15 and 16 of PACE help ensure compliance with the European Convention of Human Rights ("ECHR") requirement that any search under warrant is a proportionate interference within article 8 of the ECHR.[1] Breaches of these safeguards have led in some cases to search warrants being declared unlawful.[2]

2.4 The operation of sections 15 and 16 of PACE is governed by section 15(1) of PACE, which provides:

> This section and section 16 below have effect in relation to the issue to constables under any enactment, including an enactment contained in an Act passed after this Act, of warrants to enter and search premises; and an entry on or search of premises under a warrant is unlawful unless it complies with this section and section 16 below.

2.5 Section 15(1) of PACE therefore has two components, separated by a semicolon. First, the subsection sets out the people and warrants to which the safeguards apply. Secondly, the subsection provides that failure to comply with the safeguards renders an entry or search unlawful.

2.6 In this chapter, we consider reform to the operation of the safeguards. In particular, we discuss:

(1) when the statutory safeguards under sections 15 and 16 of PACE should apply to search warrants;

---

1 *Kent Pharmaceuticals v Director of the Serious Fraud Office* [2002] EWHC 3023 (QB) at [30] by Lord Woolf CJ.

2 For example, *R (Brook) v Preston Crown Court* [2018] EWHC 2024 (Admin), [2018] ACD 95; *R (Superior Import / Export Ltd) v Revenue and Customs Commissioners* [2017] EWHC 3172 (Admin), [2018] Lloyd's Rep FC 115; and *R (F) v Blackfriars Crown Court* [2014] EWHC 1541 (Admin).

(2) whether the statutory safeguards under sections 15 and 16 of PACE should be extended to apply to warrants which permit entry or inspection only;

(3) when regard should be had to Code B of PACE by non-police investigators;

(4) what conduct must comply with sections 15 and 16 of PACE;

(5) which elements of the search may be rendered unlawful as a result of non-compliance with sections 15 and 16 of PACE; and,

(6) when breaches of sections 15 and 16 of PACE render the entry, or search, unlawful.

2.7 In summary, we have departed from our provisional view that the statutory safeguards under sections 15 and 16 of PACE should be extended to all warrants relating to a criminal investigation by a single amendment to section 15(1) of PACE. This is because any reform of the statutory safeguards would require careful consideration of each search warrants regime which may be affected. However, we conclude that section 2 of the Criminal Justice Act 1987 ("CJA"), which relates to searches by the Serious Fraud Office ("SFO"), merits specific amendment by introducing statutory safeguards.

2.8 We then turn to consider Code B of PACE. We conclude that the burgeoning number of law enforcement agencies that can now apply for and execute warrants for the purpose of a criminal investigation justifies Code B of PACE providing more detail than it currently does. Accordingly, we recommend that the PACE Strategy Board consider amending Code B of PACE to provide guidance for non-police investigators in complying with the provisions of the Code.

2.9 Finally, we recommend amending section 15(1) of PACE to clarify the extent to which compliance with the safeguards in sections 15 and 16 of PACE is required. These reforms would lead to a greater awareness of the safeguards to be followed by law enforcement agencies when applying for and executing a search warrant.

WHEN SHOULD SECTIONS 15 AND 16 OF THE POLICE AND CRIMINAL EVIDENCE ACT 1984 APPLY?

The current law

2.10 In this section, we are concerned with the first component of section 15(1): the people and warrants to which the safeguards apply. In summary, for sections 15 and 16 to apply, a warrant under any enactment must be:

(1) issued to a constable; and

(2) to enter and search premises.

2.11 In some circumstances, sections 15 and 16 of PACE have been extended by statute so that the safeguards apply to other specified investigators who can apply for search warrants under PACE[3] or other Acts.[4] In other cases, specific statutory provisions for search warrants

[3] Welsh Revenue Authority (Powers to Investigate Criminal Offences) Regulations 2018 (SI 2018 No 400), sch 1, para 1; Police and Criminal Evidence Act 1984 (Application to Revenue and Customs) Order 2015 (SI 2015 No 1783), sch 1; Police and Criminal Evidence Act 1984 (Application to immigration officers and designated customs officials in England and Wales) Order 2013 (SI 2013 No 1542), schs 1 and 2; Police and Criminal Evidence Act

expressly state that the provision is subject to sections 15 and 16 of PACE, even if the investigation officer is not a constable.[5] Finally, in some circumstances sections 15 and 16 do not apply, but the provision under which the warrant is sought is subject to similar safeguards.[6] Warrants that are not subject to section 15(1) of PACE are still subject to common law protections, however, these requirements are far less extensive.[7]

The consultation paper

2.12 In the consultation paper, we described how section 15(1) of PACE may not afford adequate protection since it focuses on the official to whom the warrant is issued rather than the purpose of the search. The section may therefore not apply when certain investigators apply for a search warrant who do not otherwise have comparable safeguards for one of the reasons set out in paragraph 2.11 above. We illustrated this problem with the example of members of the SFO, who can apply for a search warrant under section 2(4) of the CJA.

(1) A search warrant under section 2(4) of the CJA appears to be "issued" to a member of the SFO. There is no statutory provision conferring upon members of the SFO the powers and privileges of a constable. As a consequence, section 15(1) of PACE does not apply as a search warrant under section 2(4) of the CJA is not issued to a constable.

(2) Sections 15 and 16 of PACE have not been extended specifically by statute to search warrants applied for under section 2(4) of the CJA, nor are there comparable safeguards under the CJA.

2.13 Accordingly, on our analysis, neither sections 15 and 16 nor comparable safeguards apply to search warrants under section 2(4) of the CJA.

2.14 In the light of our concern regarding the inadequacy of section 15(1) of PACE, we provisionally proposed[8] that the provision should be amended so that the statutory safeguards in sections 15 and 16 of the Police and Criminal Evidence Act 1984 apply to all search warrants that relate to a "criminal investigation". This would in effect recalibrate the focus of section 15(1) of PACE from the official to whom the warrant is issued to the purpose of the search, which we regarded as a clearer and more principled policy position.

2.15 We were keen to ensure that section 15(1) of PACE provided greater clarity and transparency about when the statutory safeguards apply. We therefore provisionally proposed[9] that an objective test should be introduced to determine whether a search warrant relates to a criminal investigation. The intention was to provide a single straightforward test to determine whether the statutory safeguards must be followed when applying for a warrant

---

1984 (Department of Trade and Industry Investigations) Order 2002 (SI 2002 No 2326), art 3; Police and Criminal Evidence Act 1984 (Application to Labour Abuse Prevention Officers) Regulations 2017 (SI 2017 No 520), reg 3.

4 Proceeds of Crime Act 2002 (Application of Police and Criminal Evidence Act 1984) Order 2015 (SI 2015 No 759) (as modified by SI 2017 No 1222), art 2.

5 Food and Environment Protection Act 1985, sch 2, para 7(4); Animal Welfare Act 2006, sch 2, para 1(1).

6 Immigration Act 1971, ss 28J and 28K.

7 *Inland Revenue Commissioners v Rossminster Ltd* [1980] AC 952. See R Stone, *The Law of Entry, Search, and Seizure* (5th ed 2013) para 1.48.

8 Consultation Question 1.

9 Consultation Question 3.

under any given search warrant provision. Accordingly, we provisionally proposed that any "search warrant that relates to a criminal investigation" should be defined as any search warrant for which the grounds for the application include facts or beliefs which (if true) would show that:

(1) a criminal offence has been, is being or is about to be committed; or

(2) there is to be found on the premises:

(a) evidence of the commission of a criminal offence;

(b) material which it is a criminal offence to possess;

(c) material obtained by means of a criminal offence or representing the proceeds of crime;

(d) material which has been, is being or is about to be used in connection with a criminal offence; or

(e) material connected to an ongoing criminal investigation.

2.16 The test was in effect intended to be a litmus test for determining whether a warrant related to a criminal investigation: if the statutory conditions on which an investigator relied for the issue of a warrant fell into one of the above categories, the safeguards would apply. The actual subjective intention of the investigator in applying for the warrant would therefore be irrelevant for the purpose of determining whether the safeguards were to be followed.

Consultation responses

2.17 In relation to our question whether the statutory safeguards should be extended so that they applied to all search warrants relating to a criminal investigation, 22 consultees responded: 20 agreed;[10] one disagreed;[11] and two expressed other views.[12]

2.18 In relation to our proposal to adopt an objective test for the purposes of determining whether a search warrant relates to a criminal investigation, 19 consultees answered this question: 14 agreed;[13] four disagreed;[14] and one expressed another view.[15]

---

10 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Guardian News and Media; Insolvency Service; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; The Law Society; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Serious Fraud Office; Financial Conduct Authority.

11 Competition and Markets Authority.

12 Crown Prosecution Service; Bar Council and the Criminal Bar Association.

13 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Insolvency Service; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; The Law Society; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; Justices' Clerks' Society; Magistrates Association; National Crime Agency; Metropolitan Police Service.

Extending the application of statutory safeguards to all search warrants relating to a criminal investigation

2.19 Consultees provided numerous reasons supporting the extension of the statutory safeguards to all search warrants relating to a criminal investigation, namely:

(1) that the current legal position is unclear and inconsistent[16] and the proposal would improve consistency in the search warrants process as well as resolve legal ambiguity;

(2) there has been an increase in the number of investigatory authorities able to apply for a warrant, with which the statutory safeguards have not kept pace;[17]

(3) safeguards should apply uniformly irrespective of who is applying for a search warrant;[18] and

(4) all search warrant applications involve a base level of intrusion irrespective of the investigator applying for the warrant.[19]

2.20 The reasons respondents gave for disagreeing with the proposal centred around the difficulty of transposing the provisions to other statutory regimes, which have their own bespoke safeguards. For example, the Competition and Markets Authority ("CMA") observed that:

(1) any extension would be unlikely to take account of the specificities of the CMA regimes;

(2) the safeguards are largely reproduced in CMA warrants;

(3) CMA warrants are of entry, not search, and therefore do not require material to be specified (this is discussed more below); and

(4) CMA execute their own search warrants and so would not want the requirement under section 16(2) of PACE extended, which would mean that a warrant must be executed by a constable whom the CMA accompany.[20]

2.21 Other consultees acknowledged that certain requirements are currently drafted in a manner that is specific to the police and would therefore require amendment.[21] In addition, it was suggested that consideration should be given to whether all of the statutory safeguards are necessary or whether some of the more administrative safeguards could be removed from

---

14 Crown Prosecution Service; Bar Council and the Criminal Bar Association; Competition and Markets Authority; Financial Conduct Authority.

15 Dijen Basu QC.

16 Council of Her Majesty's Circuit Judges.

17 Council of Her Majesty's Circuit Judges.

18 Kent County Council Trading Standards.

19 Birmingham Law Society.

20 We discuss the Police and Criminal Evidence Act 1984, s 16(2) at paragraph 7.9 below.

21 Financial Conduct Authority.

the statute and incorporated into the Codes of Practice.[22] The example was given of subsections 16(10) to (12), which govern the return of search warrants to, and retention by, the court.

2.22 The Crown Prosecution Service ("CPS"), Bar Council and the Criminal Bar Association ("CBA") considered that safeguards, be it those found in sections 15 and 16 of PACE or comparable safeguards, should not be limited to search warrants related to a criminal investigation but should extend to all search warrants. They pointed out that investigators should have little difficulty in meeting a common baseline of requirements which afford protections to the subject of the search.

Defining a search warrant that relates to a "criminal investigation"

2.23 The majority of consultees agreed with our objective formulation of a "criminal investigation" which should determine when the statutory safeguards should apply.

2.24 Of those who disagreed, there were two categories of objections raised by consultees. First, there were a number of objections to the way in which the objective test was formulated. Secondly, and more fundamentally, there were objections to adopting an objective test.

2.25 The principal objection to the way in which the objective test was formulated was that the first limb of the definition – "a criminal offence has been, is being or is about to be committed" – included the instances captured by the second limb (broadly, that evidence of a crime would be found on the premises), making the second limb superfluous.[23] Other minor amendments were also suggested to clarify when the test would apply.

2.26 The more fundamental objections to adopting an objective test for determining whether a search warrant related to a criminal investigation focused on:

(1) the workability of an objective test in practice;

(2) the preference for a subjective test for determining whether a search warrant relates to a criminal investigation; and

(3) the preference for extending the statutory safeguards to all search warrants, irrespective of the purpose for which they are obtained.

2.27 A number of consultees queried how the objective test would work in practice.[24] Several agencies have dual regulatory and prosecutorial functions: for example, the Financial Conduct Authority ("FCA"), the CMA, and the Health and Safety Executive. It was pointed out by the CPS and several other consultees that the test would impose obligations on a non-criminal or regulatory investigation which are not, and never would be, focused on securing evidence for a criminal prosecution. This is because the grounds for obtaining a search warrant may nonetheless be based on an allegation which, according to the objective test, classifies the investigation as criminal. Taking an FCA investigation as an example, the concern can be demonstrated in the following way.

---

22 Bar Council and the Criminal Bar Association.

23 Bar Council and the Criminal Bar Association; Birmingham Law Society.

24 Crown Prosecution Service; Financial Conduct Authority.

(1) No person may carry out a regulated activity in the UK (such as managing investments[25]), or purport to do so, unless they are authorised to do so or exempt from doing so.[26] A person who contravenes this general prohibition is guilty of a criminal offence.[27]

(2) The FCA may appoint investigators if it appears that there are circumstances suggesting that there has been a contravention of the above general prohibition and therefore the commission of a criminal offence.[28] Additionally, investigators may be appointed where a person may have contravened a rule made by the investigating authority which amounts to a regulatory breach.[29]

(3) A person appointed for either purpose above may require a person to provide such information as they may require for the purposes of the investigation.[30]

(4) A search warrant may be applied for where there are reasonable grounds for believing that:

(a) a person on whom an information requirement has been imposed has failed (wholly or in part) to comply with it; and

(b) on the premises specified in the warrant, there are documents which have been required, or there is information which has been required.[31]

(5) Accordingly, a search warrant may be sought from the same statutory provision in relation to both criminal and regulatory investigations.

2.28 There are two potential scenarios in which our proposed objective test may apply to investigations notwithstanding that they are civil or regulatory in nature.

2.29 First, indirectly, during a regulatory investigation, the documents for which a warrant might be sought may, on their face, disclose evidence of the commission of a criminal offence. For example, there may be cases where the conduct investigated in respect of a regulatory breach would amount to an offence in respect of the general prohibition on carrying out regulated activities. Therefore, there may be overlap between a civil investigation and our objective test of whether the investigation is criminal. Investigators carrying out civil or regulatory investigations would need to check in advance whether the facts relied on might also constitute a criminal offence. If so, the safeguards would be engaged.

2.30 Secondly, even where an investigator is *directly* searching for material which, for example, would amount to evidence that an unauthorised person is carrying out a regulated activity and therefore committing a criminal offence, a prosecution may not be the focus, or a

---

25 Financial Services and Markets Act 2000, sch 2, para 6.

26 Financial Services and Markets Act 2000, s 19.

27 Financial Services and Markets Act 2000, s 23.

28 Financial Services and Markets Act 2000, s 168(2).

29 Financial Services and Markets Act 2000, s 168(4)(c).

30 Financial Services and Markets Act 2000, s 173(2) where appointed under s 168(2) and Financial Services and Markets Act 2000, s 172(2)(b) where appointed under s 168(4).

31 Financial Services and Markets Act 2000, s 176(2).

proportionate outcome of, the investigation. This concern was also expressed by the CMA, who suggested that the objective test could result in the safeguards applying to warrants under their civil or administrative enforcement regimes where investigations are being carried out where there is no intention to institute criminal proceedings.

2.31 The CPS observed that the objective test creates a position whereby the safeguards attach not only where the warrant is sought based on the suspicion or belief of the investigator but where the objective interpretation of the content of the application causes it to be deemed criminal. The objective test will therefore require an investigator to consider which of a range of potential criminal offences might have been committed on the facts being presented even if there is, at the time of the warrant application, no intention to pursue a criminal investigation. This places a clear burden on the investigative agency which may be resource-intensive.

2.32 In defence of the objective test, the CPS acknowledged that it would protect those who are the subject of an investigation which begins as a non-criminal investigation (such as a regulatory investigation) but where the facts known to the investigator disclose a criminal offence and where ultimately the items seized lead to a prosecution.

2.33 Two alternative models to the objective test for determining whether a search warrant relates to a criminal investigation were canvassed. First, the FCA suggested that there should instead be a subjective test whereby the statutory safeguards apply where the purpose of the person making the warrant application is to determine whether to initiate criminal proceedings. In a similar vein, the Bar Council and the CBA queried the need to define a phrase as simple as "a search warrant that relates to a criminal investigation".[32]

2.34 Secondly, the CPS raised for consideration whether the safeguards *should* be restricted to criminal investigation warrants. The following observations were made:

(1) Section 6(1) of the Human Rights Act 1998 provides that it is unlawful for a public authority to act in a way which is incompatible with a Convention right. The duty is not restricted to the acts of public authorities in respect of criminal investigations only.

(2) Warrants which authorise entry into premises, be it for criminal or other purposes, intrinsically engage article 8 of the ECHR.

(3) The statutory safeguards are intended to ensure that where a person's premises, in particular their home, is invaded as a matter of law, they have sufficient information about why this is so.

(4) If there is concern regarding the fact that a person may be liable to criminal prosecution and penalties as a result of a warrant, then the safeguards to be focused on are those governing the use to which the material seized is to be put, and these are to be found in: (1) section 78 of Police and Criminal Evidence Act 1984; (2) the power to stay proceedings as an abuse of process; or (3) the powers to challenge a search warrant.

[32] We observe, however, the difficulty seemingly simple phrases have generated, such as a "criminal cause of matter". See *R (Belhaj) v DPP* [2018] UKSC 33, [2019] AC 593 at [73].

(5) Accordingly, it could be said that the statutory safeguards should not be restricted to search warrants which relate to a criminal investigation. Instead, they should apply to all warrants.

Analysis

2.35 In the light of consultees' responses, we are fortified in our view that, as a matter of policy, the statutory safeguards in sections 15 and 16 of PACE should apply to all search warrants relating to a criminal investigation. However, having regard to the concerns raised and after further detailed discussion with the Office of the Parliamentary Counsel, we are no longer of the view that the best way to give effect to that policy is by way of general amendment to section 15(1) of PACE to provide that sections 15 and 16 apply to all search warrants that relate to a criminal investigation. Instead, we consider that it would be better for legislative amendment to target directly those instances where the safeguards do not, but ought to apply.

The appropriateness of an objective test

2.36 Whilst a number of consultees supported the provisionally proposed objective test, we are persuaded that such a test might have unintended and arbitrary consequences in respect of agencies with dual roles to investigate criminal and civil matters. Such a test would require investigators to consider whether the safeguards apply even when carrying out a purely civil investigation with no prospect of criminal proceedings. This would impose an additional burden on investigators.

2.37 If the investigator did identify a criminal offence that applied, it would then be necessary to apply the safeguards in the course of applying for and executing a warrant that was only likely ever to have civil law consequences. That burden would, we are persuaded, be disproportionate. The test would not target criminal investigations in the way in which we intended when formulating our policy. We discuss the issues with expanding our enquiry into civil and regulatory regimes at paragraph 2.48 below. It would also be misleading to describe the statutory test as applying to search warrants which relate to a criminal investigation when in fact it may apply to other investigations.

2.38 We also consider that an objective test may introduce more legal ambiguity than we were seeking to remove. Determining whether the safeguards apply may involve an in-depth case analysis by investigators. The test may also be difficult to apply by those affected by a warrant. Without knowing the precise grounds on which the warrant was issued, an individual would not be able to ascertain if the safeguards applied and therefore whether there are grounds for challenging the warrant. The current law is therefore more workable from a practical perspective, as the question of whether the safeguards apply can be answered relatively straightforwardly by considering the wording of the statutory provision.

2.39 For these reasons, we now disagree with a statutory test centred on the facts which underpin the grounds for making the application.

The appropriateness of a subjective test

2.40 We accept that a test, similar to that propounded by the FCA, where the safeguards apply whenever a warrant is sought *for the purpose of* a criminal investigation, would be more practical.

2.41 Examples of the statutory safeguards being applied in this way already exist. Sections 15 and 16 of PACE have been specifically extended to search warrants *sought for the purposes*

of a confiscation investigation, a money laundering investigation, a detained cash investigation, a detained property investigation or a frozen funds investigation.[33] Notably, section 9(1) of PACE also uses the phrase "for the purposes of a criminal investigation", which the Divisional Court has read in the light of the definition of "criminal investigation" provided in section 22(1) of the Criminal Procedure and Investigations Act 1996.[34]

2.42 While a subjective test would be preferable to the objective test we provisionally proposed, we have concluded that neither an objective nor subjective test is desirable as a method for applying the statutory safeguards in sections 15 and 16 of PACE to over a hundred different statutory provisions. On the one hand, an objective test requires the application of rigid rules which may capture non-criminal investigations; it would therefore be over-inclusive. On the other hand, a subjective test may not capture some investigations in which criminal proceedings are later initiated; it would therefore risk being under-inclusive. Under a subjective test, disputes may also arise regarding whether the true and dominant purpose of a warrant is for a criminal investigation where that is but one of a potential range of purposes.[35]

The appropriateness of an all-encompassing test

2.43 Irrespective of how a test is formulated, the problem remains that we do not consider it practical to have a general, all-encompassing test in section 15(1) of PACE which seeks to capture *all* warrants which relate to a criminal investigation. We agree with the CMA that applying the safeguards in sections 15 and 16 of PACE to all search warrants relating to a criminal investigation is unlikely to account for the specificities of each and every enforcement regime.

2.44 The safeguards could not be transposed wholesale as they would require significant modification. The first set of problems relate to statutory wording. For example, references to constables would have to be changed.

2.45 The second set of problems relate to the nature of the powers conferred by the safeguards. For example, sections 16(2) to (2B) of PACE authorise a person to accompany a constable and exercise the same powers as that constable only in the constable's company and under the constable's supervision. This is not a modification that would be practical across all enforcement regimes.

2.46 From a drafting perspective, both of these issues could be overcome. However, more fundamentally, following detailed discussions with the Office of the Parliamentary Counsel, we have concluded that the application of the safeguards to each possible regime would have to be considered on a case by case basis. Without doing so, it is uncertain what the consequences would be of extending sections 15 and 16 of PACE wholesale to *all* regimes under which a search warrant may be sought for the purposes of a criminal investigation. Therefore, it is better to consider each regime separately, so that the safeguards can be

---

33 Proceeds of Crime Act 2002 (Application of Police and Criminal Evidence Act 1984) Order 2015 (SI 2015 No 759) (as modified by SI 2017 No 1222), art 2.

34 *R (BBC) v Newcastle Crown Court* [2019] EWHC 2756 (Admin), [2020] 1 Cr App R 16 at [22].

35 This problem could be met by statutory drafting which provides that the safeguards apply where the purpose, or one of the purposes, for which a warrant is sought is for a criminal investigation.

tailored appropriately. Moreover, this task was undertaken in 2014 as part of the Government's powers of entry review.[36]

2.47 We also agree with the observation made by the CPS at paragraph 2.34 above that our analysis poses the question whether the safeguards should be limited to criminal investigation warrants. We recognise the force of the observation that entry on premises intrinsically engages article 8 of the ECHR and that the duty under section 6 of the Human Rights Act 1998 is not limited to criminal investigations. Accordingly, there are strong arguments for extending the safeguards to all search warrants, irrespective of the purpose for which they are obtained. As stated by Lord Woolf CJ, sections 15 and 16 of PACE help to ensure that a search complies with article 8 of the ECHR.[37] The safeguards under sections 15 and 16 of PACE are not, therefore, directed simply at protecting the right to a fair trial. For this reason, it may be unprincipled to limit the application of the safeguards to criminal investigation warrants.

2.48 Our concerns with extending sections 15 and 16 of PACE to all search warrant provisions are fourfold. First, consideration of all civil and regulatory enforcement regimes would involve straying far outside of our terms of reference to matters on which we have not received consultation responses indicating the likely ramifications. Secondly, our concerns expressed at paragraph 2.46 above apply equally here: it would be better for legislative amendment to target directly those instances where the safeguards do not, but ought to apply, rather than extending the safeguards in a criminal statute to every single regime. Thirdly, the CPS's argument assumes that the statutory safeguards and article 8 of the ECHR are coterminous in that sections 15 and 16 of PACE are only designed to safeguard article 8 rights. Fourthly, article 8 of the ECHR is of course a qualified right and so fewer safeguards may be justified under certain regimes. Therefore, each regime would have to be considered separately.

2.49 We note at paragraph 2.41 above that sections 15 and 16 of PACE have been specifically extended to search warrants sought for the purposes of a confiscation investigation, a money laundering investigation, a detained cash investigation, a detained property investigation and a frozen funds investigation.[38] Such investigations are not, strictly speaking, criminal investigations.[39] At the same time, we consider it right that sections 15 and 16 apply to such investigations. We see this as further reinforcing the argument that it is best to amend individual legislative provisions on a case-by-case basis, so as to construct the most appropriate set of bespoke procedural safeguards for that regime. This would be instead of a sweeping approach by extending sections 15 and 16 of PACE as a one-size fits all test, which may not work for some regimes.

Targeted reform of the statutory safeguards

2.50 Although we are attracted to the idea of making tailored amendments to apply appropriate safeguards to search warrant regimes across the statute book, it is difficult for us to do so given that our terms of reference only relate to criminal investigations. There is an arguable

---

36 See https://www.gov.uk/government/collections/reviews-of-all-powers-of-entry. See paragraphs 19.19 to 19.20 for further discussion of the Government's powers of entry review.

37 *Kent Pharmaceuticals v Director of the Serious Fraud Office* [2002] EWHC 3023 (QB) at [30] by Lord Woolf CJ.

38 Proceeds of Crime Act 2002 (Application of Police and Criminal Evidence Act 1984) Order 2015 (SI 2015 No 759) (as modified by SI 2017 No 1222), art 2.

39 *R v Southwark Crown Court ex parte Bowles* [1998] AC 641, 648 per Lord Hutton.

case that reform should not be artificially limited to search warrants which relate to a criminal investigation. However, due to the lack of consultation responses discussing particular regimes, we do not have a sufficient evidence base to recommend reform. Further consultation will be needed before widespread changes are proposed.

2.51 Based on our research to date and consultation responses there is, however, one particular search warrant provision that we have concluded would merit reform. As discussed at paragraph 2.12 and 2.13 above, we were concerned in the consultation paper that neither sections 15 and 16 of PACE nor comparable safeguards apply to SFO search warrants issued under section 2(4) of the CJA. However, further discussions with the SFO indicate that they consider section 15(1) does apply and proceed on this basis.

2.52 The answer turns on to whom a section 2(4) of the CJA warrant is issued: if it is to the member of the SFO who applies for the warrant, the safeguards do not apply. If it is issued to the constable who subsequently executes the warrant, by virtue of section 15(1) of PACE, the safeguards do apply. A careful reading of the final sentence of section 2(4) and (5) of the CJA reveals no clear answer.

2.53 We were informed that, in the *Kent Pharmaceuticals* litigation,[40] Lord Woolf CJ dismissed a renewed application for judicial review in respect of warrants granted under section 2(4) of the CJA where the claimant argued that there had been breaches of sections 15 and 16 of PACE. Although these arguments did not succeed, it was clear that the approach of the parties and the court was premised on the assumption that the statutory safeguards applied.

2.54 Be that as it may, we have concluded that the CJA should be amended to include statutory safeguards modelled on sections 15 and 16 of PACE for the following reasons. First, it should be made clear whether CJA warrants are subject to statutory safeguards so that investigators and those subject to a search understand the precise duties that must be fulfilled. Secondly, the safeguards provide enforceable standards of conduct, non-compliance with which may lead to the quashing of a warrant. Treating the statutory safeguards as if they apply is markedly different from the safeguards applying. Thirdly, if the safeguards are followed by the SFO as a matter of course then making this position clear in statute should not place additional burdens on the organisation. Fourthly, we make further recommendations relating to CJA search warrants in the next chapter, which would require clear safeguards similar to those currently contained in sections 15 and 16 of PACE.

2.55 For these reasons, we recommend that statutory safeguards, modelled on section 15 and 16 of PACE, are inserted into the CJA.

---

40 *Kent Pharmaceuticals v Director of the Serious Fraud Office* [2002] EWHC 3023 (QB).

Recommendation 1

2.56 We recommend that statutory safeguards, modelled on sections 15 and 16 of the Police and Criminal Evidence Act 1984, be inserted into the Criminal Justice Act 1987.

EXTENDING SECTIONS 15 AND 16 OF THE POLICE AND CRIMINAL EVIDENCE ACT 1984 TO ENTRY AND INSPECTION WARRANTS

The current law

2.57 When discussing the two components of section 15(1) of PACE at paragraph 2.10 above, we observed that, for section 15 and 16 of PACE to apply, a warrant under any enactment must be to enter and *search* premises.

2.58 Many warrants authorise the entry and inspection of premises, but not their search.[41] We refer to these as inspection warrants. Other warrants authorise only entry of premises.[42] We refer to these as entry warrants. Powers of inspection or search may or may not be engaged once an investigator is lawfully on premises, but if so, these powers are granted to the investigator by virtue of their office, rather than by the warrant. Sections 15 and 16 of PACE do not apply to inspection warrants or entry warrants on a strict reading of section 15(1) of PACE.

2.59 There is a line of authority, however, suggesting that, as a matter of sensible construction, the powers to enter and inspect premises plainly carry with them a power to search premises.[43] In *R (Helidon Vuciterni) v Brent Magistrates' Court*, Davis LJ observed that it was difficult to see how an enforcement officer could effectively exercise a power to inspect if "having lawfully obtained entry, [he was] confined to standing in the hallway and looking around by way of 'inspection' for what he can (or cannot) see".[44] He continued:

> The powers conferred necessarily connote a power to, for example, search a desk or cabinet to see if there are relevant documents which may be required to be copied, if a breach has reasonably been suspected; they connote that an enforcement officer may, for example, go into back rooms and store rooms to see if there are goods that should be seized or detained, if there is reason or cause to believe (not just suspect) a breach; and likewise may search for containers or vending machines.[45]

---

41 Theatres Act 1968, s 15; Local Government (Miscellaneous Provisions) Act 1982, ch 3, para 25; Food Safety Act 1990, s 32(2); Civil Aviation (Investigation of Air Accidents and Incidents) Regulations 2018 (SI 2018 No 321), reg 14(3); Public Regulated Service (Galileo) Regulations 2018 (SI 2018 No 230), reg 22 (not yet in force).

42 Gambling Act 2005, s 306; Local Government (Miscellaneous Provisions) Act 1982, s 12; Alternative Fuels Infrastructure Regulations 2017 (SI 2017 No 897), reg 10(1); Nuclear Security (Secretary of State Security Directions) Regulations 2018 (SI 2018 No 408), sch 1, para 2.

43 *R (Helidon Vuciterni) v Brent Magistrates' Court* [2012] EWHC 2140 (Admin), (2012) 176 JP 705; *Hargreaves v Brecknock and Radnorshire Magistrates' Court* [2015] EWHC 1803 (Admin), (2015) 179 JP 399 at [34].

44 *R (Helidon Vuciterni) v Brent Magistrates' Court* [2012] EWHC 2140 (Admin), (2012) 176 JP 705 at [48].

45 *R (Helidon Vuciterni) v Brent Magistrates' Court* [2012] EWHC 2140 (Admin), (2012) 176 JP 705.

The consultation paper

2.60 We noted in our consultation paper that section 15(1) of PACE applies only to warrants "to enter and search" premises.[46] We considered that, as a matter of principle, there was a strong case for saying that entry and inspection warrants which carry a power of search should also be subject to the same protections offered by sections 15 and 16 of PACE.

2.61 We therefore invited consultees' views[47] on whether the statutory safeguards in sections 15 and 16 of PACE should apply to entry or inspection warrants conferring or giving rise to a power of search that relate to a criminal investigation and, if so, to which provisions this should apply.

Consultation responses

2.62 Seventeen consultees answered this question: 11 agreed;[48] two disagreed;[49] and four expressed other views.[50]

2.63 Several consultees acknowledged that entry and inspection warrants often have the same purpose as police search warrants, namely to ascertain whether a criminal offence has been committed and to identify and secure relevant evidence.[51] The reasons given to justify the application of the safeguards to search warrants applied equally in respect of entry and inspection warrants.

2.64 The main discussion generated by consultees' responses related to whether, as a matter of statutory construction, the safeguards in sections 15 and 16 of PACE in their present form, which are drafted with the intention of providing protections in the context of searching premises, could be applied to entry and inspection warrants. In the view of some consultees,[52] they could not. However, several consultees considered the position to be workable, both in respect of the statutory provisions and the design of any application forms.[53]

2.65 The CPS gave the example of the requirement under section 15(2)(c) of PACE to "identify, so far as is practicable, the articles sought". Read literally, that would seem like an impossible criterion for those seeking an entry warrant to satisfy. The CPS, however, considered that the matter was already addressed by the use in PACE of the qualified "so far as is practicable". As it is not practicable to identify the articles sought when applying for an entry warrant, a person complies with the provision by marking that part of the application form as "not applicable". An alternative way of ensuring that such a requirement is met even

---

46 Law Commission, *Search Warrants: Consultation Paper* (2018) CP No 235 paras 3.30 to 3.37.

47 Consultation Question 4.

48 Professor Richard Stone; Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Birmingham Law Society; The Law Society; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service.

49 Southern Derbyshire Magistrates' Bench; Competition and Markets Authority.

50 HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Financial Conduct Authority.

51 Kent County Council Trading Standards.

52 Southern Derbyshire Magistrates' Bench; Competition and Markets Authority.

53 Council of HM Circuit Judges; Crown Prosecution Service; and Law Society.

in the context of an entry warrant was said to be to amend the provision to require the person making the application for the warrant (of whatever kind) to "… identify, so far as is practicable, the articles or persons to be sought *or otherwise the object and purpose of entry and inspection*".

2.66 Kent County Council Trading Standards helpfully confirmed that they already apply the protections in sections 15 and 16 in relation to entry warrants for which they apply. It was accepted that these require some element of modification. For example, where the application form requires specification of the articles sought, Trading Standards Officers, being unable to fulfil that obligation literally, instead set out in detail in the court application the articles that they may have the power to inspect or require production of upon lawful entry.

2.67 Two reasons for disagreeing with the extension of sections 15 and 16 of PACE to entry and inspection warrants were given by the Southern Derbyshire Magistrates' Bench, CMA and FCA. First, in their current form, the statutory safeguards could lead to confusion when magistrates are considering them as they are designed with search in mind.[54] Secondly, this would impose more burdens than are currently placed on certain law enforcement agencies.[55]

2.68 The CPS again observed that article 8 of the ECHR and section 6 of the Human Rights Act 1998 justified an extension of the safeguards to all entry and inspection warrants, irrespective of whether they related to a criminal investigation.

Analysis

2.69 We remain of the view that warrants conferring a power of entry and inspection that relate to a criminal investigation should be subject to statutory safeguards. The mere fact that the warrant does not expressly confer a power of search is not, in our view, a satisfactory reason for the safeguards in sections 15 and 16 of PACE not to apply.

2.70 Our consultation question was predicated on our proposal that sections 15 and 16 of PACE should be extended to all search warrants relating to a criminal investigation. As we have made clear at paragraphs 2.35 to 2.49 above, extending the statutory safeguards along the lines which we provisionally proposed in our consultation paper would be impractical.

2.71 As a consequence, we begin at the same starting point as we did in the section above. First, it is difficult to devise a test to capture inspection warrants that relate to a criminal investigation. We have rejected both objective and subjective tests due to their potential unintended consequences and arbitrary results. We have also rejected seeking to formulate any test which would extend sections 15 and 16 of PACE across the warrant landscape without considering in detail the effects it would have on each regime.

2.72 As discussed at paragraph 2.49, it would be preferable to consider individual legislative provisions separately to construct the most appropriate set of bespoke procedural safeguards for that inspection warrant regime. We have also concluded that sections 15 and 16 of PACE could not apply to inspection warrants in their current form and would require careful amendment. Due to the lack of consultation responses discussing these points, it is

---

54 Southern Derbyshire Magistrates' Bench.

55 Competition and Markets Authority; Financial Conduct Authority.

not possible for us to identify relevant inspection powers to which statutory safeguards should, but do not, apply, and then to construct those safeguards. We also consider that this exercise would be best conducted, if at all, in the context of a more comprehensive review of enforcement powers.

WHEN REGARD SHOULD BE HAD TO CODE B OF PACE

The current law

2.73 There are eight PACE Codes of Practice, A to H, issued by the Home Secretary under sections 66 and 67 of PACE. Code B of PACE governs the exercise of police powers to search premises; it restates many of the safeguards found in sections 15 and 16 of PACE and supplements them with further guidance. One such example is the requirement that a search be conducted at a reasonable hour unless this might frustrate the purpose of the search. Code B of PACE also adds safeguards not included in sections 15 and 16 of PACE, such as the requirement to make sure the premises is secure before leaving and to provide a notice of powers and rights to an occupier.[56] The PACE Codes are regularly updated; however, Code B of PACE was last updated in 2013.

2.74 Section 67(9) of PACE states that:

> Persons other than police officers who are charged with the duty of investigating offences or charging offenders shall in the discharge of that duty have regard to any relevant provision of a code.

2.75 A failure by a police officer or other person required to have regard to the provisions of a Code of Practice does not, of itself, render them liable to criminal or civil proceedings.[57] However, to the extent that they are relevant, the Codes of Practice are admissible in evidence in criminal or civil proceedings.[58] For example, an application to exclude allegedly unfair prosecution evidence under section 78 of PACE may be mounted on the grounds of non-compliance with a provision of a Code of Practice. A significant and substantial breach of a PACE Code will likely result in the exclusion of evidence obtained in consequence.[59]

2.76 Where Code B of PACE does not apply, the Home Office Powers of Entry Code of Practice applies, which is similar in scope and content to Code B of PACE.[60]

The consultation paper

2.77 We wrote in our consultation paper that it is unclear which provisions of Code B of PACE are "relevant" to investigators who are not constables. Stakeholders have told us that the position is uncertain. Particular agencies may follow Code B of PACE as a matter of policy, but it is said to be unclear whether there is a legal duty to do so.

---

56 We discuss the provision of a notice of powers and rights in more detail at paragraphs 7.172 to 7.179 below.

57 Police and Criminal Evidence Act 1984, s 67(10).

58 Police and Criminal Evidence Act 1984, s 67(11).

59 *R v Keenan* [1990] 2 QB 54.

60 Produced pursuant to the Protection of Freedoms Act 2012, s 47. Home Office, *Code of Practice: Powers of Entry* (December 2014). Available at https://www.gov.uk/government/publications/powers-of-entry-code-of-practice.

2.78 In addition to the uncertainty over the application of Code B of PACE to investigators other than the police, it is unclear whether Code B of PACE applies to warrants to enter or inspect, rather than search, premises.

2.79 In order to clarify the position for investigators, and to achieve parity between the statutory safeguards and Code B of PACE, we provisionally proposed[61] that anyone who applies for a search warrant that relates to a criminal investigation should be required to follow Code B of PACE.

2.80 It is important to note that this proposal in the consultation paper proceeded on the assumption that the proposed objective test for determining whether a search warrant relates to a criminal investigation would apply.

Consultation responses

2.81 Twenty-one consultees answered this question: 18 agreed;[62] one disagreed;[63] and two expressed other views.[64]

2.82 The overwhelming majority of consultees agreed that it would be desirable to clarify when investigators other than police must have regard to Code B of PACE and in relation to which provisions. The main reasons for agreeing were the need for clarity, transparency and consistency.

2.83 The CMA raised concerns that this would place additional obligations on their officers, however, this objection was in part founded on their concerns regarding an objective test for classifying when a search warrant relates to a criminal investigation. (As previously explained at paragraph 2.35 above, that aspect of the provisional proposals is not being taken forward as a recommendation). This concern about additional obligations was echoed by the FCA. They considered that changes to the Code should not inadvertently create obligations and rights for inspections undertaken within the regulatory or civil sphere.

2.84 The SFO also reported that the current requirement to "have regard" to the Code was preferable to a formal duty to "follow" it. The SFO took this view because some of the content of Code B of PACE is not relevant to non-police agencies.[65]

2.85 A number of further comments were raised regarding modification of the content of Code B of PACE. It was suggested that the bodies which would be subject to Code B of PACE could

---

61 Consultation Question 2.

62 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Insolvency Service; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; The Law Society; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service.

63 Competition and Markets Authority.

64 Serious Fraud Office; Financial Conduct Authority.

65 Serious Fraud Office.

be listed in a schedule to PACE so as to provide certainty as to who is subject to the safeguards in sections 15 and 16 of that Act.[66]

2.86 It was also pointed out that the PACE Codes of Practice are designed for those with police powers and in accordance with the police rank structure. The Codes would have to be reconsidered to take account of a multitude of investigative agencies if they are to apply to all as opposed to those other agencies simply having to "have regard" to their provisions.[67] The FCA were not clear whether we envisaged permitting agencies to define an equivalent structure independently, or intended to define this ourselves on further consultation.

2.87 It was also said that it would be useful to revise Code B of PACE to provide guidance on the approach to searches where police officers execute search warrants applied for by other agencies, particularly where representatives of such agencies take part in the search.[68] At present, the Code is silent on the subject and provides no guidance on matters such as agreeing respective responsibilities in advance or whether a person other than a police officer may act as the "officer in charge of the search".[69]

Analysis

2.88 We agree with the SFO that any new requirement imposed on non-police agencies should be for *regard* to be had to Code B of PACE, rather than that it is *followed*. This reflects the current requirement under section 67(9) of PACE, which we set out at paragraph 2.74 above.

2.89 We are therefore not seeking to change the force of the provisions of Code B of PACE, but rather to clarify the provisions of Code B to which regard should be had by non-police agencies and how.

2.90 On one view, it is not appropriate for Code B of PACE to set this out. After all, the Code is for police officers and it could be argued that it is not for a police Code of Practice to tell non-police investigators how to conduct their investigations. It is therefore for the particular agency concerned to decide to what extent regard should be had.

2.91 The point has also since been made by the College of Policing that section 66(1)(c) of PACE requires the Secretary of State to issue codes of practice in connection with searches of premises by *police officers*. For the codes of practice to address non-police powers could be *ultra vires*, meaning beyond the legal authority of the PACE Codes.

2.92 In our view, however, the burgeoning number of law enforcement agencies that can now apply for and execute warrants for the purpose of a criminal investigation justifies Code B of PACE providing more detail than it currently does. After all, the Codes of Practice are to assist in the application of the PACE provisions, which do not just apply to the police. Amendment could also be made to section 66(1)(c) of PACE to overcome the issue identified by the College of Policing.

---

66 Law Society.

67 Bar Council and the Criminal Bar Association.

68 Serious Fraud Office.

69 Serious Fraud Office.

2.93 In our view, Code B of PACE should not expand into a general code of practice on the search of premises by all investigators. We are nonetheless of the view that guidance notes attached to each code could be better utilised with non-police investigators in mind. In reaching this view, we have taken into account the fact that guidance note 3J of Code C of PACE provides guidance to "non-police investigators" in respect of informing suspects of their right to legal advice. Further, as section 67(9) of PACE *requires* persons other than police officers to have regard to any relevant provision of a code, it is, in our view, desirable for Code B to provide guidance for non-police investigators.

2.94 In our view, any person other than a police officer applying for a warrant which confers a power of entry where one of the purposes of the investigation is to investigate the commission of a criminal offence should have regard to Code B of PACE. We do not agree with the suggestion made by the Law Society that the bodies which must have regard to Code B should be listed in a schedule to PACE 1984. In our view, the focus should be on the type of investigation rather than the agency involved. Such a list might also require frequent updating to capture new agencies, albeit we accept that this would not be a significant issue; if a new agency is created by statute it would just require a consequential amendment to the list.

2.95 Nor do we consider that regard to the Code should be limited to search warrants as, in our view, Code B does currently apply to police entry and inspection warrants given the qualifier used in paragraph 2.5 of Code B, which provides:

> This Code does not apply to the exercise of a statutory power to enter premises or to inspect goods, equipment or procedures *if the exercise of that power is not dependent on* the existence of grounds for suspecting that an offence may have been committed and the person exercising the power has no reasonable grounds for such suspicion (emphasis added).

2.96 As to which provisions the investigator should have regard to, we consider it unnecessary for us here to descend into a detailed discussion. The precise provisions on which guidance should be provided will require consideration and consultation by the PACE Strategy Board. We do, however, observe that the answer for each agency may vary depending on their institutional structure and capabilities. A general guidance note may be useful, pointing out that other agencies are required to have regard to the Code.

2.97 In the light of the concerns raised by the SFO and FCA, we also see merit in guidance being introduced into Code B of PACE on the approach to searches where police officers execute search warrants applied for by other agencies, particularly where representatives of those agencies take part in the search. At present, the Code is silent on the subject and provides no guidance on matters such as agreeing respective responsibilities in advance or whether a person other than a police officer may act as the "officer in charge of the search".

Recommendation 2

2.98 We recommend that the PACE Strategy Board consider amending Code B of the Police and Criminal Evidence Act 1984 to provide guidance for non-police investigators in complying with the provisions of the Code.

WHEN AN ENTRY ON OR SEARCH OF PREMISES UNDER A WARRANT IS RENDERED UNLAWFUL

2.99 The remainder of the consultation questions in Chapter 3 of the consultation paper focused on clarifying the latter half of section 15(1) which provides that:

> … an entry on or search of premises under a warrant is unlawful unless it complies with this section and section 16 below.

2.100 It has been said that this provision is not entirely easy to understand.[70] There has, at times, been conflicting case law on its interpretation. Accordingly, we identified three aspects of section 15(1) of PACE that lack clarity:

(1) the conduct that must comply with section 15(1) of PACE;

(2) the elements of the search which are rendered unlawful as a result of non-compliance with section 15(1) of PACE; and

(3) the breaches of sections 15 and 16 of PACE which make the entry, or search, unlawful.

Conduct which must comply with the statutory safeguards

The current law

2.101 Section 15(1) of PACE states that "an entry on or search of premises under a warrant is unlawful unless *it* complies with this section and section 16 below". There is an ambiguity in the word "it". Does "it" refer to the warrant, to the entry and search, or to both?

2.102 The seemingly favoured view as expressed by the Divisional Court is that "it" refers to both the warrant, and the entry and search:

> We read "it" as referring to the composite process of entering and searching under a warrant so that in order for that process to be lawful the application for and issue of the warrant has to have been in compliance with section 15 and its execution has to comply with section 16. This does no violence to the language of the subsection and gives effect to what seems to us to be its obvious legislative purpose.[71]

2.103 This reading accords with the Police and Criminal Evidence (Northern Ireland) Order 1989, which provides that the warrant, entry and search must comply with the requirements of the

---

70 *R v Central Criminal Court ex parte AJD Holdings* [1992] Criminal Law Review 669.

71 *R v Chief Constable of Lancashire ex parte Parker and another* [1993] QB 577, 584. See for a discussion R Stone, *The Law of Entry, Search, and Seizure* (5th ed 2013) para 4.19.

articles.[72] This view also accords with the modifications to section 15(1) in respect of search warrants under the Proceeds of Crime Act 2002,[73] which states that "an entry on or search of premises under such a warrant is unlawful unless the warrant complies with this section and is executed in accordance with section 16."

2.104 Case law suggests that section 15(1) of PACE does not apply to events that occur after the entry and search have been completed; therefore, entry and search does not include post-search activity (section 16(9) to (12) of PACE).[74] Nor, it seems, does section 15(1) of PACE apply to seizure: section 16(8) of PACE is only directed at excessive *searching* and not seizure.[75]

The consultation paper

2.105 Whilst a workable interpretation has been reached by the Divisional Court, as to what "it" refers to (the warrant, entry and search),[76] we expressed the view in our consultation paper that the section should be clarified.

2.106 In light of the case law, we provisionally proposed[77] that section 15(1) of PACE should be amended to clarify that entry, search and seizure are unlawful unless *both the warrant, and the entry and search* comply with sections 15 and 16 of PACE.

Consultation responses

2.107 Sixteen consultees answered this question: 15 agreed;[78] none disagreed; and one expressed another view.[79]

2.108 This consultation question was designed to gather views on whether section 15 of PACE should be amended to clarify the conduct that must comply with section 15(1) of PACE. However, some stakeholders discussed instead the broader question of the appropriate threshold to be reached before a finding of unlawfulness is made. These comments fell more appropriately within consultation question 7 and are therefore discussed below.

2.109 Insofar as the provisional proposal was concerned, the overwhelming majority of consultees agreed.

---

72 Police and Criminal Evidence (Northern Ireland) Order 1989 (SI 1989 No 1341), Art 17(1).

73 Proceeds of Crime Act 2002 (Application of Police and Criminal Evidence Act 1984) Order 2015 (SI 2015 No 759) (as modified by SI 2017 No 1222), art 2(2).

74 *R (Hicks) v Commissioner of the Metropolis* [2012] EWHC 1947 (Admin), [2012] ACD 102 at [247] per Richards LJ; *R (Haly) v Chief Constable of West Midlands Police* [2016] EWHC 2932 (Admin) at [17].

75 *R v Chesterfield Justices, ex parte Bramley* [2000] QB 576, 588 to 589.

76 *R v Chief Constable of Lancashire ex parte Parker and another* [1993] QB 577.

77 Consultation Question 6.

78 One member of the public; Professor Richard Stone; Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; The Law Society; Southern Derbyshire Magistrates' Bench; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; Bar Council and the Criminal Bar Association; Serious Fraud Office.

79 National Crime Agency.

Analysis

2.110 As above, we remain of the view that section 15(1) of PACE would benefit from clarification in this regard and have received no responses which cause us to change our provisional view.

Recommendation 3

2.111 We recommend that section 15(1) of the Police and Criminal Evidence Act 1984 be amended to clarify that entry, search and seizure are unlawful unless *the warrant, entry and search* comply with sections 15 and 16 of the Police and Criminal Evidence Act 1984.

Elements of the search rendered unlawful following breach

The current law

2.112 Section 15(1) of PACE states that failure to comply with the provisions in sections 15 and 16 of PACE will render any entry or search unlawful. It is important to note, though, that non-compliance with sections 15 and 16 does not render the warrant itself unlawful. Therefore, it does not follow that a warrant will be quashed where there has been a breach of section 15 or 16 of PACE: the quashing of a warrant is a discretionary form of relief on judicial review.

2.113 Although not in the wording of the statute, the Divisional Court has on a number of occasions expressed the view that non-compliance with section 15(1) also renders *seizure* unlawful.[80] Seizure may occur under the authority of the warrant itself,[81] or under other statutory powers that require a constable to be lawfully on premises.[82]

The consultation paper

2.114 It was suggested by one stakeholder during our preliminary discussions that section 15(1) should be clarified to state that, unless the safeguards are complied with, any seizure is also unlawful. We agreed and therefore provisionally proposed[83] that section 15(1) of the Police and Criminal Evidence Act 1984 should be amended to clarify that an entry on, search of, or seizure of materials from, any premises under a warrant is unlawful unless the warrant, entry, search *and seizure* complies with sections 15 and 16 of the Police and Criminal Evidence Act 1984.

---

80 *R (Bhatti) v Croydon Magistrates' Court* [2010] EWHC 522 (Admin), [2011] 1 WLR 948 at [31] by Elias LJ. See also *Lees v Solihull Magistrates' Court* [2013] EWHC 3779 (Admin), [2014] Lloyd's Rep FC 23 at [39]; *R v Chief Constable of the Warwickshire Constabulary, ex parte Fitzpatrick* [1999] 1 WLR 564, 569A; *R v Chief Constable of Lancashire ex parte Parker and another* [1993] QB 577, 587C.

81 Police and Criminal Evidence Act 1984, s 8(2).

82 Police and Criminal Evidence Act 1984, s 19.

83 Consultation Question 5.

Consultation responses

2.115 Eighteen consultees answered this question: 15 agreed;[84] one disagreed;[85] and two expressed other views.[86]

2.116 As with the provisional proposal above, our focus here was a narrow one: clarifying the elements of the search rendered unlawful following a breach of the statutory safeguards. Our provisional proposal was in effect to codify the decisions of the Divisional Court holding that any subsequent seizure would also be rendered unlawful by breach of the statutory safeguards. Consultation responses regarding the appropriate threshold to be reached before a breach occurs are discussed in the context of Consultation Question 7 below.

2.117 The majority of consultees agreed with our provisional proposal and no concerns were raised that caused us to doubt its utility. The Magistrates Association viewed the provisional proposal as sensible, but considered that thought should be given to its operational impacts. Dijen Basu QC agreed with the provisional proposal, with the proviso that it should be made clear for the avoidance of doubt, by way of an express saving, that the sections have no effect on the lawfulness of an otherwise lawful entry, search or seizure in reliance on other powers (for example sections 17, 18 and 32 of PACE).

Analysis

2.118 As stated above, the majority of consultees agreed with this provisional proposal. We have received no responses which cause us to change our view. Further, we remain of the view that clarifying section 15(1) would be beneficial.

2.119 Consideration of the operational impact of our recommendations is crucial in relation to all aspects of this report. However, as the proposed amendment to section 15(1) would amount only to a clarification of the existing law rather than a substantive change, we consider that its operational impact will be limited to helping to ensure that the existing law is properly understood.

2.120 We agree that a finding of unlawfulness in relation to section 15(1) of PACE has no direct bearing on the lawfulness of other search powers, the legality of which would need to be specifically challenged. We do not consider that statutory amendment is required to make this clear.

---

84 One member of the public; Professor Richard Stone; Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; The Law Society; Southern Derbyshire Magistrates' Bench; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; Bar Council and the Criminal Bar Association; Serious Fraud Office.

85 Insolvency Service.

86 National Crime Agency; Competition and Markets Authority.

Recommendation 4

2.121 We recommend that section 15(1) of the Police and Criminal Evidence Act 1984 be amended to clarify that an entry on, search of, or *seizure* of materials from, any premises under a warrant is unlawful unless *the warrant, entry and search* comply with sections 15 and 16 of the Police and Criminal Evidence Act 1984.

Breaches resulting in unlawfulness

The current law

2.122 Although section 15(1) of PACE provides that "an entry or search of premises under a warrant is unlawful unless it complies with this section and section 16", there is no consistent approach regarding the circumstances in which a failure to comply with those sections renders the entry, search and any subsequent seizure unlawful. As we have indicated at paragraph 2.104, case law suggests that section 15(1) of PACE does not apply to events that occur after the entry and search have been completed; therefore, entry and search does not include post-search activity (section 16(9) to (12) of PACE).[87]

2.123 The courts have sometimes held that the wording of section 15(1) is unequivocal[88] and that the requirements of sections 15 and 16 of PACE should be applied stringently.[89] In other circumstances, the courts have taken a more pragmatic approach, observing that the statutory safeguards must be applied in a manner which takes careful account of the practical realities of running complex criminal investigations.[90] It has also been said that the court may readily find reasons for overlooking trivial or unimportant irregularities.[91] A breach may therefore be regarded as *de minimis* and so not lead to a finding of unlawfulness.[92]

2.124 Even where the courts find a breach of section 15(1) of PACE, relief is discretionary. For example, in *Hicks*, the Divisional Court held that:

> In the present case we are not satisfied that the breach of s.16(10) has caused the claimants any real injustice, let alone that it should lead to the invalidation of what were, in our judgment, otherwise lawful searches. We would therefore decline to grant the claimants any relief in respect of this issue even if the point taken is technically well founded.[93]

2.125 By way of another example, in *Glenn & Co (Essex) Ltd*, the Divisional Court, following a finding of a breach of section 16(5) of PACE, observed that the impracticality of handing

---

87 *R v Chesterfield Justices, ex parte Bramley* [2000] QB 576, 588 to 589.

88 *R (Bhatti) v Croydon Magistrates' Court* [2010] EWHC 522 (Admin), [2011] 1 WLR 948 at [31] by Elias LJ.

89 *R v Central Criminal Court ex parte AJD Holdings* [1992] Criminal Law Review 669.

90 *R (Superior Import / Export Ltd) v Revenue and Customs Commissioners* [2017] EWHC 3172 (Admin), [2018] Lloyd's Rep FC 115 at [85]. See also *Intertrade Wholesale Ltd v Revenue and Customs Commissioners* [2018] EWHC 3476 (QB).

91 *Krohn v DPP* [1997] EWHC 286 (Admin) at [20] and [25] per Brooke LJ. See also *Intertrade Wholesale Ltd v Revenue and Customs Commissioners* [2018] EWHC 3476 (QB) at [39]

92 *R v Chief Constable of the Warwickshire Constabulary, ex parte Fitzpatrick* [1999] 1 WLR 564, 575G.

93 *R (Hicks) v Commissioner of the Metropolis* [2012] EWHC 1947 (Admin), [2012] ACD 102 at [247] by Richards LJ.

over a copy of the warrant should not inevitably lead to the grant of what is discretionary relief.[94] Accordingly, it was not ordered that any material obtained in the search should be returned.

2.126 In *R (Goode)*, Lord Justice Pitchford wrote:

> In my judgment the only ground of challenge to these warrants which has legal merit is the omission of DI Kennedy's name as the applicant on the face of the warrants. It is my view that the breach of section 15(6)(a) was so technical that in the circumstances of the present case there is no prospect that the court would use its discretionary powers either to quash the warrants or to make a declaration of invalidity.[95]

The consultation paper

2.127 Given these inconsistent approaches, we considered that clarity should be brought to the following question: when does non-compliance with the statutory provisions render the entry, search and seizure unlawful? Again, it is important to note that non-compliance with sections 15 and 16 does not render the warrant itself unlawful but only the subsequent entry, search and seizure under the warrant.[96]

2.128 For this reason, we invited consultees' views on whether every breach of section 15 or 16 of PACE ought to have the effect that any search and seizure of material is unlawful. If not, which breaches should and should not have this effect? In particular, we were interested in consultees' views on:

(1) section 15(6) of PACE (the requirement of specificity); and

(2) section 16(9) to (12) of PACE (post-search requirements to return the warrant to the court once executed).

We also invited consultees' views on whether it would be desirable to confirm the above position in statute.

Consultation responses

2.129 Twenty-one consultees[97] answered this question. Responses to this question raised two distinct issues: first, when should non-compliance with the statutory provisions render the entry, search and seizure unlawful; and, secondly, what should be the consequences of a finding of unlawfulness. Each is addressed in turn.

---

94 *R (Glenn & Co (Essex) Ltd) v HMRC* [2011] EWHC 2998 (Admin), [2012] 1 Cr App R 22 at [77].

95 *R (Goode) v Nottingham Crown Court* [2013] EWHC 1726 (Admin), [2014] ACD 6 at [48].

96 *Lees v Solihull Magistrates' Court* [2013] EWHC 3779 (Admin), [2014] Lloyd's Rep FC 23 at [43].

97 One member of the public; Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Insolvency Service; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; The Law Society; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Serious Fraud Office; Competition and Markets Authority; Financial Conduct Authority.

Whether all forms of non-compliance with sections 15 or 16 PACE 1984 ought to result in unlawfulness

2.130 Professor Richard Stone considered that there should be a strong exclusionary rule whereby all non-compliant searches should be rendered unlawful. However, the majority of other consultees argued that there is a variation, on the face of it, in the importance of different safeguards and the likely impact of non-compliance. The prevailing view, therefore, was that the question of non-compliance was highly fact-sensitive and that there should be wide judicial discretion for the following reasons:

(1) each case needs to be determined on its facts;[98]

(2) undue rigidity could encourage technical and unmeritorious challenges which would unduly limit the ability of the state to combat serious crime;[99]

(3) it would be undesirable to limit by statute those breaches that would lead to this result, or to list extensively all the types of breach that will lead to such a determination;[100]

(4) it is not possible to anticipate every situation in which a breach might occur, nor should the statute be unnecessarily prescriptive;[101] and

(5) an amendment to the stringency of the requirement to comply with the statutory safeguards may lead to a proliferation of applications for judicial review of search warrants in relation to what may, in some cases, be fairly minor breaches.[102]

2.131 The following examples of the factors that should be taken into account for the purposes of determining whether non-compliance should render the entry, search or subsequent seizure unlawful were suggested:

(1) whether breaches were minor;

(2) whether the breaches were of form rather than substance; and

(3) following determination of there being a substantive breach, whether it would be just and equitable to find the non-compliance to be unlawful.

2.132 There were opposing views expressed as to how judicial discretion should operate:

(1) one consultee considered that the legislation should be amended to reflect the discretion of the court to deal with non-compliance;[103] and

(2) another considered that judicial discretion was already afforded under the current law.[104]

---

98 Law Society.

99 Bar Council and the Criminal Bar Association.

100 Law Society.

101 Council of Her Majesty's Circuit Judges; Southern Derbyshire Magistrates' Bench; Justices' Clerks' Society.

102 HM Council of District Judges (Magistrates' Court).

103 Insolvency Service.

Consequence of a finding of unlawfulness

2.133 Although we did not directly consult on this point, a number of consultees commented upon the consequence of a finding of unlawfulness.

2.134 Professor Richard Stone, again in favour of a strong exclusionary rule, stated that he would support the view that, where a non-compliant search was unlawful, any evidence obtained as a result of the search should be rendered inadmissible.

2.135 The majority of law enforcement agencies considered that there should be a discretion as to the result of a finding of unlawfulness. They did not consider that every breach should result in material being returned. Further, they argued that the trial process is equipped through the power in section 78 of PACE to exclude evidence obtained in breach of the provisions.

Analysis

Whether all forms of non-compliance with the safeguards ought to result in unlawfulness

2.136 In the light of the views expressed by consultees, we agree that each case must turn on its own facts and therefore a wide margin of judicial discretion should be afforded.

2.137 To take an example: the requirement to identify the "articles" sought under section 15(6)(b) of PACE could be breached. A lack of specificity must be viewed in light of the nature of the investigation. Determining whether the breach renders the entry, search and seizure unlawful will be fact dependent. Should the warrant have specified a "black iPhone X 512GB" rather than a "phone"? This will depend on, amongst other factors, the information known and the type of investigation: a complex, urgent investigation may justify a search warrant being couched in broader terms. We consider that this wide margin of judicial discretion is both essential and adequately catered for under the current law.

2.138 The statutory safeguards provide an important constitutional check. At the same time, unmeritorious technical challenges should be discouraged and the safeguards applied pragmatically. This balancing exercise can be seen in operation within the case law. For this reason, we do not consider that legislative amendment is necessary.

Consequence of a finding of unlawfulness

2.139 We understand that the main concern of law enforcement is to avoid the introduction of a rule whereby a finding of unlawfulness automatically triggers the return of material, which may result in the collapse of complex criminal investigations. We do not consider that every breach should result in material being returned, a view reflected in current case law. We endorse the pragmatic view taken by the courts to technical challenges of breaches of sections 15 and 16.

2.140 We agree that, from an evidential standpoint, section 78 of PACE provides an important avenue through which to assess whether material ought to be excluded. Section 78 provides the court with a discretion to refuse to allow prosecution evidence if, having regard to all the circumstances, including those in which the evidence was obtained, its admission would have an adverse effect on the fairness of the proceedings. Lord Justice Leveson described section 78 of PACE as an ample control mechanism in the context of material seized

---

[104] Justices' Clerks' Society.

pursuant to unlawful warrants.[105] At the same time, we agree that there are cases in which the return of the material seized is an appropriate remedy. Again, this an area in which we consider judicial discretion has operated successfully and ought to be retained.

[105] *R (Cummins) v Manchester Crown Court* [2010] EWHC 2111 (Admin), [2010] Lloyd's Rep FC 551 at [13].

Chapter 3: Agencies empowered to apply for and execute search warrants

INTRODUCTION

3.1 In this chapter, we consider whether some agencies which are not at present entitled independently to apply for and execute search warrants should be given the power to do so. We use the term "execute" to refer to both acts of effecting lawful entry and exercising powers including search and seizure. We consider the following matters:

(1) expanding the pool of agencies entitled to apply for a search warrant;

(2) expanding the pool of agencies authorised to execute a search warrant; and

(3) amending the requirement under some regimes that certain agencies can only exercise powers of search and seizure on premises if they are in the company, and under the supervision of, a constable.

3.2 In summary, we recommend that the NHS Counter Fraud Authority ("NHSCFA"), the NHS Counter Fraud Service Wales ("NHSCFSW") and the Insolvency Service each be empowered to apply for search warrants where particular conditions are met. We recommend that a search warrant applied for by the NHSCFA or NHSCFSW permit either that agency or a constable to execute the warrant, and that neither agency be required to exercise powers of search and seizure in the presence of a constable. We recommend that the Insolvency Service be empowered to execute its own search warrants, and that sections 19 to 22 of PACE be extended to the Insolvency Service, with necessary modifications. We conclude that providing these powers and duties would address gaps in these agencies' powers of investigation, improve efficiency by making them less reliant on the police, and rationalise search warrants legislation.

3.3 We also recommend dispensing with the current requirement under the Criminal Justice Act 1987 ("CJA") and the Financial Services and Markets Act 2000 ("FSMA") that a constable must be present in order for accompanying agencies to exercise their powers of search and seizure. This would render the law more efficient and cost effective because a constable who is no longer needed during the execution of a warrant once lawful entry has been facilitated could leave the premises.

AGENCIES ENTITLED TO APPLY FOR A SEARCH WARRANT

The current law

3.4 Under the current law, most search warrants which relate to a criminal investigation can only be applied for by a constable,[1] which includes an officer of the National Crime Agency

[1] For example, Anti-terrorism, Crime and Security Act 2001, s 66; Channel Tunnel (Security) Order 1994 (SI 1994 No 570), art 14(5); Control of Trade in Endangered Species (Enforcement) Regulations 1997 (SI 1997 No 1372), reg 9(1); Copyright Act 1956, s 21A; Copyright (Computer Software) Amendment Act 1985, s 3; Copyright, Patents and Designs Act 1988, ss 109, 200 and 297B; Crime (International Co-operation) Act 2003, s 17; Criminal Justice Act 1988, s 142; Customs and Excise Management Act 1979, s 161A(3); Dogs (Protection of Livestock) Act 1953, s 2A;

("NCA").[2] The power to apply for a search warrant under PACE has been extended by statute to other investigators, including Welsh Revenue Authority officers;[3] officers of HM Revenue and Customs ("HMRC");[4] immigration officers and designated customs officials;[5] officers of the department for Business, Energy and Industrial Strategy;[6] and labour abuse prevention officers.[7]

3.5 Other provisions allow an application to be made by either a police constable or some other specified category of investigator.[8] A large number of agencies have the power to apply for a search warrant, or authorise an individual to apply for a warrant on their behalf. These include the Charity Commission;[9] the Immigration Services Commissioner;[10] the Information Commissioner;[11] an immigration officer;[12] the Bank of England;[13] the Serious Fraud Office ("SFO");[14] the Financial Conduct Authority; ("FCA")[15] the Competition and Markets Authority ("CMA");[16] the Prudential Regulation Authority;[17] an officer of HMRC;[18] approved mental

---

Drug Trafficking Act 1994, s 56; Extradition Act 2003, s 156; International Criminal Court Act 2001, s 37 and sch 5; Knives Act 1997, s 5; Northern Ireland (Location of Victims' Remains) Act 1999, s 6; Protection from Harassment Act 1997, s 2B; Public Order Act 1936, s 2(5); Public Order Act 1986, ss 24 and 29H; Sexual Offences Act 2003, s 96B; Terrorism Act 2000, s 42 and sch 5, para 11; Terrorism Prevention and Investigation Measures Act 2011, sch 5, para 8; Trade Marks Act 1994, s 92A.

2 Crime and Courts Act 2013, s 10.

3 Welsh Revenue Authority (Powers to Investigate Criminal Offences) Regulations 2018 (SI 2018 No 400), sch 1, para 1.

4 Police and Criminal Evidence Act 1984 (Application to Revenue and Customs) Order 2015 (SI 2015 No 1783), sch 1.

5 Police and Criminal Evidence Act 1984 (Application to immigration officers and designated customs officials in England and Wales) Order 2013 (SI 2013 No 1542), schs 1 and 2.

6 Police and Criminal Evidence Act 1984 (Department of Trade and Industry Investigations) Order 2002 (SI 2002 No 2326), art 3.

7 Police and Criminal Evidence Act 1984 (Application to Labour Abuse Prevention Officers) Regulations 2017 (SI 2017 No 520), reg 3.

8 Animal Welfare Act 2006, ss 19(4) and 23(1): either a constable or an inspector as appointed by the appropriate national authority or a local authority under the Animal Welfare Act 2006, s 51; Wireless Telegraphy Act 2006, s 97(1): either a constable or person authorised by the Office of Communications ("Ofcom") or the Secretary of State.

9 Charities Act 2011, s 48: a member of staff of the Charity Commission.

10 Immigration and Asylum Act 1999, s 92A: the Immigration Services Commissioner (this includes a reference to a member of staff authorised in writing by the Immigration Services Commissioner under the Immigration and Asylum Act 1999, s 92A(7)).

11 Data Protection Act 2018, sch 15, para 1(1).

12 Immigration Act 1971, ss 28FB, 28B and 28D.

13 Banking Act 2009, s 194: an inspector (as appointed by the Bank of England under the Banking Act 2009, ss 83ZC and 83ZD).

14 Criminal Justice Act 1987, s 2(4).

15 Financial Services and Markets Act 2000, ss 122D and 131FB: by, or on behalf of, the Financial Conduct Authority.

16 Competition Act 1998, ss 28, 28A, 62, 62A, 63 65G and 65H and Enterprise Act 2002, s 194.

17 Friendly Societies Act 1992, s 62A: by, or on behalf of, the Financial Conduct Authority or the Prudential Regulation Authority.

18 Customs and Excise Management Act 1979, s 161A(1).

health professionals;[19] the Gas and Electricity Markets authority;[20] the European Securities and Markets Authority;[21] and the Office of Communications (colloquially known as "Ofcom").[22]

3.6 Private companies may enlist the help of the police to obtain a search warrant on their behalf. This may be for the purpose of advancing a private prosecution.[23] For example, in *R v Zinga*,[24] the Metropolitan Police Service assisted Virgin Media Ltd by obtaining search warrants for the purpose of a private prosecution against an individual for conspiracy to defraud.

The consultation paper

3.7 In our consultation paper, we invited consultees' views[25] on whether the power to apply for a search warrant should be extended to Government agencies which have a duty to investigate offences, but which currently lack search warrant powers. We also invited consultees' views on:

(1) which agencies ought to be able to apply for a search warrant; and

(2) the types of investigations for which those agencies ought to be able to apply for a search warrant.

Consultation responses

3.8 Nineteen consultees answered this question: 10 agreed that the power to apply for a search warrant should be extended;[26] two disagreed;[27] and eight expressed other views.[28]

3.9 Several consultees agreed that the power to apply for a search warrant should be extended to either all or named Government agencies, provided that investigators have direct

---

19 Mental Health Act 1983, s 135: an approved mental health professional (as approved by a local social services authority (as defined in s 145(1)) under the Mental Health Act 1983, s 114).

20 Electricity and Gas (Market Integrity and Transparency) (Enforcement etc) Regulations 2013 (SI 2013 No 1389), reg 16: a person authorised by the Gas and Electricity Markets Authority.

21 Credit Rating Agencies Regulations 2010, reg 33(5): an official of, or person authorised by, the European Securities and Markets Authority.

22 Wireless Telegraphy Act 2006, s 97(1): either a constable or person authorised by Ofcom or the Secretary of State.

23 Prosecution of Offences Act 1985, s 6(1). The right to bring a private prosecution is long established: its history is summarised in the judgments of Lord Wilson and Lord Mance in *R (Gujra) v Crown Prosecution Service* [2012] UKSC 52, [2013] 1 AC 484.

24 *R v Zinga* [2014] EWCA Crim 52, [2014] 1 WLR 2228.

25 Consultation Question 8.

26 NHS Counter Fraud Authority; Professor Richard Stone; Council of Her Majesty's Circuit Judges; Insolvency Service; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; Justices' Clerks' Society; Magistrates Association; Bar Council and the Criminal Bar Association.

27 One member of the public; Kent County Council Trading Standards.

28 Department for Work and Pensions; HM Council of District Judges (Magistrates' Court); Kent County Council Trading Standards; The Law Society; Dijen Basu QC; National Crime Agency; Metropolitan Police Service; Financial Conduct Authority.

knowledge of the investigation.[29] It was stressed that agencies should only be able to make an application in relation to those offences which they are responsible for investigating.[30] However, it was observed that the term "Government agency" may be unduly restrictive as it does not catch bodies corporate such as the FCA.[31]

3.10 Kent County Council Trading Standards did not see the benefit of expanding the pool of agencies capable of applying for a search warrant if those bodies could not then execute the warrant. They considered that the investigating agency should be able to both apply for and execute the warrant.

3.11 Some consultees suggested that we should be cautious about extending the pool of agencies entitled to apply for a warrant: any extension of powers would require extensive additional training for officers. It was said that those agencies newly granted the power to apply for warrants would need to match the level of expertise, experience and training of the police.[32]

3.12 In the consultation paper, we noted that the Department for Work and Pensions ("DWP") is an example of a Government department which has investigators and a prosecutorial remit but has no power to apply for search warrants. As a result, if they want to apply for and execute a warrant they must obtain the assistance of the police.

3.13 Despite this, in their consultation response, DWP indicated that they did not want the power to apply for a search warrant in their own right for two reasons. First, from an investigations perspective, they were content with their existing practice of asking the police to apply for a warrant under PACE. Secondly, DWP believe that police officers have the necessary skills and experience to respond to questions posed by the magistrate issuing the warrant.

3.14 However, in its response, the NHSCFA made a compelling case for it to have the power to apply for a search warrant. The Insolvency Service also made a compelling case for its existing powers to apply for search warrants to be extended.

The NHS Counter Fraud Authority

3.15 The NHSCFA investigates high value economic crime within the NHS.[33] It exercises the power of the Secretary of State under section 197 of the National Health Service Act 2006 (NHS Act 2006) to serve a notice requiring the production of documents.[34] As there is no express limitation on the face of the power, the NHSCFA can require the production of confidential medical records, which would constitute "excluded material"[35] under section 11 of PACE and therefore could only be the subject of a production order or search warrant

---

29 Richard Stone; The Council of Her Majesty's Circuit Judges; Birmingham Law Society.

30 Birmingham Law Society; Justices' Clerks' Society; Bar Council and the Criminal Bar Association.

31 Bar Council and the Criminal Bar Association; Financial Conduct Authority.

32 HM Council of District Judges (Magistrates' Court); Law Society.

33 See the NHS Counter Fraud Authority (Establishment, Constitution, and Staff and Other Transfer Provisions) Order 2017 (SI 2017 No 958).

34 See the NHS Counter Fraud Authority (Establishment, Constitution, and Staff and Other Transfer Provisions) Order 2017 (SI 2017 No 958), sch 1, para 2 (the *vires* for which is NHS Act 2006, s 7(1)).

35 Broadly speaking, excluded material, as defined in the Police and Criminal Evidence Act 1984, s 11, covers confidential personal records, human tissue or tissue fluid and confidential journalistic material. We discuss the treatment of special procedure material in Chapter 12.

under PACE if stringent conditions were met.[36] While the NHSCFA can require the production of documents, it has no power to apply for a search warrant or to seize material.

3.16 The NHS Counter Fraud Authority suggested that one reason why it was not granted these powers may have been the assumption that the professionals investigated, who are principally medical consultants and dentists, would cooperate with investigations. The Authority informed us that this is not always the case.

3.17 Putting the power of the NHSCFA to secure and preserve evidence on a more effective and robust footing was therefore said to be desirable. The Authority proposed that:

(1) they should have the authority to apply for their own search warrants;

(2) the NHS Act 2006 Codes of Practice[37] should apply to search warrant applications to ensure the security and confidentiality of any materials seized; and

(3) there should be appropriate scrutiny within the application process to ensure the rights of all those involved are protected in a proportionate and fair way, taking into account the role of the NHSCFA in protecting the resources of the NHS and the public purse.

3.18 The Authority argued that these reforms would make it simpler for them to access evidence containing special procedure material[38] and excluded material as part of their criminal investigations.

3.19 The Codes of Practice which accompany the NHS Act 2006 aim to ensure that when personal records are handed over to the NHSCFA there is a system in place to keep them secure and confidential.[39] The NHS Act 2006 also makes it an offence to disclose information which was obtained pursuant to a production notice, except under the circumstances specified in the Act.[40]

3.20 Dijen Basu QC agreed that the NHSCFA should have the power to apply for a search warrant. At present, the Authority can ask the police to apply for a warrant under section 8 of PACE on their behalf. However, the Authority will often be seeking a search warrant to obtain evidence which will include medical or dental records. These constitute "excluded material" under section 11 of PACE and cannot be the subject of a section 8 warrant.[41] As a result, a search warrant cannot be obtained to search for medical records which provide

---

36 We discuss the availability under the Police and Criminal Evidence Act 1984 of confidential personal records, which includes medical records, at paras 12.10 to 12.16 below.

37 Department of Health and Social Care, *Accessing and using documents to counter fraud in the NHS: Code of Practice* (2018).

38 Broadly speaking, special procedure material, as defined in the Police and Criminal Evidence Act 1984, s 14, includes non-confidential journalistic material and confidential information created or held for business or official purposes, other than legally privileged or excluded material. We discuss the treatment of special procedure material in Chapter 13.

39 Department of Health and Social Care, *Accessing and using documents to counter fraud in the NHS: Code of Practice* (2018) para 6.1.

40 NHS Act 2006, s 205(1).

41 Excluded material may be the subject of a search warrant under the Police and Criminal Evidence Act 1984, sch 1, however, for reasons that we will come on to explain at para 3.33 below, this option will not be possible.

evidence of fraud by evidencing that NHS treatment was unnecessary, not provided or that no materials were used.

3.21 Accordingly, when the Authority is faced with an uncooperative suspect or occupier who is unlikely to comply with a production notice, they may feel that the only option is to seek to persuade the police to arrest the person on suspicion of fraud. Once arrested, a search for relevant evidence could be carried out pursuant to sections 18 or 32 of PACE, because these provisions contain no exemptions in relation to excluded or special procedure material.[42]

The Insolvency Service

3.22 The Insolvency Service welcomed our proposal to broaden the power to apply for a search warrant. They explained that, while they have had some powers under PACE extended to their officers,[43] those powers are currently limited to applying for special procedure material under schedule 1 to PACE.[44] In most cases, the material they intend to search for is a mixture of special procedure material and ordinary material which can only be sought under a section 8 of PACE warrant. Because the Insolvency Service do not have the power to apply for a section 8 of PACE warrant, they stated that they must ask the police to make an application on their behalf. It was said that this creates challenges for the Insolvency Service, as they regard themselves as likely having a far more detailed understanding of the case than the police officer applying for the warrant.

3.23 Additionally, because the Insolvency Service investigators are not the applicants, they lack standing and so cannot make submissions to the court or answer any questions. The Insolvency Service argued that permitting their investigators to make applications under both schedule 1 to and section 8 of PACE would remove the burden from the police and put Insolvency Service investigators in the best position to assist the court. Were a person affected by a warrant later to challenge the warrant, the Insolvency Service said that they would be able to deal with the issues directly.

Analysis

3.24 In the light of consultees' responses, we consider that some increase in the pool of agencies entitled to apply for a search warrant will make the current search warrants regime more efficient. Increasing the number of investigative agencies who can apply for a warrant would reduce the burden placed on the police and increase the likelihood that the issuing authority will be provided with all of the necessary information and have their questions answered adequately.

3.25 We disagree with Kent County Council Trading Standards' observation that any investigating agency who has the power to apply for a search warrant should also have the power to execute it. Those agencies who apply for warrants must have the knowledge to ensure that

---

42 We discuss at para 3.31 below the reasons why relying on powers of arrest may be less desirable to applying for a search warrant.

43 Police and Criminal Evidence Act 1984 (Department of Trade and Industry Investigations) Order 2002 (SI 2002 No 2326); The Secretaries of State for Business, Energy and Industrial Strategy, for International Trade and for Exiting the European Union and the Transfer of Functions (Education and Skills) Order 2016 (SI 2016 No 992), sch 1, para 26.

44 Police and Criminal Evidence Act 1984 (Department of Trade and Industry Investigations) Order 2002 (SI 2002 No 2326), arts 3 and 4(7)(a) and (i).

all necessary information is provided to the issuing authority. Those who execute warrants must have the power to use force and deal with uncooperative or aggressive occupiers where necessary. A single agency may or may not be equipped to perform both roles. A good example is the SFO, who can apply for a search warrant but once obtained the warrant must be executed by the police, whom they may accompany. It is therefore sensible in principle to retain the distinction between applying for and executing a warrant.

3.26 We agree with those consultees who argued that there must be a strong justification for giving each new agency the power to apply for a search warrant. Those officials applying for search warrants must be subject to stringent safeguards and undergo training to understand the duties owed to the court when making a without notice application. However, the training should not necessarily mirror that which is given to the police, but instead be tailored to each agency and the nature of their investigations.

3.27 We consider that the case for giving the NHSCFA and NHSCFSW the power to apply for search warrants has been made out. We also consider that the case for extending the existing powers of the Insolvency Service to apply for search warrants has been made out. We are of the view that these changes would enable these agencies to conduct investigations more effectively and bring about wider procedural efficiency. We also see these benefits as outweighing any perceived risk that these powers would be open to misuse or be exercised improperly.

3.28 Before we discuss each agency, we make one final observation regarding the provision of police assistance to private prosecutors through applying for search warrants. We mention the case of *R v Zinga* at paragraph 3.6 above, in which a search warrant was applied for by the police on behalf of Virgin Media Ltd. In this case, two individuals were convicted of conspiracy to defraud. They subsequently appealed their convictions on the ground that the trial judge ought to have acceded to an application to stay the prosecution as an abuse of process. It was submitted that the trial judge fell into error in finding that the identity of Virgin Media Ltd as the likely prosecutor was not a matter that the police was required to explain to the issuing authority when applying for the warrants. While the appellants were not successful on this point, the Court of Appeal did consider that the police ought to have disclosed the identity of the intended prosecutor.[45]

3.29 We conclude at paragraph 4.75 below that the identity of an intended prosecutor ought to be included as part of a non-exhaustive list of examples of matters relevant to the duty of candour in search warrant application forms. This would include whether it is envisaged that the investigation will result in a private prosecution. More generally, it has recently been highlighted that there is currently no guidance as to when the police should assist a company's investigative team which lacks powers to seek a warrant to search premises.[46] It has also been suggested that such guidance would be desirable to prevent potential miscarriages of justice.[47] We go no further than simply making these observations. This is not a matter on which we have received any consultation responses. It also relates to the

---

45 *R v Zinga* [2012] EWCA Crim 2357 at [32], [2013] Crim LR 226.

46 Oral evidence session, Justice Committee – Private Prosecutions: Safeguards, HC 497 (7 July 2020) Q65, https://committees.parliament.uk/oralevidence/673/pdf/.

47 Jonathan Rogers, "Private prosecutions and safeguards" [2020] *Criminal Law Review* 769, 771.

wider area of private prosecutions, the safeguards in connection with which are currently being examined by the Justice Committee.[48]

The NHS Counter Fraud Authority

3.30 We have considered in detail whether the current law provides sufficient mechanisms for the NHSCFA to obtain medical records where a person is unlikely or unwilling to provide them. There are currently two possible avenues, neither of which is ideal, and both of which would involve the NHSCFA seeking the assistance of the police. The first is for the police to arrest an individual in order to trigger the powers under sections 18 or 32 of PACE. The second is to make an application under schedule 1 to PACE.

3.31 On the first of these avenues, we take the point made by Dijen Basu QC that the lack of capability to apply for a search warrant may push the agency down the route of persuading a constable to arrest an individual in order to trigger the search of premises. While we have no evidence that arrest in these circumstances occurs in practice, we are concerned about the possibility of arrest being used to enable the NHSCFA to gain access to medical records which it may need during the course of an investigation. Arrest is likely to be a disproportionate means of obtaining evidence and may, in some cases, amount to a misuse of arrest, leading to litigation concerning its lawfulness. In addition, arresting someone is a time-consuming and bureaucratic procedure for police officers, and could have long-term consequences for the person arrested.[49]

3.32 In contrast, the use of a search warrant is a proportionate and targeted infringement of the occupier's rights. Crucially, a warrant application will have been scrutinised by a judicial officeholder.

3.33 The second avenue we have considered is the use of schedule 1 to PACE. This can be used to access "excluded material", which would include medical records, but only in very limited circumstances. In order to access excluded material under schedule 1, the "second set of access conditions" must be met.[50] To satisfy the second set of access conditions, the investigator must be able to identify a provision which was enacted prior to PACE under which a search warrant could have been issued in respect of the target material.[51] We discuss the problems with the second set of access conditions at paragraphs 12.68 to 12.74 below.

3.34 We have concluded that there are few, if any, pre-PACE provisions under which a search warrant could have been obtained in respect of medical records. Section 7 of the Forgery and Counterfeiting Act 1981 permits the search and seizure of "false instruments". However,

---

48 See https://committees.parliament.uk/work/401/private-prosecutions-safeguards. The Law Commission considered the right to bring a private prosecution as part of its work on consents to prosecution. See, Consents to Prosecution (1998) Law Com No 255.

49 Being arrested may have long-term consequences for an individual, even if they are later de-arrested or it is established that the arrest was wrongful. An arrest will be recorded on the Police National Computer and may be disclosed pursuant to an enhanced Disclosure and Barring Service (DBS) check. Photographs, fingerprints and non-intimate DNA samples may have been taken by force. For healthcare professionals, there may be a requirement to notify their professional body. An individual may also be required to declare any arrests on a visa application.

50 Police and Criminal Evidence Act 1984, sch 1, para 3. Note that the first set of access conditions cannot be used to obtain excluded material: see Police and Criminal Evidence Act 1984, sch 1, para 2(a)(ii).

51 Police and Criminal Evidence Act 1984, sch 1, para 3(b).

in our view, using this provision to obtain a warrant under schedule 1 to PACE for an NHSCFA investigation would create problems. The provision permits searches for false instruments themselves, not for evidence that instruments have been falsified. The NHSCFA may be required to check claims made by the suspect against non-falsified patient records. Therefore, the provision is not broad enough to cover all of the medical records for which the Authority may need to search.

3.35 In Chapter 10 we discuss the operation of the "iniquity exception", whereby material may lose its confidentiality or even its status as protected material where it is held in furtherance of a crime. However, we do not think that such an exception would overcome the problems caused by the second set of access conditions. Depending on the formulation of the exception, it would apply to documents created, acquired or held with the intention of furthering a criminal purpose. This may capture the falsified part of patient records, but the remainder of the record would be likely to remain excluded material. Nor would it enable the Authority to obtain non-falsified patient records to cross-check claims made by a suspect.

3.36 For these reasons, we have concluded that there is a strong case for the NHSCFA to have a specific regime, which would (1) allow them to apply for search warrants in their own right (rather than having to enlist the help of the police); and (2) allow them to search for material consisting of medical records, which cannot currently be the subject of a search warrant under PACE. The power to apply for a search warrant, and the types of material it should cover, should be subject to a specially tailored regime, rather than a modified application of PACE, which would sit within existing health legislation. In general terms, we consider that a search warrant should be available where the suspect has not complied with a production notice, it would be impracticable to issue a production notice or service of a production notice may seriously prejudice the investigation.

3.37 Following discussions with the NHSCFSW, we have identified that they would also benefit from being empowered to apply for search warrants. The NHSCFSW is the Welsh counterpart of the NHSCFA and overseen by the Senedd Cymru (Welsh Parliament). The NHSCFSW are, in effect, a mirror image of the NHSCFA, and undertake the same work and carry out the same functions as the NHSCFA;[52] they too suffer the same obstacles as the NHSCFA as a result of being unable to obtain search warrants.

3.38 We are of the view that our conclusions regarding the NHSCFA have equal application to the NHSCFSW. Importantly, without the power to apply for a search warrant, an unprincipled and inconsistent position would exist between the investigatory powers of the NHSCFA and NHSCFSW. We have therefore concluded that there is an equally strong case for the NHSCFSW to be empowered to apply for search warrants in their own right and search for material consisting of medical records.

3.39 We are therefore recommending that:

(1) the NHSCFA and NHSCFSW should be entitled to apply for search warrants;

(2) this power should apply where a person fails to comply with a production notice under section 197 of the NHS Act 2006, or under section 145 of the NHS (Wales) Act 2006 in the case of the NHSCFSW;

---

[52] See National Health Service (Wales) Act 2006, Part 10; National Assembly for Wales, National Health Service Act 1977 Directions to NHS Bodies on Counter Fraud Measures 2005.

(3) the power to search under such warrants should extend to medical records (and other material that might constitute excluded material under PACE); and

(4) NHSCFA and NHSCFSW officers or a constable should be empowered to enter and search premises (discussed at paragraphs 3.63 to 3.67 below).

3.40 Beyond these points, the precise structure of the powers, including further conditions for issuing a warrant and the safeguards that should apply, would be matters for the sponsoring department, the Department of Health and Social Care (and the Welsh Government's Department of Health and Social Services from the perspective of the NHSCFSW), in consultation with relevant stakeholders.

Recommendation 5

3.41 We recommend that the NHS Counter Fraud Authority and the NHS Counter Fraud Service Wales be given powers to apply for a search warrant where there has been non-compliance with, or it is impracticable to issue, a production notice. Such powers should include searching for medical records and other related material which might constitute "excluded material" under the Police and Criminal Evidence Act 1984.

The Insolvency Service

3.42 The power to apply for a schedule 1 PACE warrant for special material procedure has been extended to officers of the Insolvency Service by an order made under section 114A of PACE ("the PACE Order").[53] However, article 3 of the PACE Order extends the provisions of schedule 1 to PACE to BEIS investigators "as far as they relate to special procedure material",[54] which means that the Insolvency Service may only search for and seize special procedure material. Accordingly, Insolvency Service officers do not currently have the power to apply for search warrants for ordinary material under section 8 of PACE, or for a warrant under schedule 1 which relates to mixed material (ordinary material and special procedure material).

3.43 We have concluded that the Insolvency Service should also be able to apply for a warrant under section 8 of PACE and for a mixed warrant under schedule 1. We are of the view that if the Insolvency Service has been entrusted by Parliament with the power to obtain a schedule 1 warrant, which is for protected categories of material, it should be empowered to obtain a section 8 warrant, which is for ordinary material which does not attract additional statutory protection. We consider that there is a gap in the Insolvency Service's enforcement powers which places an unnecessary burden on police resources.

3.44 It seems to us sensible for the Insolvency Service to be permitted to obtain a warrant under section 8 of PACE for two reasons: firstly, because section 8 of PACE does not require an application to be made to a Circuit judge in the Crown Court, and secondly, because it is

---

53 Police and Criminal Evidence Act 1984 (Department of Trade and Industry Investigations) Order 2002 (SI 2002 No 2326), arts 3 and 4(2), 4(7)(a) and (i).

54 Police and Criminal Evidence Act 1984 (Department of Trade and Industry Investigations) Order 2002 (SI 2002 No 2326), art 3(a).

conceivable that the only material sought by the Insolvency Service is ordinary material.[55] We also consider that the Insolvency Service should be able to apply for warrants in relation to mixed material under schedule 1 to PACE, rather than only for special material procedure.

3.45 These recommendations would require a change to primary legislation. Section 114A(1) of PACE confers on the Secretary of State (in practice, the Secretary of State for Business, Energy and Industrial Strategy ("BEIS")) the power to direct that schedule 1 to PACE applies to BEIS investigators (which would include Insolvency Service officers), but only insofar as it relates to special material procedure. Accordingly, extending the powers of Insolvency Service officers could not be made by order and would instead require primary legislation.

Recommendation 6

3.46 We recommend that the Insolvency Service be given the statutory power to apply for a search warrant under section 8 of the Police and Criminal Evidence Act 1984 and to apply for a "mixed warrant" relating to both ordinary material and special procedure material under schedule 1 to that Act.

AGENCIES ENTITLED TO EXECUTE A SEARCH WARRANT

The current law

3.47 Section 16(1) of PACE provides that a warrant to enter and search premises may be executed by any constable. Individuals who are not constables can only execute a search warrant where legislation so provides. For example, an immigration officer may be authorised to enter and search premises under the Immigration Act 1971.[56]

3.48 Search warrant provisions usually operate in one of two ways. Some provisions, such as section 8 of PACE, empower the same individual to both apply for and execute a search warrant. Other warrant provisions permit one individual to apply for a search warrant and another (usually a constable) to execute it. The applicant may merely *accompany* the person executing the warrant. This is the case for warrants sought by the SFO and the Insolvency Service: officials within these organisations may apply for a warrant, however, the warrant must be executed by a constable, whom the officials may accompany.

The consultation paper

3.49 In our consultation paper, we wrote that the reason why some statutes only allow for warrants to be executed by constables while others allow for warrants to be executed by the agency seeking the warrant can be explained by the likely differing policy decisions made when the provisions were drafted. These differences are justified by the distinct nature of the investigations envisaged under each regime and the official concerned. A fixed and uniform rule across all warrant provisions specifying who can execute a search warrant would therefore be undesirable as not all those who apply for a warrant would be in a position to execute it safely.

---

55 In particular, the confidentiality of some material may be affected by the iniquity exception: see further discussion in Chapter 10 of this report.

56 Immigration Act 1971, s 28FB(3).

3.50 We nonetheless invited[57] consultees' views on whether there are any investigative agencies whose investigatory or enforcement powers are unnecessarily hindered because they are currently unable to execute a search warrant.

Consultation responses

3.51 Fourteen consultees[58] answered this question. Generally, consultees considered that there were no agencies which were unnecessarily hindered because they were unable to execute a search warrant. However, it was accepted that where agencies that are unable to execute a search warrant are assisted by the police, this is perhaps not a sensible use of police resources.[59]

3.52 The NHSCFA, Insolvency Service and DWP made specific comments about their inability to execute a search warrant.

3.53 DWP put forward a number of reasons why they would not want the power to execute a warrant. These reasons were the need for further training, the need for devising of policies regarding search and seizure and the potential adverse cost and resource implications.

The NHS Counter Fraud Authority

3.54 On the strength of the arguments presented by the NHSCFA, we recommend at paragraph 3.41 above that the Authority be given the power to apply for a search warrant where there has been non-compliance with, or it is impracticable to issue, a production notice. We sought further clarification after close of the consultation as to whether they had a preference as between:

(1) being able to execute their own warrants; or

(2) accompanying a constable executing a warrant which had been applied for by an NHSCFA officer.

3.55 The NHSCFA explained that, in their view, they should be able to apply to the court for the warrant but, once granted, lawful entry should be effected by a constable. The Authority argued that this would protect their staff from potential violence or breaches of the peace, with which they do not have the necessary powers or training to deal. In addition, it would allow the police to prevent breaches of the peace and take the appropriate action where persons attempt to obstruct NHSCFA staff in their search, which may include arrest.

3.56 That said, the Authority also suggested that the police ought not to be required to be present throughout the whole search, as they currently are under section 16(2B) of PACE. They suggested that the police should be able to leave the premises once they have gained lawful entry and a risk assessment has been carried out regarding the safety of NHSCFA staff.

---

57 Consultation Question 28.

58 Department for Work and Pensions; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Kent County Council Trading Standards; Insolvency Service; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; The Law Society; Magistrates Association; Dijen Basu QC; National Crime Agency; Competition and Markets Authority; Serious Fraud Office; Financial Conduct Authority.

59 Birmingham Law Society.

The Insolvency Service

3.57 We recommend at paragraph 3.46 above that the Insolvency Service be given the power to apply for a search warrant under section 8 of PACE. The Insolvency Service expressed the view that being able to execute their own warrants would also be extremely beneficial.

3.58 As indicated at paragraph 3.48 above, the Insolvency Service can apply for search warrants under schedule 1 to PACE to search for and seize special procedure material.[60] However, the statutory instrument that gives the Insolvency Service that power provides that their warrants authorise a *constable*, together with any other person named in it and any other constables, to enter and search the premises.[61] The Insolvency Service therefore cannot execute search warrants concerning their own investigations. Where Insolvency Service officers do accompany a constable, they may only exercise powers in the company, and under the supervision, of a constable.[62]

3.59 The Insolvency Service strongly supported the suggestion that powers be introduced to allow them to execute their own search warrants. Their experience is that the police do not always have a detailed understanding of the investigation and so are unable to make informed judgments about what material should be seized. This can lead to more material being seized than is necessary.

Analysis

3.60 At paragraph 3.49 above, we expressed the view that a uniform rule across all search warrant provisions specifying who can execute a warrant would be undesirable. Confirming this, the NHSCFA and the Insolvency Service expressed different views about whether they ought to be able to execute their own warrants: the NHSCFA wished to be able to execute the search part of the warrant, but for a constable to have to effect entry, whereas the Insolvency Service wished to be able to execute both aspects.

3.61 In our view, whoever executes a warrant must have adequate knowledge of the case and be capable of executing the warrant safely and seizing evidence securely, while following necessary safeguards. Depending on the investigation, the individual best place to do this may be a constable, someone from another investigative agency or the police in conjunction with that agency. Therefore, we recognise that the most desirable model may differ by institution, depending on the nature of their investigations.

3.62 A flexible, agency-specific approach will make little difference to the level of protection afforded to those whose property is searched. Anyone who executes a warrant must act within the terms of the warrant and follow general public law principles by exercising their powers rationally, proportionately and in good faith.

The NHS Counter Fraud Authority

3.63 We have considered the argument advanced by the NHSCFA that they should be able to apply for a search warrant but a constable, whom they are entitled to accompany, should be

---

60 Police and Criminal Evidence Act 1984 (Department of Trade and Industry Investigations) Order 2002 (SI 2002 No 2326), art 3(1)(a).

61 Police and Criminal Evidence Act 1984 (Department of Trade and Industry Investigations) Order 2002 (SI 2002 No 2326), art 4(7)(i).

62 Police and Criminal Evidence Act 1984 s 16(2A) and (2B).

required to effect lawful entry. We agree that this would protect NHSCFA staff from any violent or uncooperative individuals on the premises. However, to enable operational flexibility, we consider that legislation should permit *either* an NHSCFA officer or a constable to execute a warrant,[63] with each being able to accompany the other under the warrant. This position would still enable a search warrant applied for by the NHSCFA to be executed by the police should it be deemed that the execution of a warrant might present a genuine risk to the safety of NHSCFA staff. In those cases where no risk exists, the NHSCFA would be permitted to apply for and execute their own warrants without taking up the time of, and at a cost to, the police.

3.64 We do, however, accept the observation made by the NHSCFA at paragraph 3.56 above that it would be unnecessary for a constable to be required to be present throughout the whole search should they be accompanied by NHSCFA officers. We discuss the requirement, which exists under certain statutes, for a constable to remain on premises in order for other agencies to exercise powers of search and seizure at paragraphs 3.82 to 3.106 below, where we identify several reasons why it is an undesirable requirement and recommend reform accordingly. A number of those arguments have force in respect of the NHSCFA, namely that the requirement for a constable to remain present may place an unnecessary burden on police resources when their presence is unnecessary for the safe and effective execution of a warrant. For these reasons, we have concluded that, in relation to NHSCFA warrants, the continued presence of a constable following the execution of a search warrant ought to be an operational decision rather than a legal requirement for the warrant to remain in effect.

3.65 Given that the continued presence of a constable may not be required once lawful entry to the premises has been effected, thought will need to be given to whether obstructing someone who is executing a search warrant should be made an offence. We discuss why obstruction offences may be necessary in instances where a constable is not required to remain on the premises at paragraphs 3.99 to 3.104 below.

3.66 Additionally, safeguards similar to those found in section 16 of PACE should apply to the NHSCFA to ensure consistent protection to those affected by a warrant. We also see merit in an investigator being required to adhere to a Code of Practice made under section 200 of the NHS Act 2006, which may have to be amended. Supplementary powers and duties in relation to the access to, copying and retention of material may also be required.

3.67 Finally, we repeat the observations that we made above at paragraph 3.37 that the NHSCFSW, which is the Welsh counterpart of the NHSCFA, suffers the same obstacles as the NHSCFA as a result of being unable to obtain and execute search warrants. To ensure that it too is equipped to investigate effectively high value economic crime within the NHS, the same position ought to be adopted in respect of the NHSCFSW.

---

[63] For an example of a search warrant provision drafted in this way, see the Animal Welfare Act 2006, s 23(1).

Recommendation 7

3.68 We recommend that a search warrant applied for by the NHS Counter Fraud Authority or NHS Counter Fraud Service Wales permit either that agency or a constable to execute the warrant.

3.69 An NHS Counter Fraud Authority officer or NHS Counter Fraud Services Wales officer authorised to accompany a constable under a warrant should be able to exercise powers of search and seizure under the warrant irrespective of whether they are in the company, or under the supervision, of a constable, after the constable has effected entry.

The Insolvency Service

3.70 As indicated at paragraphs 3.48 and 3.58 above, the Insolvency Service cannot execute search warrants concerning its own investigations. It must enlist the help of a constable to execute the warrant, whom officials from the Insolvency Service are entitled to accompany.[64]

3.71 The Insolvency Service has expressed the firm view that the requirement for a constable to execute a search warrant which relates to its criminal investigations is unnecessary. We agree that there may be occasions when it is unnecessary and needlessly costly for a constable to execute a warrant applied for by or on behalf of the Insolvency Service.

3.72 Importantly, Insolvency Service officers executing a warrant would still be required to comply with the same statutory safeguards as constables when applying for a warrant under section 15 of PACE. Section 16 of PACE would, however, require extension and modification.

3.73 By way of example, section 16 of PACE does not apply to Insolvency Service officers given that they are not empowered to execute warrants. Section 16(3A) and (3B), which govern authorisation for the purpose of multiple entry and all premises warrants, require authorisation by a "police officer of at least the rank of inspector". The words have been modified for other agencies.[65]

3.74 In this context, to maintain the stringency of the safeguard, we consider an appropriate level of authorising officer to be "a crime[66] investigating officer in the Insolvency Service at Grade 7 or above". This is the civil service grade at which a Chief Investigator sits. Reference to the grade rather than the job title would allow the wording to survive changes in job titles. There is also precedent for similar wording.[67]

---

64 Police and Criminal Evidence Act 1984 (Department of Trade and Industry Investigations) Order 2002 (SI 2002 No 2326), art 4(7)(a) and (i).

65 In the context of HMRC, the words "police officer of at least the rank of inspector" have been replaced with "officer of Revenue and Customs of at least the grade of higher officer": see Police and Criminal Evidence Act 1984 (Application to Revenue and Customs) Order 2015 (SI 2015 No 1783), art 3(2) and (3).

66 The inclusion of the word "crime" would prevent authorisation being given by a senior Insolvency Service officer who oversees the Service's civil enforcement work.

67 Namely the words "An investigating officer in the Insolvency Service at Grade 7 or above": see Investigatory Powers (Codes of Practice and Miscellaneous Amendments) Order 2018 (SI 2018 No 905) art 4(5).

3.75 There are officers in other investigative agencies who are empowered to execute search warrants without a constable being present, including immigration officers,[68] HMRC,[69] the SFO,[70] the FCA,[71] and officers of "enforcers"[72] under consumer protection legislation.[73] Therefore, the mere fact that Insolvency Service officers are not police constables is not a sufficient reason for the Insolvency Service not having the power to execute search warrants.

3.76 Although the Insolvency Service may wish for a constable to be present to ensure the safety of its officers, we consider that this should be an operational decision rather than a legal requirement to effect lawful entry. In other words, the presence of a constable may be unnecessary where members of the Insolvency Service have adequate knowledge of the case and are capable of executing the warrant safely and seizing evidence securely, while following necessary safeguards. However, there may be occasions where it would still be desirable for a constable to execute a search warrant even though it has been applied for by an Insolvency Service officer, and this option should still be available.

3.77 We are also of the view that sections 19 to 22 of PACE should be extended to the Insolvency Service, with necessary modifications. These sections provide powers of seizure and compulsion while on premises,[74] in addition to regulating the access, copying and retention of material.[75]

3.78 These provisions therefore provide supplementary powers and duties in relation to search warrants which ensure effective criminal enforcement and safeguards regarding the treatment of material. Further, we note that these provisions have been extended to other agencies who have been given the power to apply for search warrants under PACE, including immigration officers,[76] designated customs officials,[77] and officers of Revenue and Customs.[78] Sections 21 and 22 of PACE have also been extended to powers of seizure

---

68 Police and Criminal Evidence Act 1984 (Application to immigration officers and designated customs officials in England and Wales) Order 2013 (SI 2013 No 1542), sch 1; Proceeds of Crime Act 2002, s 352.

69 Police and Criminal Evidence Act 1984 (Application to Revenue and Customs) Order 2015 (SI 2015 No 1783), sch 1; Proceeds of Crime Act 2002, s 352.

70 Proceeds of Crime Act 2002, s 352.

71 Proceeds of Crime Act 2002, s 352.

72 This includes officers of the Competition and Markets Authority; a local weights and measures authority in Great Britain; a district council in England; the Secretary of State; the Gas and Electricity Markets Authority; the Civil Aviation Authority; the British Hallmarking Council; the Office of Communications; and the Information Commissioner (see Consumer Rights Act 2015, sch 5, paras 3 and 4).

73 Consumer Rights Act 2015, sch 5, para 32(1).

74 Police and Criminal Evidence Act 1984, ss 19 and 20.

75 Police and Criminal Evidence Act 1984, ss 21 and 22.

76 Police and Criminal Evidence Act 1984 (Application to immigration officers and designated customs officials in England and Wales) Order 2013 (SI 2013 No 1542), sch 1(1), para 1.

77 Police and Criminal Evidence Act 1984 (Application to immigration officers and designated customs officials in England and Wales) Order 2013 (SI 2013 No 1542), sch 2(1), para 1.

78 Police and Criminal Evidence Act 1984 (Application to Revenue and Customs) Order 2015 (SI 2015 No 1783) sch 2(1), para 1.

pursuant to search warrants issued to an "appropriate person"[79] under section 352 of the Proceeds of Crime Act 2002.[80]

3.79 At Recommendation 6 above,[81] we recommend that Insolvency Service officers should be given the power to apply for a search warrant under section 8 of PACE. Were this recommendation to be implemented, we consider that the power of the Insolvency Service to execute warrants should extend to warrants under both section 8 of and schedule 1 to PACE.

Recommendation 8

3.80 We recommend that the Insolvency Service be empowered to execute search warrants obtained under the Police and Criminal Evidence Act 1984 (Department of Trade and Industry Investigations) Order 2002, without the need to accompany a constable. This would extend to exercising the powers of entry as well as search.

3.81 We also recommend that sections 19 to 22 of the Police and Criminal Evidence Act 1984 be extended to the Insolvency Service, with necessary modifications.

REQUIRED PRESENCE OF A CONSTABLE IN ORDER TO EXERCISE POWERS

3.82 Although it was not discussed in our consultation paper, consultees drew to our attention that problems arise in practice from the requirement that certain investigators can only exercise their powers of search and seizure in the presence of a constable.

Consultation responses

3.83 Two consultees[82] addressed the problem of the required presence of a constable in order to exercise powers on premises pursuant to a warrant. The SFO and the FCA both identified an issue under their respective legislative regimes. Under section 2 of the CJA, a member of the SFO can apply for a search warrant in the context of an investigation into serious fraud. Similarly, an FCA officer can apply for a search warrant under section 176 of the FSMA to investigate breaches of that Act. However, once obtained, search warrants under both provisions must be executed by a constable with the agency only able to exercise powers whilst in their company and under their supervision.[83] This means that if the constable leaves the premises, even to return later, the warrant's authority is spent from the point of their departure.

3.84 Neither the SFO nor the FCA identified problems with the requirement that a constable must effect lawful entry. The SFO maintained the view that the police or NCA officers (who can be

---

79 Proceeds of Crime Act 2002, s 352(5): a Financial Conduct Authority officer; a National Crime Agency officer; an officer of Revenue and Customs; a Serious Fraud Office officer; an immigration officer; and an accredited financial investigator.

80 Proceeds of Crime Act 2002 (Application of Police and Criminal Evidence Act 1984) Order 2015 (SI 2015 No 759) arts 4 and 5.

81 See para 3.46 above.

82 Serious Fraud Office; Financial Conduct Authority.

83 Criminal Justice Act 1987, s 2(6A); Financial Services and Markets Act 2000, s 176(5C).

designated as constables for the purposes of section 8 of PACE) were better placed to secure entry to premises. This was primarily because it might be necessary to use force and constables are trained to do this safely and proportionately.[84]

3.85 Both agencies argued that requiring a constable to remain on the premises leads to an unnecessary drain on police resources. This will be the case when an investigation requires a lengthy search, the premises has been secured and the occupants are not considered to pose a danger to those conducting the search. The problem was said to be exacerbated by the ever-increasing need for the skills of digital forensic officers in the course of such searches. It was also pointed out that investigators of the relevant agency are likely to be in a better position than constables to assess whether material falls within the scope of the warrant.

3.86 The SFO and FCA therefore suggested that the requirement for a constable to execute a search warrant should be limited to the act of entry and not require the constable's ongoing presence. In their view, the authority of a search warrant should not become spent solely because all constables have left the search premises.

3.87 It was accepted that in some cases it may be desirable for a constable to remain on the premises for the duration of the search. However, it does not follow that the lawfulness of a search should be contingent on a constable being present. The agencies argued that whether a constable should remain on the premises, and for how long, should be decided by carrying out an operational risk assessment.

Analysis

3.88 Whether a search warrant sought by an investigative agency must be executed by a constable varies by agency, depending on the circumstances: legislative consistency should not be pursued for its own sake. Each search warrant provision must be considered separately, taking into account differences in how crimes are committed and criminal investigations are conducted.

3.89 We see merit in the suggestion that members of the SFO and the FCA ought to be able to remain on the premises and exercise powers of search and seizure without a constable's ongoing presence once a constable has effected lawful entry. In fact, section 2 of the CJA and section 176 of FSMA both allow certain other persons, in addition to members of the SFO and FCA, to accompany a constable executing search warrants under those sections.[85] In the rest of this chapter, references to members of the SFO and the FCA include those other persons.

3.90 Several factors have led us to this conclusion. First, we agree that due to technological advances, there is now a significant demand placed on digital forensic officers in criminal investigations. Where they are seeking to retrieve evidence onsite, digital forensics officers may need to remain on premises for extended periods of time to deal with large volumes of data. These officers are vital in identifying, recovering and preserving relevant evidence on or accessible from electronic devices. The time these officers spend on premises has risen

---

[84] We are aware that Serious Fraud Office and Financial Conduct Authority officers are empowered to execute search warrants under the Proceeds of Crime Act 2002 without the assistance of a constable, however, we were not informed specifically why this model under the Proceeds of Crime Act 2002 would be undesirable.

[85] See Criminal Justice Act 1987, s 2(6) and (7) and Financial Services and Markets Act 2000, s 176(5B).

exponentially due to the increase in the number of digital items individuals own and their storage capacity. For example, the imaging of a server by digital forensics specialists during a search of business premises can last for several days. To search large quantities of electronic data safely and legally requires time. This means that there is a risk of a warrant's authority being spent before a search is complete because the constable on the premises is needed elsewhere.

3.91 Secondly, in considering possible reform, we have also taken into account the fact that there may be no occupier on the premises while the search is carried out. Where occupiers are on premises, we do not consider that significant value is provided to an occupier by the presence of a constable. Other agents of the state must follow public law principles by exercising their powers rationally, proportionately and in good faith. Further, the skillset and resources required by the police when executing a search warrant are clearly capable of being replicated by other agencies. For these reasons, we agree that there are occasions when a constable should not be required to remain on the premises for the duration of the search.

3.92 Thirdly, members of the SFO and the FCA are currently empowered to apply for and execute search warrants under section 352 of the Proceeds of Crime Act 2002 ("POCA"), where this is necessary in the course of an investigation under that Act. Under this provision, a constable need not be involved in any part of the execution of the warrant. Parliament therefore has already entrusted the SFO and the FCA to execute search warrants without a constable being present or having any involvement in the search.

3.93 The powers which we consider should no longer only be exercisable in the presence, or under the supervision, of a constable are:

(1) the power to search premises in section 2(5)(a) of the CJA and the powers contained in section 2(5)(b) of the CJA to take possession of any documents or to take steps necessary to preserve documents; and

(2) the powers contained in section 176(5)(b) to (d) of FSMA to search premises, to take possession of documents, to take steps to preserve documents, to take copies and to require explanations from persons on the premises.

3.94 If members of the SFO and the FCA were permitted to exercise such powers when not in the company, and under the supervision, of a constable, we consider that there are three areas where consequential changes may be appropriate:

(1) the application and modification of section 16 of PACE;

(2) the application and modification of Code B of PACE; and

(3) the creation of a new offence of obstructing a person who is carrying out functions under a search warrant.

We discuss each of these in turn below.

The application and modification of section 16 of PACE

3.95 As we explained in Chapter 2 at paragraphs 2.51 and 2.52 above, it is not clear on the face of the legislation whether section 16 of PACE applies to search warrants under section 2 of

the CJA. Accordingly, at Recommendation 1 above,[86] we recommend that statutory safeguards, modelled on section 15 and 16 of PACE, are inserted into the CJA. By contrast, section 176(6) of FSMA expressly applies section 16(3) to (12) of PACE.

3.96 If SFO and FCA members were permitted to search premises not in the company of a constable, modifications to section 16(8) to (12) of PACE would be needed to make it clear that the duties contained in those sections continue to apply. These subsections place duties on a constable both during and after the execution of a search warrant. In summary, these are:

(1) limiting the extent of a search under warrant to that which is required for the purpose for which the warrant was issued;

(2) requiring a constable to endorse the warrant stating whether the material sought was found and whether any material other than that which was sought was seized; and

(3) requiring a constable to return the warrant to the designated officer for the local justice area or court officer.

3.97 Consideration would also be needed as regards the application of section 16(5) to (7) of PACE, which contain requirements about identification of the person executing the warrant and leaving it on the premises: these duties might have to be carried out by SFO or FCA members in the situation where the occupier was not on the premises when entry was effected but returned during the course of the search.

The application and modification of Code B of PACE

3.98 Secondly, with respect to Code B of PACE, where a constable does not remain on the premises, the equivalent of the "officer in charge of the search" would need to be a member of the investigative agency carrying out the search. At Recommendation 2 above,[87] we recommend that the PACE Strategy Board consider amending Code B of PACE to provide guidance for non-police investigators in complying with the provisions of the Code. This could helpfully include explaining the role of those accompanying police and whether a person other than a police officer may act as the "officer in charge of the search". This would clarify the duties owed by investigative agencies carrying out searches.

The creation of a new obstruction offence

3.99 Thirdly, we consider that a new offence of obstruction would be needed for SFO officers carrying out searches under section 2 of the CJA. At present the offence of obstruction cannot be committed unless a constable is on the premises. Under section 89(2) of the Police Act 1996, any person who resists or wilfully obstructs a constable, or a person *assisting* a constable, in the execution of their duty is guilty of an offence. The offence is punishable on summary conviction by imprisonment for a term not exceeding one month or a fine not exceeding level 3 on the standard scale, or both.

3.100 A gap in the SFO's enforcement powers would therefore exist where a constable is no longer on premises. This can be contrasted with warrants under section 176 of FSMA, where it is an offence to intentionally obstruct the exercise of "any rights conferred by a

---

86 See para 2.56 above.

87 See para 2.98 above.

warrant".[88] Accordingly, we consider that it should be an offence to wilfully obstruct a person who is acting in the exercise of a power conferred by a search and seizure warrant issued under section 2 of the CJA.

3.101 We recognise that new offences should not be created lightly, and in reaching this conclusion we have taken into account the following three matters.

3.102 Firstly, although there is no case law on this point, it is our view that an offence under section 89(2) of the Police Act 1996 would be committed where an officer who is not a constable but accompanying a constable on a search is wilfully obstructed, especially when exercising powers. This is because they are "assisting" a constable for the purposes of the provision. Therefore, appropriate persons under the CJA are arguably protected under the current law when they accompany a constable executing a warrant. This protection would be lost without a new obstruction offence.

3.103 Secondly, obstruction offences also exist for other agencies, so there would seem to be no matter of principle in restricting such an offence to obstructing a constable.[89] It is of practical note that an obstruction offence already exists in relation to "appropriate persons" acting in the exercise of a power conferred by a search warrant issued under section 352 of POCA.[90] Appropriate persons include FCA officers and members of staff of the SFO.[91] This is not the only obstruction offence for members of staff of the SFO under POCA.[92]

3.104 Thirdly, we consider that an obstruction offence is desirable to prevent searches under warrant being frustrated and would be a proportionate response. Section 2(5)(b) of the CJA provides powers to enable investigation into serious criminality and we consider that it is appropriate that such powers be backed up by an obstruction offence, in the same way that other equivalent powers on the statute book are.

---

88 Financial Services and Markets Act 2000, s 177(6).

89 Commissioners for Revenue and Customs Act 2005, s 32; UK Borders Act 2007, ss 22 and 23; Proceeds of Crime Act, s 453A.

90 Proceeds of Crime Act 2002, s 356A(2).

91 Proceeds of Crime Act 2002, s 356A(5)(a) read with s 352(5A).

92 Proceeds of Crime Act 2002, s 453B.

Recommendation 9

3.105 We recommend that the following powers be exercisable by members of the Serious Fraud Office and the Financial Conduct Authority (in addition to appropriate officers and authorised officers) irrespective of whether they are in the company, or under the supervision, of a constable:

(1) the power of search in section 2(5)(a) of the Criminal Justice Act 1987, and the additional powers in section 2(5)(b); and

(2) the powers in section 176(5)(b) to (d) of the Financial Services and Markets Act 2000.

3.106 We also recommend:

(1) that the duties in section 16(8) to (12) of the Police and Criminal Evidence Act 1984 apply to members of the Serious Fraud Office and the Financial Conduct Authority who are executing search warrants not in the presence of a constable;

(2) that consideration be given to how the safeguards in section 16(5) to (7) of the Police and Criminal Evidence Act 1984 should apply; and

(3) the creation of an offence of wilfully obstructing a person who is acting in the exercise of a power conferred by a warrant issued under section 2 of the Criminal Justice Act 1987.

Chapter 4: Search warrant application documents

INTRODUCTION

4.1 In Chapter 4 of the consultation paper, we considered potential reforms to the procedure by which an investigator applies for a search warrant. A large portion of the chapter was devoted to discussing the documents used to apply for a warrant: search warrant application forms and draft warrant templates. In this chapter, we focus exclusively on how these documents should be reformed. More specifically, we discuss:

(1) the need for bespoke warrant application forms;

(2) the content of warrant application forms;

(3) the need for draft warrant templates; and

(4) the introduction of an online application portal.

4.2 The aims of the provisional proposals contained in our consultation paper were to improve procedural efficiency and reduce the scope for serious errors when applying for a search warrant. Errors at the application stage have frequently led to warrants being declared unlawful.[1] As one means of addressing this, we provisionally proposed that application forms be clarified and amended to promote greater compliance with statutory criteria and the duty to make full and frank disclosure.[2]

4.3 Consultees' responses have fortified our view, and we recommend below that further guidance be provided on what application forms should contain. We also recommend the creation of application forms and a warrant template for entry warrants as, at present, investigators must modify search warrant forms for this purpose. Finally, we recommend that consideration be given to introducing an online search warrant application portal to guide

---

1 *R (Brook) v Preston Crown Court* [2018] EWHC 2024 (Admin), [2018] ACD 95; *R (Superior Import / Export Ltd) v Revenue and Customs Commissioners* [2017] EWHC 3172 (Admin), [2018] Lloyd's Rep FC 115; *R (Hart) v Blackfriars Crown Court* [2017] EWHC 3091 (Admin), [2018] Lloyd's Rep FC 98; *Hargreaves v Brecknock and Radnorshire Magistrates' Court* [2015] EWHC 1803 (Admin), (2015) 179 JP 399; *R (Chatwani) v National Crime Agency* [2015] EWHC 1283 (Admin), [2015] ACD 110; *R (Kouyoumjian) v Hammersmith Magistrates' Court* [2014] EWHC 4028 (Admin), [2015] ACD 27; *R (Mills) v Sussex Police* [2014] EWHC 2523 (Admin), [2015] 1 WLR 2199; *Sweeney v Westminster Magistrates' Court* [2014] EWHC 2068 (Admin), (2014) 178 JP 336; *R (CPW) v Harrow Crown Court* [2014] EWHC 2061 (Admin); *R (F) v Blackfriars Crown Court* [2014] EWHC 1541 (Admin); *(B) v Huddersfield Magistrates' Court* [2014] EWHC 1089 (Admin), [2015] 1 WLR 4737; *R (Golfrate Property Management Ltd) v Southwark Crown Court* [2014] EWHC 840 (Admin), [2014] 2 Cr App R 12; *Lees v Solihull Magistrates' Court* [2013] EWHC 3779 (Admin), [2014] Lloyd's Rep FC 23; *R (S) v Chief Constable of the British Transport Police* [2013] EWHC 2189 (Admin), [2014] 1 WLR 1647; *R (Hoque) v City of London Magistrates' Court* [2013] EWHC 725 (Admin), [2013] ACD 67; *R (Global Cash & Carry Ltd) v Birmingham Magistrates' Court* [2013] EWHC 528 (Admin), [2013] ACD 48; *R (Anand) v Revenue and Customs Commissioners* [2012] EWHC 2989 (Admin), [2013] CP Rep 2; *R (Rawlinson and Hunter Trustees) v Central Criminal Court* [2012] EWHC 2254 (Admin), [2013] 1 WLR 1634; *R (G) v Commissioner of Police of the Metropolis* [2011] EWHC 3331 (Admin); *R (Power-Hynes) v Norwich Magistrates' Court* [2009] EWHC 1512 (Admin), [2009] Lloyd's Rep FC 619; *Bates v Chief Constable of Avon and Somerset* [2009] EWHC 942 (Admin), (2009) 173 JP 313; *R (Faisaltex) v Preston Crown Court* [2008] EWHC 2832 (Admin), [2009] 1 WLR 1687; *R (Redknapp) v Commissioner of the City of London Police* [2008] EWHC 1177 (Admin), [2009] 1 WLR 2091.

2 Also known as the duty of candour, which we discuss in further detail in Chapter 5.

investigators through the application process, generate relevant documents and allocate hearing slots.

THE NEED FOR BESPOKE APPLICATION FORMS

The current law

4.4 Primary legislation does not prescribe the form an application for a search warrant must take, and the Criminal Procedure Rules ("CrimPR") only require the applicant to apply in writing.[3] The CrimPR and the Criminal Practice Directions ("CrimPD") direct that these forms should be used where possible but provide no sanction for failing to use them. A judge or magistrate may therefore issue a warrant even though a different form, or no form, was used in the application, provided that all the required information is supplied.

4.5 For some search warrant provisions, including section 8 and schedule 1 to PACE, the CrimPR has prescribed a tailored application form to guide applicants through the relevant statutory criteria of each provision.[4] The current form for applying for warrants under section 8 of PACE was introduced in April 2016.[5] The form contains boxes which prompt the applicant to provide information which corresponds to the statutory access conditions. For example, section 8(1)(c) of PACE requires that there be reasonable grounds for believing that material on the premises is likely to be relevant evidence. The third box on the application form asks why the applicant believes that the material for which they want to search is likely to be relevant evidence. There are also notes at the end of the form that provide guidance on completing the form. The form is therefore designed to prompt applicants to provide the information which is required by legislation, the CrimPR and the common law duty of candour.

4.6 Another application form prescribed by the CrimPR is more generic. It is designed to be used when applying for a search warrant under a provision to which sections 15 and 16 of PACE apply and for which there is no specific application form.[6] This form covers the majority of warrant applications not covered by the section 8 of PACE application form. However, some warrants remain outside of its scope.

4.7 CrimPR Division XI 47A, introduced in October 2015 and amended most recently in October 2019, governs the process of applying for and issuing warrants generally. Among other things, it requires investigators applying for a search warrant to use the application forms prescribed by Part 47 of the CrimPR. Where there is no form designed for a particular warrant:

> The forms should still be used, as far as is practicable, and adapted as necessary. The applicant should pay particular attention to the specific legislative requirements for the

---

3 Criminal Procedure Rules, r 47.26(2)(a).

4 Police and Criminal Evidence Act 1984, s 8; Police and Criminal Evidence Act 1984, sch 1; Criminal Justice Act 1987, s 2; Terrorism Act 2000, sch 5, para 11; Proceeds of Crime Act 2002, s 352; Crime (International Co-operation) Act 2003, s 16; Criminal Justice (European Investigation Order) Regulations 2017, regs 6, 11 and 15 to 19. In the case of production orders (including explanation orders, information orders, account monitoring orders and other similar procedures) ten provisions have application forms prescribed under the Criminal Procedure Rules.

5 Criminal Procedure Rules, Part 47, https://www.justice.gov.uk/courts/procedure-rules/criminal/docs/forms/iw001-eng.doc.

6 The application form can be found at: https://www.justice.gov.uk/courts/procedure-rules/criminal/docs/crimpr-part6-rule6-32app.pdf.

granting of such an application to ensure that the court has all of the necessary information, and, if the court might be unfamiliar with the legislation, should provide a copy of the relevant provisions.[7]

4.8 In *Hargreaves*,[8] the Divisional Court stressed the need for caution when adapting a form designed for other legislation, as there is a risk of adapting the form incorrectly. In that case, both the individual who filled out the application form and the magistrate who heard the application failed to address each of the statutory grounds for issuing the warrants, which resulted in the warrants being quashed.[9] This highlights the risk that when modifying an application form, the relevant statutory test may be misconstrued or misapplied, which may lead to a search warrant being declared unlawful.

4.9 Even if sections 15 and 16 of PACE were extended to cover all search warrants relating to a criminal investigation, there is divergence across search warrant provisions as to the statutory grounds for issuing a warrant. As a result, a generic application form could not guide applicants through the precise statutory criteria for a given warrant.

The consultation paper

4.10 In the consultation paper, we provisionally concluded that prescribed application forms are desirable for two reasons.[10] First, application forms are a useful way to guide applicants and prompt them to provide the necessary information. Secondly, well-drafted application forms reduce the risk of errors.

4.11 We considered the advantages and disadvantages of creating a specific application form for each search warrant provision. The principal advantage would be that it would ensure that the applicant and issuing authority are guided through the relevant statutory criteria. However, to be weighed against that is the disadvantage that creating forms for every search warrant provision would be a significant undertaking, which might potentially overburden the Criminal Procedure Rule Committee ("CPRC") and make the Rules themselves overly complex. Additionally, some search warrant provisions are likely used so infrequently that it may be regarded as a waste of time to create application forms for them.

4.12 However, the disadvantage in terms of the time and resources needed to create application forms for every search warrant provision may not prove to be as significant an undertaking as it first appears. First, there is likely to be common ground between many statutory provisions, meaning that an application form designed for one warrant could cover others with little, if any, amendment. Secondly, given the scale of the task, it could be completed in stages, with the assistance of the specialist users or tribunals concerned.

4.13 Without reaching a provisional view, we asked a series of consultation questions.[11] We invited consultees' views on whether:

---

7 Criminal Practice Directions, Division XI 47A.5 (as amended 2019).

8 *Hargreaves v Brecknock and Radnorshire Magistrates' Court* [2015] EWHC 1803 (Admin), (2015) 179 JP 399 at [16].

9 *Hargreaves v Brecknock and Radnorshire Magistrates' Court* [2015] EWHC 1803 (Admin), (2015) 179 JP 399 at [32].

10 Search Warrants (2018) Law Commission Consultation Paper No 235, paras 4.29 to 4.35.

11 Consultation Question 9.

(1) the lack of prescribed application forms causes problems in practice, and if so, for which search warrant provisions;

(2) in principle, bespoke application forms should be prescribed for all search warrant provisions;

(3) bespoke application forms should be prescribed for only the most common types of warrant;

(4) there should be generic application forms not linked to particular types of warrant; or

(5) there should be no prescribed forms, and applicants should simply set out all the relevant information in narrative form.

Consultation responses

4.14 Twenty-three consultees[12] answered these questions concerning application forms. Below, we consider their responses under the following headings:

(1) whether there are problems in practice resulting from the lack of prescribed forms; and

(2) the number of application forms there ought to be.

Problems in practice

4.15 Some consultees were not aware of problems in practice resulting from the lack of prescribed forms.[13] The Magistrates Association conducted a survey of their members and reported that 74% of respondents said they did not feel the lack of prescribed forms caused problems in practice. However, most respondents said that the police forces in their respective areas did use the prescribed forms.

4.16 Kent County Council Trading Standards considered that problems arose from there being no application forms for entry warrants under the Consumer Rights Act 2015 ("CRA"). While the application form designed for warrants to which sections 15 and 16 of PACE apply ("the sections 15 and 16 of PACE form") can be modified when applying for an entry warrant, the questions asked by the form focus on search and are therefore ill-suited to entry warrants. This view was also expressed by the Association of Chief Trading Standards Officers, who considered that an entry warrant application form would be beneficial.

The numbers of forms

4.17 Consultees disagreed over whether it would be better to prescribe a bespoke application form for each warrant type or to have generic forms which can be tailored to suit the warrant

---

12 Criminal Procedure Rule Committee; Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Birmingham Law Society; West London Magistrates' Bench; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; The Law Society; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Serious Fraud Office; Competition and Markets Authority; Members of the Senior Judiciary; Financial Conduct Authority.

13 Council of Her Majesty's Circuit Judges; Bar Council and the Criminal Bar Association.

being applied for. The majority considered that application forms should be prescribed for all search warrant provisions.[14] Some of the reasons provided for this were:

(1) application forms are a useful guide for applicants and those issuing warrants;[15]

(2) application forms allow applicants to explain why the warrant is sought, and encourage consistency and precision;[16]

(3) there is no principled reason why a form could not be devised for each warrant provision;[17]

(4) provided the work is completed in stages, with priority given to the most utilised warrant provisions, creating bespoke forms would not be overly burdensome;[18]

(5) prescribing application forms for each statutory provision reduces the risk that some of the statutory conditions for issuing the warrant will be overlooked, both when the applicant is filling out the form and at the hearing;[19] and

(6) it is undesirable for applicants to adapt forms.[20]

4.18 Some consultees disagreed. For instance, the CPRC considered that although more bespoke application forms might be desirable, one for each of the 176 provisions identified was unlikely to be proportionate.

4.19 The Justices' Clerks' Society favoured bespoke application forms for every warrant provision in theory, but understood the arguments for only prescribing forms for the most common types of warrants.

4.20 The Council of Her Majesty's Circuit Judges argued that there should be a generic form which encourages the applicant to tailor the application to the type of warrant being applied for and to the circumstances under which the warrant is sought. They considered that encouraging an applicant to write in narrative form would, at least in part, allay concerns about a tick-box mentality setting in. Several other consultees championed generic forms.[21] One argument presented was that problems stemming from issues such as the duty of candour are not linked to there not being a specific form for each warrant.

Analysis

4.21 Having considered consultees' views, we are not persuaded that bespoke application forms should be created for every search warrant provision. This would be a significant

---

14 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Birmingham Law Society; West London Magistrates' Bench; The Law Society; Magistrates Association; National Crime Agency; Bar Council and the Criminal Bar Association.

15 HM Council of District Judges (Magistrates' Court); Birmingham Law Society; The Law Society.

16 Crown Prosecution Service.

17 HM Council of District Judges (Magistrates' Court).

18 Crown Prosecution Service.

19 Crown Prosecution Service.

20 HM Council of District Judges (Magistrates' Court).

21 National Crime Agency; Metropolitan Police Service; Financial Conduct Authority.

undertaking and the amount of work in doing so would be likely to be disproportionate to the benefit gained, given that many search warrant provisions are used so infrequently, if at all.

4.22 In addition, we consider that many of the issues that arise in the context of applications for warrants will stem not from the fact that there is no bespoke application form, but rather from an applicant's failure to comply with the duty of candour. Such failures can occur even when a bespoke form is used.

4.23 That said, we do not consider that there should *only* be generic forms. There are already a number of specific application forms which successfully guide applicants through the statutory conditions for the warrants to which they apply. These forms were highly praised by stakeholders. Applicants may also be tempted to modify generic forms better to suit the warrant they are applying for, but the case of *Hargreaves* suggests that such modifications carry risk.[22] In addition, there is a risk that investigators who create or modify their own application forms may not base them on the most up-to-date version of the forms issued by the CPRC. Modified application forms may therefore not include recent changes, such as those recently proposed to the declaration form.[23]

4.24 For the above reasons, we regard tailored application forms as more desirable than generic forms. However, we accept that if creating a specific form is not possible or practicable then having a generic form is preferable to there being no form at all.

4.25 Our favoured approach is therefore that advocated by the Justices' Clerks' Society: prescribing application forms for the most common types of search warrant provisions beyond those which have already been prescribed. We regard this as the most proportionate course of action, which still recognises the benefits of bespoke application forms. For the avoidance of doubt, we do not consider the mandatory force of using the forms should be altered: there may be circumstances in which it is desirable to present an application by means other than the prescribed forms.

4.26 We turn now to consider for which warrant provisions application forms should be prescribed. In relation to *search* warrants, we have received no evidence of specific provisions that would benefit from a bespoke form. As for entry warrants, as discussed above, Kent County Council Trading Standards considered that problems flowed from there being no prescribed application form for entry warrants under the CRA. This problem was also acknowledged by the Association of Chief Trading Standards Officers. Notably, it was an entry warrant under trading standards legislation that gave rise to the case of *Hargreaves*:[24] the Divisional Court quashed a Trading Standards entry warrant due to the improper modification of an application form meant for a search warrant.

4.27 Kent County Council Trading Standards' own practice indicates that search warrant forms are still being adapted to apply for entry warrants. This practice risks causing errors when applying for an entry warrants, given the different purposes and statutory conditions for search warrants and entry warrants. We therefore see good reason to prescribe application forms specifically for entry warrant applications.

---

22 *Hargreaves v Brecknock and Radnorshire Magistrates' Court* [2015] EWHC 1803 (Admin), (2015) 179 JP 399. See para 4.8 above.

23 See para 4.119 below.

24 *Hargreaves v Brecknock and Radnorshire Magistrates' Court* [2015] EWHC 1803 (Admin), (2015) 179 JP 399. See para 4.8 above.

4.28 While we do not have quantitative data to confirm this, consultees' responses suggest that the most frequently sought entry warrants are those under the CRA.[25] Therefore, it is our view that there should be a bespoke entry warrant application form for entry warrants under the CRA.

4.29 The legislative regime for entry warrants under the CRA applies not only to Trading Standards officers, but also to a number of other enforcement agencies, including the Competition and Markets Authority ("CMA"). The CMA did not agree that there should be a prescribed form for their warrant applications, commenting as follows:

> In the CMA's experience, the best way of presenting the relevant facts and considerations, as well as discharging the CMA's duty of full and frank disclosure, and ensuring that all relevant matters are fully considered by the court, is by setting out a comprehensive narrative in writing, the precise form and structure of which will vary from case to case. The CMA does not consider that the creation of prescribed application forms would assist in the case of CMA warrants. In fact, there is a risk that the creation of prescribed forms, unless specifically designed for the purpose of the legislation under which the warrant is being sought, may increase the risk that one or more of the requirements for a warrant may be overlooked.

4.30 We have considered the CMA's arguments, but we do not consider that the creation of an application form for entry warrants sought under the CRA would have a negative impact on the CMA as it would be "specifically designed for the purpose of the legislation" to ensure that none of the requirements for a warrant are overlooked. In addition, we are not recommending that using an application form, even one designed for a particular provision, would be compulsory when applying for a warrant. Therefore, those agencies who do not currently use an application form would not be required to alter their current practice. That said, we are of the view that using a tailored form, which prompts the applicant to consider all of the relevant legal and procedural requirements, will be preferable in the majority of cases.

4.31 Another important consideration is whether the CPRC has the power to prescribe a form for a warrant under the CRA. We understand that the Committee is likely to only have the power to prescribe forms relating to criminal investigations. As with several warrant provisions, a warrant under the CRA may be obtained for the purpose of a criminal or civil investigation. For example, a warrant may be sought as part of an investigation into an offence under regulations 8 to 12 of the Consumer Protection from Unfair Trading Regulations 2008/1277.

4.32 There are, of course, several other entry warrant provisions.[26] To capture these warrants, we see value in there being an additional generic entry warrant application form which is sufficiently broad to be completed by applicants. This would mirror the position with search warrant applications where there is a specific form for the most common warrants and a generic form for those instances where a different warrant is sought.

4.33 Beyond entry warrants, we have received no firm evidence of other provisions which would benefit from bespoke application forms. Accordingly, we make no further recommendations.

---

25 See para 32, sch 5.

26 Search Warrants (2018) Law Commission Consultation Paper No 235, para 3.30.

Recommendation 10

4.34 We recommend that the Criminal Procedure Rule Committee consider designing two entry warrant application forms:

(1) a specific entry warrant application form for applications under paragraph 32 of schedule 5 to the Consumer Rights Act 2015; and

(2) a generic entry warrant application form which can be modified for other entry warrant provisions.

CONTENT OF APPLICATION FORMS AND THE DUTY OF CANDOUR

The current law

4.35 When applying for a warrant, an applicant must make full and frank disclosure of all matters which may influence the court's decision. This includes disclosing any circumstances that might undermine the application and therefore militate against the search warrant being issued. This is referred to as the "duty of candour". As a common law duty, the duty of candour derives from a large body of case law but is not expressed in any statute.[27] Failure to comply with the duty of candour can lead to a warrant being quashed on judicial review.[28]

4.36 The CrimPR and CrimPD make reference to the duty of candour, which we set out at paragraph 5.9 below, where we examine the duty beyond its expression on application forms. Search warrant application forms currently prompt the applicant to provide any information that might undermine the application. In full, the section provides:

> Is there anything of which you are aware that might reasonably be considered capable of undermining any of the grounds of this application, or which for some other reason might affect the court's decision? Include anything that reasonably might call into question the credibility of information you have received, and explain why you have decided that that information still can be relied upon. …
>
> Information that might undermine any of the grounds of the application must be included in the application, or the court's authority for the search may be ineffective. The court will not necessarily refuse to issue a warrant in every case in which there is information that undermines the grounds of the application.
>
> The applicant must explain why information is thought to be credible where it comes from a source that cannot be tested (for example, a report from an anonymous informant).

---

27 *R v Lewes Crown Court ex parte Hill* (1991) 93 Cr App R 60, 69 by Bingham LJ; *R (Energy Financing Team) v Bow Street Magistrates' Court* [2005] EWHC 1626 (Admin), [2006] 1 WLR 1316, 1325 by Kennedy LJ; *R (Rawlinson and Hunter Trustees) v Central Criminal Court* [2012] EWHC 2254 (Admin), [2013] 1 WLR 1634; *R (Golfrate Property Management Ltd) v Southwark Crown Court* [2014] EWHC 840 (Admin), [2014] 2 Cr App R 12 at [25]; Adam Craggs, "Golfrate Property Management: applicants for search warrants" (2014) 1237 *Tax Journal* 13.

28 *R (Daly) v the Commissioner of Police of the Metropolis* [2018] EWHC 438 (Admin), [2018] 1 WLR 2221 at [33] by Sir Brian Leveson P.

The applicant must inform the court if there is anything else that might influence the court's decision to issue a warrant. This may include whether the premises have been searched before, and with what outcome, or whether there is any unusual feature of the investigation or of any potential prosecution.

4.37 The Divisional Court has made clear that compliance with the duty of candour is not met by simply providing information in a discursive mass.[29]

The consultation paper

4.38 In our consultation paper, we provisionally proposed a series of amendments to the content of application forms. Our aim was to make the forms clearer and more accessible, to help applicants to fill them in correctly. We concentrated in particular on how amendments could assist applicants to fulfil their duty of candour.

The duty of candour

4.39 Reported cases and preliminary discussions with stakeholders revealed that the failure to discharge the duty of candour is a frequent ground of challenge and arises regularly in practice. Recognising the risk of applicants simply providing information as a discursive mass, we suggested that search warrant application forms ought to include specific questions to help applicants to satisfy their duty of full and frank disclosure.

4.40 To assist in ensuring compliance with the duty of full and frank disclosure, we provisionally proposed[30] that search warrant application forms should require the applicant to provide details, if applicable, of:

(1) any previous search warrant applications for the same premises, and pertaining to the same investigation, of which they are aware;

(2) whether there is any reason to suspect that legally privileged material may be on the premises;

(3) the agency which it is intended will be responsible for any prosecution of the suspected offence; and

(4) any known circumstances which might weigh against the warrant being issued.

Other amendments to application forms

4.41 Additionally, we observed that search warrant application forms currently ask the applicant to estimate how long the court is likely to need to consider the application. However, the form does not provide a space to record how long considering the application actually took. The time taken is information which the occupier might reasonably request, as it is a potential indicator of how thoroughly the court scrutinised the application.[31] For this reason, we provisionally proposed[32] that all search warrant application forms should be amended to

---

29 *Fitzgerald v Preston Crown Court* [2018] EWHC 804 (Admin) at [20].

30 Consultation Question 12.

31 *Sweeney v Westminster Magistrates' Court* [2014] EWHC 2068 (Admin), (2014) 178 JP 336; *R (Chatwani) v National Crime Agency* [2015] EWHC 1283 (Admin), [2015] ACD 110.

32 Consultation Question 10.

require the issuing authority to record the time taken to consider the application. This should be divided into the time taken for pre-reading and the hearing itself.

4.42 We also invited[33] consultees' views on how else search warrant application forms ought to be amended.

Consultation responses

The duty of candour

4.43 In respect of the amendments we provisionally proposed to assist with the duty of full and frank disclosure, 25 consultees responded: 18 agreed;[34] and 17 (including some who agreed) suggested modification or other information.[35]

Other amendments to application forms

4.44 In respect of our provisional proposal to require the recording of the time taken by the issuing authority to consider the search warrant application, 21 consultees responded: 13 agreed;[36] seven disagreed;[37] and one expressed another view.[38]

4.45 Some consultees discussed amendments to application forms in respect of electronic material. We discuss these comments in Chapter 15 in the context of Consultation Question 56, which asked questions specifically about electronic material.[39]

Summary of consultation responses

4.46 We received a large volume of comments from consultees. This stems from the fact that we asked three consultation questions regarding the content of application forms, one of which was an open question inviting views generally on how application forms should be amended. As a result, we have categorised consultation responses into two broad headings which we discuss in our analysis. First, those consultation responses relating to the duty of candour. Secondly, those consultation responses relating to other amendments to application forms.

---

33 Consultation Question 10.

34 Robert Della-Sala JP; Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Insolvency Service; Birmingham Law Society; West London Magistrates' Bench; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; The Law Society; Southern Derbyshire Magistrates' Bench; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; National Crime Agency; Metropolitan Police Service; Financial Conduct Authority.

35 Nigel Shock JP; Crown Prosecution Service; Kent County Council Trading Standards; Insolvency Service; Birmingham Law Society; Southern Derbyshire Magistrates' Bench; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Serious Fraud Office; Competition and Markets Authority; Members of the Senior Judiciary; Privacy International.

36 Professor Richard Stone; Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Insolvency Service; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; The Law Society; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Financial Conduct Authority.

37 Criminal Procedure Rule Committee; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Justices' Clerks' Society; Magistrates Association; Serious Fraud Office.

38 Competition and Markets Authority.

39 See paras 15.83 to 15.118 below.

4.47 The topics discussed by consultees relating to the duty of candour were:

(1) the scope of the duty;

(2) previous applications;

(3) associated powers which may be exercised;

(4) the intended prosecutor;

(5) the type of premises to be searched;

(6) the anticipated timing of the search;

(7) the suspected presence of legally privileged material on the premises;

(8) the evidence of good character of the owner or occupier;

(9) the conduct of the occupier;

(10) the presence of children or vulnerable persons; and

(11) the reliability of informants.

4.48 The topics discussed by consultees relating more generally to the amendment of application forms were:

(1) guidance on completing the application form;

(2) confirming the applicant's detailed knowledge;

(3) recording the time taken to consider an application; and

(4) a greater opportunity for the issuing authority to provide reasons.

Analysis

Factors relevant to discharging the duty of candour

4.49 The sheer number of suggestions by consultees concerning the duty of candour indicates how many relevant factors there can be when considering whether to issue a search warrant. We remain of the view that search warrants must be capable of being obtained quickly, as stated recently by the Supreme Court.[40] Therefore, application forms must strike a balance between being capable of completion within a reasonable time and allowing for enough information to be provided to discharge the duty of candour. We are also conscious that application forms should not become overlong or over-prescriptive.

4.50 In relation to the duty of candour, there are countless factors which may be relevant when discharging this duty. As noted above, search warrant application forms generally include

[40] *R (Haralambous) v Crown Court at St Albans* [2018] UKSC 1, [2018] AC 236 at [15]. Discussed in *R (Hafeez) v Southwark Crown Court* [2018] EWHC 954 (Admin), [2018] ACD 46 at [13].

specific question boxes prompting information and notes for guidance for applicants.[41] The Serious Fraud Office ("SFO") and the Crown Prosecution Service ("CPS") considered that search warrant application forms should include a non-exhaustive list of factors relevant to the duty of candour, rather than specific questions. The CPS suggested that these could then be explicitly addressed by the applicant in a tick-box way.

4.51 In our view, application forms should contain an extensive, but non-exhaustive, list of factors which could be relevant to the duty of candour. Although a matter for the CPRC, we consider that this list of factors should be included within the guidance notes of application forms, although some might appropriately be included as questions in the form. We are of the view that this would prevent the application process from becoming a tick-box exercise, a concern expressed by several consultees.[42]

4.52 In the section which follows, we discuss the factors relevant to discharging the duty of candour which were identified by consultees. We recommend that the CPRC consider amending search warrant application forms to contain guidance on the factors which could be relevant to the duty of candour. However, we are not making specific recommendations as to exactly what those factors are, or how the guidance should be worded, as we consider that those are more appropriately matters for the CPRC.

4.53 We nonetheless set out the factors identified by consultees to inform the CPRC in its considerations.

Recommendation 11

4.54 We recommend that the Criminal Procedure Rule Committee consider amending search warrant application forms to include within the guidance notes an extensive (but non-exhaustive) list of factors which could be relevant to discharging the duty of candour. Some of the factors may also lend themselves to specific questions; where this is appropriate these should be included in the application form.

The scope of the duty of candour

4.55 We provisionally proposed including a question on the application form asking if there are any known circumstances which might weigh against the warrant being issued. Virtually all consultees agreed. Some consultees considered that this was already addressed by the question in the existing forms which requests any information that might reasonably be considered capable of undermining the application or affecting the court's decision.[43] That said, it was acknowledged that there is scope to expand on and clarify the duty of candour. Suggested modifications were to:

41 See the search warrant forms prescribed under the Criminal Procedure Rules at: http://www.justice.gov.uk/courts/procedure-rules/criminal/forms#Anchor11.

42 Magistrates Association; Council of Her Majesty's Circuit Judges.

43 National Crime Agency; The Independent Office for Police Conduct.

(1) make clear that the duty of full and frank disclosure is a continuing duty and persists following an application hearing where new matters come to light;[44]

(2) replace the current wording, which refers to "known circumstances", with a test which focuses on whether all relevant information has been disclosed;[45] and

(3) amend the current wording, which refers to "known circumstances", to require something less than knowledge.[46]

4.56 We agree that the duty of full and frank disclosure is a continuing duty,[47] and that this could be made clearer. However, we are less convinced as to the merits of replacing a requirement that disclosure is limited to "known circumstances". We are concerned that these suggestions would expand the duty of candour from not only those facts which are known by the applicant but to those which ought to be known. In our view, this conflates the duty of full and frank disclosure with the duty to make reasonable inquiries.[48]

4.57 There is, we accept, conflicting case law on this point. The Divisional Court has distinguished between a failure to make full and frank disclosure and a failure to make proper inquiries: an investigator cannot be said to have failed to make full and frank disclosure by failing to reveal something of which they were unaware.[49] More recently, however, the Divisional Court has observed that the duty of candour *does* extend not only to facts known to the investigator but to facts which would have been known if proper inquiries had been made.[50]

4.58 We favour the view, expressed in *R (Superior Import / Export Ltd)*,[51] that the duty of candour and duty to pursue all reasonable lines of enquiry are separate but interlocking duties. In support of this interpretation, we have taken into account previous formulations of the duty of candour.[52] The recent case of *National Crime Agency v Baker* is also instructive, in which Lang J discharged three unexplained wealth orders, finding that while there had not been material non-disclosure, the National Crime Agency's case was flawed by inadequate investigation into obvious lines of enquiry.[53]

---

44 These comments were made during a roundtable held with the senior judiciary.

45 Birmingham Law Society.

46 Justices' Clerks' Society; Dijen Basu QC.

47 See *JSC BTA Bank v Ablyazov* [2018] EWHC 259 (Comm).

48 Such a duty is imposed by virtue of the Criminal Procedure and Investigations Act 1996, s 23. Code B of PACE (2013) para.3.3 also requires an officer to make reasonable inquiries to establish whether the premises has been searched previously and, if so, how recently.

49 *R (Superior Import / Export Ltd) v Revenue and Customs Commissioners* [2017] EWHC 3172 (Admin), [2018] Lloyd's Rep FC 115 at [53].

50 *R (Brook) v Preston Crown Court* [2018] EWHC 2024 (Admin), [2018] ACD 95 at [16].

51 *R (Superior Import / Export Ltd) v Revenue and Customs Commissioners* [2017] EWHC 3172 (Admin), [2018] Lloyd's Rep FC 115 at [53].

52 *R (Chatwani) v National Crime Agency* [2015] EWHC 1283 (Admin), [2015] ACD 110 at [106]: "the duty extends to all known information that may be material to the court's decision"; *Fitzgerald v Williams* [1996] QB 657, 667: "In seeking ex parte relief an applicant must disclose to the judge any fact known to him which might affect the judge's decision whether to grant relief or what relief to grant".

53 *National Crime Agency v Baker* [2020] EWHC 822 (Admin) at [217] to [218].

4.59 For these reasons, we see merit in amending the guidance notes of search warrant application forms to clarify the scope of the duty of candour. In particular, guidance could explain that the duty of candour is a continuous duty and covers facts known by the applicant. In our view, this would encourage greater candour on the part of applicants.

Previous applications

4.60 The accompanying guidance appended to search warrant application forms provides:

> The applicant must inform the court if there is anything else that might influence the court's decision to issue a warrant. This may include whether the premises have been searched before, and with what outcome.

4.61 To encourage greater candour, we provisionally proposed that search warrant application forms should require the applicant to specify whether they are aware of any previous search warrant applications concerning the same investigation for the same premises.

4.62 The majority of consultees agreed with the proposal, however, a number of observations were made.

(1) The question should be expanded to cover search warrant applications previously made in respect of the same premises concerning investigations other than the one presently being conducted.[54]

(2) The question should be expanded to cover search warrant applications previously made in connection with a specific individual.

(3) The question should also prompt applicants to state whether any previous applications were granted and, if so, the outcome of the search.[55]

(4) The question is unnecessary as the general duty of full and frank disclosure would oblige an applicant to disclose whether an identical application had been recently refused.[56]

(5) Such a requirement could prove unduly onerous and could create practical difficulties.[57] For example, an investigation into ongoing multi-handed organised crime or terrorism might need a number of inter-related warrants at short notice, due to suspects moving quickly between different premises.[58]

(6) The infrastructure to enable this question to be answered, namely an online database, was unlikely to exist.[59] An agency might only be able to detail its own applications and not ones by other agencies.[60]

---

54 Independent Office for Police Conduct; Crown Prosecution Service.

55 Crown Prosecution Service; Magistrates Association; West London Magistrates' Bench.

56 Bar Council and the Criminal Bar Association.

57 Bar Council and the Criminal Bar Association.

58 Bar Council and the Criminal Bar Association.

59 Robert Della-Sala JP.

60 Insolvency Service.

4.63 We consider, first, the concerns raised by consultees. We do so in the light of the shift in our focus from recommending that direct questions be asked in the application form to recommending that a range of factors be included in guidance. In our view, this justifies examples being put in broader terms.

4.64 We accept that the general duty of full and frank disclosure would already oblige an applicant to disclose whether an identical application had been recently refused. However, it does not follow that this will always in fact be disclosed.[61]

4.65 Our underlying aim is to ensure that applicants are aware of those matters which ought to be disclosed under the duty of candour. In our view, the fact that a previous application was made for the same premises may influence the court's decision to issue a warrant. Therefore, we consider that that this matter should be included in guidance.

4.66 We acknowledge the concerns regarding how onerous the question might be and that in some cases it may not be possible to reach a definitive answer. However, as discussed above, the duty of candour only covers known facts; it is accompanied by a separate duty on criminal investigators to pursue reasonable lines of enquiry. For this reason, we do not consider that the duty would be unduly onerous; it would depend on the particular circumstances whether any previous applications were known.

4.67 Next, we have considered how the example in guidance might be formulated. We agree with all the modifications suggested by consultees as we would be in favour of the example being as widely drawn as possible so that any relevant previous applications would be prompted to be disclosed. For these reasons, we do not consider that the example should be limited to searches pursuant to a warrant; it should apply to any investigative powers exercised. For example, a production order, rather than a warrant, may have been applied for. A search of premises may also have previously been conducted following arrest rather than pursuant to a warrant.

4.68 We also note that this formulation is wider than the one currently contained in search warrant application forms and we therefore consider that it is likely to encourage greater compliance with the duty of candour. Thought should be given to whether this formulation would be too wide if it were to capture applications made under the Investigatory Powers Act 2016 given the sensitivities around the exercise of such powers.

Associated powers which may be exercised

4.69 Responding to the consultation question about how search warrant forms should be amended, the Magistrates Association observed that the power to search for or seize material may arise once an officer is lawfully on the premises, rather than directly from the authority of the warrant. It was suggested that such associated powers should be stated on the application form so that the issuing authority understands the possible implications of warrants being executed. The Financial Conduct Authority ("FCA") also suggested that application forms should include a section to allow applicants to state whether they expect to

[61] *R (Wood) v North Avon Magistrates' Court* [2009] EWHC 3614 (Admin), (2010) 174 JP 157 at [29].

exercise seize and sift powers under section 50 or 51 of the Criminal Justice and Police Act 2001 ("CJPA").[62]

4.70 We see merit in including associated powers in a list of examples as they may influence a court's decision to issue a warrant. The Divisional Court has held that the duty of candour includes a duty to disclose any secondary or incidental purpose which might call into question the dominant purpose of the search.[63] We can see that the planned exercise of other statutory powers may fall within this category or may otherwise affect the decision to issue a warrant.

4.71 However, we do not think that it would be useful simply to list all possible powers which may theoretically be exercised on premises. First, the list of associated powers could be extremely long. Secondly, it may give a misleading impression that all of the powers within an investigator's armoury will be deployed.

4.72 We consider that what would be of greater utility is for an applicant to list only those associated powers which it is reasonably contemplated might be exercised on the premises. For example, this might include their powers under section 50 or 51 of the CJPA. In the case of entry warrants, this may include powers to search and compel the production of information. This would help the issuing authority to focus its mind only on those powers which are likely to be exercised.

The intended prosecutor

4.73 Currently, guidance accompanying application forms states that the duty of candour may include "unusual features of any potential prosecution". We provisionally proposed amending application forms to require the applicant to specify the agency which it is intended will be responsible for prosecuting the suspected offence. This was a matter raised by the Court of Appeal in the context of a private prosecution: the Court considered that the police ought to have disclosed the identity of the intended prosecutor.[64]

4.74 All consultees agreed that the application form should require the applicant to specify the intended prosecution body, even where the intended prosecutor is a state agency. The Bar Council and the Criminal Bar Association saw particular value in the obligation being explicit given that they envisaged the numbers of private prosecutions increasing. Consultees suggested the following modifications to the form to ensure that the most helpful information is provided:

(1) that any question asked should make clear that the duty applies only where the intended prosecutor is known, which may not be the case if, for instance, it is a joint operation;[65] and

(2) that any question asked should prompt the applicant to indicate whether there has been early engagement with a prosecution agency (which is now routine in large or

---

62 These powers allow for material to be seized and sorted through at a later stage because it is not reasonably practicable, during the search, to determine into which category the material falls or to separate the material into what may and may not be seized.

63 *R (Chatwani) v National Crime Agency* [2015] EWHC 1283 (Admin) at [129].

64 *R v Zinga* [2012] EWCA Crim 2357 at [32], [2013] Crim LR 226.

65 Insolvency Service.

complex cases) and whether it is envisaged that the case will result in a private prosecution.[66]

4.75 In our view, it would suffice for the intended prosecutor to be listed as a relevant factor in the guidance, including if it is envisaged that the investigation will result in a private prosecution. If the duty of candour were clarified to make clear that it extends only to those facts which are known, it would be unnecessary to specify that it only applies where the intended prosecutor is known. As for detailing whether there has been early engagement with a prosecutor, while this may be of relevance, we are concerned that this might be an unnecessary level of detail for a non-exhaustive list of examples.

The type of premises to be searched

4.76 The Magistrates Association suggested that there ought to be a section in search warrant application forms for detailed information on the type of property to be searched. The information should include whether the premises is residential or commercial and whether the premises is multi-occupancy.

4.77 We consider that these are matters which may influence the court's decision to issue a search warrant and so their inclusion ought to be considered within accompanying guidance on factors relevant to the duty of candour.

Anticipated timing of the search

4.78 The FCA suggested that search warrant applications should be amended to prompt applicants to provide information about the proposed timing of the search, any collateral intrusion that it is anticipated the search may cause and how such intrusion is to be mitigated.

4.79 We observe that application forms already prompt applicants, at the very beginning, to provide the planned *date* of execution. However, they are not required to specify the proposed timing of the search.

4.80 Again, we consider that these are matters which may influence the court's decision to issue a search warrant. We are also of the view that prompting applicants to specify the proposed timing of the search would encourage the applicant and the issuing authority to consider whether the warrant will be executed at a reasonable hour, as required under section 16(4) of PACE. We accept that, in some cases, this is a matter which may be dictated by operational matters which are not known at the time of applying for a search warrant. We note too that this matter may lend itself better to a direct question rather than set out in guidance.

Suspected presence of legally privileged material on the premises

4.81 Most application forms ask the applicant to record whether the material sought is or contains legally privileged material. This is because the court cannot issue a warrant to search for items subject to legal privilege, unless they are held with the intention of furthering a criminal purpose.[67]

---

66 Bar Council and the Criminal Bar Association.

67 Police and Criminal Evidence Act 1984, s 10(2).

4.82 We provisionally proposed[68] that application forms should ask the applicant to record whether any reason exists to suspect that legally privileged material may be on the premises, irrespective of whether it falls within the scope of the material actually *sought* under the warrant.

4.83 The majority of consultees agreed, however, some consultees considered that the question was unnecessary given that most application forms already require the applicant to specify whether the material sought is or contains legally privileged material.[69] The Metropolitan Police Service ("MPS") considered that the question should remain limited to whether any of the material sought under the warrant is legally privileged, otherwise investigators would be required to consider material that might be on the premises but which relates to other aspects of a person's life, such as divorce proceedings.

4.84 Other consultees suggested modifications to our proposed formulation. The Magistrates Association suggested that application forms should include questions relating to other categories of information for which the applicant may be prohibited from searching, namely excluded and special procedure material. The Independent Office for Police Conduct (IOPC) suggested that all search warrant application forms should include a question about whether legally privileged material falls within the scope of the warrant, to ensure that applicants can demonstrate to the court that they have addressed their minds to the issue.

4.85 There are, as we see it, two separate issues which emerge from consultees' comments:

(1) the strict requirement on an application form to state whether the material sought consists of or includes material which cannot be searched for under the main search power; and

(2) what guidance, if any, should be appended to search warrant application forms relating to material which cannot be searched for under the main search power.

4.86 First, we consider that whether the material sought is or contains protected categories of material is a question which should be addressed on all application forms.

4.87 At present, the only application form which does not ask a specific question about the presence of legally privileged material is the sections 15 and 16 of PACE form. All other application forms contain questions about whether the material sought consists of or includes privileged material, and some forms also make reference to excluded and special procedure material.

4.88 For example, the application form designed for warrants sought under section 8 of PACE requires the applicant to disclose any reasons they are aware of for thinking that the material for which they wish to search consists of or includes items subject to legal privilege, excluded material or special procedure material. This reflects the exclusion of all such material from searches under section 8(1)(d) of PACE. By contrast, for example, excluded and special procedure material can be searched for under section 2 of the Criminal Justice Act 1987 and schedule 5 to the Terrorism Act 2000. Therefore, those forms do not prompt the applicant to state whether the material consists of or includes special procedure or excluded material.

---

68 Consultation Question 12.

69 National Crime Agency; Metropolitan Police Service.

4.89 The sections 15 and 16 of PACE form does not require applicants to provide information regarding protected material and only makes reference to legally privileged material in the guidance. This is because the extent to which an applicant may be permitted to search for protected material will depend on the type of warrant for which they are applying.

4.90 We nonetheless consider that an appropriate form of words could be included in the sections 15 and 16 of PACE form in the question box regarding the articles or person(s) sought. A possible form of words might be:

> Is there any reason to suspect or believe that the material sought consists of or includes material which cannot be searched for under the main search power (such as legally privileged material, excluded material or special procedure material)?

4.91 In our view, including a question along these lines would be beneficial as it would serve to encourage applicants to consider the presence of protected categories of information and any necessary arrangements to protect confidentiality.

4.92 Finally, we consider whether it is desirable to amend the guidance in search warrant application forms in respect of protected material.[70] There are three circumstances under which protected material will be a relevant consideration during the application process. These are:

(1) where protected material is the material actually sought under the warrant;

(2) where protected material is not sought under the warrant but is likely to be encountered; and

(3) where protected material is neither sought under the warrant nor likely to be encountered during its execution, but it is on the premises to be searched.

4.93 We agree that in some cases it will be particularly onerous for an applicant to consider what other forms of protected material may be on premises, other than the material sought or likely to be encountered. In addition, we acknowledge that the presence of some forms of protected material, such as material relating to divorce proceedings, on the premises is unlikely to be of any relevance to the issuing authority deciding whether to grant a warrant.

4.94 All application forms require applicants to specify the material to be searched for. In addition to this, we are of the view that it is also relevant for the applicant and the issuing authority to consider what material is likely to be encountered. For this reason, we see value in accompanying guidance focusing on material which may be encountered by asking what arrangements, if any, are to be put in place regarding protected material which may be encountered during the search.

4.95 For example, when searching internet-enabled electronic devices, investigators are likely to encounter and seize data which is not sought under the warrant and is exempted from the search. A lawyer's phone is a paradigm example, as it will be likely to contain legally privileged material. We consider it crucial that an investigator makes full and frank disclosure of what arrangements, if any, are to be put in place regarding such material.

---

[70] We use the term "protected material" as a general term to cover all those categories of material that may not be the subject of a search warrant under the relevant search warrant provision concerned.

The existence of good character

4.96 The CPS considered that the occupier's good character is an example of a relevant factor which the court should always take into account when deciding whether to issue a warrant. Robert Della-Sala JP, a serving magistrate, also stated that when hearing applications for warrants he typically asks for information regarding the character of the owner or occupiers of the premises.

4.97 The National Crime Agency, in their review of all warrants and orders obtained in ongoing prosecutions, identified as a common issue a failure to state that the subject of the warrant and/or occupier of the premises are of previous good character.[71]

4.98 On reflection, we consider that this is better expressed as the absence of any record of bad character. We see merit in the absence of any record of bad character being included in a list of factors relevant to the duty of candour. In terms of how this should be formulated, one option may be to seek parity with the definition of "bad character" in section 112 (and section 98) of the Criminal Justice Act 2003. This is defined as having a disposition towards "misconduct", namely the commission of an offence or of other reprehensible behaviour. However, in our view, this is not the most helpful definition given that it is prone to ambiguity.[72] For this reason, a preferable formulation may be the disclosure of the absence of recorded convictions or cautions.

Conduct of the occupier

4.99 A common precondition for applying for a warrant is that there is no reasonable prospect that the material which is the subject matter of the warrant could be obtained by other means, such as simply asking the owner for it. Therefore, the CPS suggested that search warrant application forms should also address the conduct of the occupier, including occasions on which they have previously cooperated with investigators.

4.100 We consider that this would be a sensible addition to the non-exhaustive list of factors. If an occupier has previously cooperated with an investigation, this would clearly be relevant to the question of whether entry to the premises would be likely to be granted without a warrant. In addition, if the occupier has previously given an account or explanation for something during discussions with an agency, this may cast doubt on any allegation they face.

4.101 Failure to detail previous co-operation has led to warrants being quashed.[73] In *Dulai*, for example, Essex County Council were granted entry to the claimant's premises on seven previous occasions and provided with relevant documentation in relation to the offence which they were investigating, which was not disclosed to the issuing authority.

Presence of children or vulnerable persons

4.102 The Magistrates Association and Birmingham Law Society both suggested that there ought to be an opportunity on application forms for applicants to provide detailed information on who (other than any named individual) may be present at the premises. They suggested that the form should invite applicants to disclose information which includes the following:

---

71 National Crime Agency, *Warrant Review Closing Report* (March 2016).

72 *R v Palmer* [2016] EWCA Crim 2237.

73 *R (Dulai) v Chelmsford Magistrates' Court* [2012] EWHC 1055 (Admin), [2013] 1 WLR 220 at [46] by Stanley Burnton LJ; *R (Hart) v Blackfriars Crown Court* [2017] EWHC 3091 (Admin), [2018] Lloyd's Rep FC 98.

(1) whether children or vulnerable adults are likely to be present;

(2) if the property is commercial, whether staff or customers are likely to be present; and

(3) if so, the steps to be taken to address their presence during the execution of the warrant.

4.103 We agree that the above matters are important and may influence a court's decision as to whether to issue a warrant. The presence of children, vulnerable adults or staff or customers may also affect what may be considered to be a "reasonable hour" for any warrant to be executed, as required by section 16(4) of PACE.

Reliability of informants

4.104 Sometimes an application for a search warrant will be based on information provided by an informant. Where an informant may not be completely reliable, this is a matter that we consider must be disclosed under the duty of candour. However, such information is clearly sensitive and would need protection.

4.105 The Magistrates Association argued that where an informant has provided intelligence relied upon in an application there ought to be a section where information on the informant can be recorded. They suggested that the following details could be included.

(1) Is the informant registered as such with the local police force?

(2) Has the informant previously provided information used in search warrant applications?

(3) Is there evidence of the reliability of the informant?

(4) Is the informant paid?

The West London Magistrates' Bench also suggested that applicants should indicate the quality grading[74] of the informant.

4.106 We agree that these matters may influence a court's decision to issue a warrant. We hesitate slightly regarding the provision of payment to an informant as payment appears an equivocal indicator of the reliability of the information.

4.107 Given the inherent sensitivity of this information, care would have to be taken with how the information was prompted. Rule 47.26(4) of the CrimPR provides that an applicant may identify information which they contend ought not to be supplied to anyone but the court.

4.108 In Chapter 8 of this report, we endorse the observation of the Supreme Court in *Haralambous* that, whenever practicable, sensitive information should be recorded on a separate sensitive material schedule, pursuant to rule 47.26(4) of the CrimPR.[75] We therefore see value in including a prompt on the application form for applicants to include any sensitive material in a separate schedule.

---

74 Some agencies having grading for informants, for example, A = always reliable; B = mostly reliable; C = sometimes reliable, etc.

75 *R (Haralambous) v Crown Court at St Albans* [2018] UKSC 1, [2018] AC 236 at [27].

4.109 Answers to the questions set out at paragraph 4.104 above are likely to be highly sensitive and, as such, an applicant is unlikely to want to disclose them to an occupier, who is entitled to request a copy of the application form. Were such a request made by an occupier, the investigator would be entitled to seek a ruling from the court that the sensitive material schedule should not be disclosed because doing so would not be in the public interest.[76] We discuss how this procedure operates in Chapter 8 of this report.

Other amendments to application forms

4.110 The remainder of this section addresses the topics to which we referred to paragraph 4.48 above which relate more generally to the amendment of application forms rather than the duty of candour.

Guidance on completing the application form

4.111 The Magistrates Association argued that it would assist the police if application forms were accompanied by more guidance. The following were specific suggestions as to what that guidance should include.

(1) Guidance as to the detail required in identifying items to be searched for. This was said to be most important in relation to electronic material. For instance, guidance should explain that an application for "all computer equipment and mobile phones on premises" was likely to be considered too wide and generic: the applicant should be specific about what is being sought.

(2) A checklist, to be gone through before submitting an application, to make sure no necessary information is missed.

(3) A reminder to those making the application that the issuing authority may request additional information, so they should be prepared to answer any questions.

(4) A general reminder that jargon or abbreviations should not be used. Echoing this concern, the Council of Her Majesty's Circuit Judges had no views on how forms should be amended save that they should be written in plain English.

4.112 Taking these suggestions in turn, the material an applicant intends to search for, whether electronic devices or not, must always be described in as much detail as possible. However, a search warrant couched in broad terms may be permissible in complex and/or urgent investigations. We therefore do not consider it helpful to provide examples of how search warrants should be drafted. Further, the guidance attached to search warrant application forms already makes clear that the applicant must explain what the search is for in as much detail as is practicable, as does Code B of PACE.

4.113 Nor do we consider a checklist to be necessary. If each of the application form boxes are filled out adequately and the duty of candour is complied with, no necessary information should be missed.

4.114 We see value in reminding applicants that the issuing authority may request additional information, and they should be prepared to answer any questions. Although already in statute,[77] this would encourage full and frank disclosure and highlight the importance of the

---

[76] Also known as claiming "public interest immunity".

[77] Police and Criminal Evidence Act 1984, s 15(4).

applicant having sufficient knowledge of the investigation. Several consultees explained that applicants are sometimes sent away by the court because they are unable to satisfactorily answer questions asked during an application hearing. This wastes both the investigator and the court's time.

4.115 We also see value in guidance reminding applicants that jargon or abbreviations should not be used. We acknowledge that abbreviations become commonplace within agencies, but familiarity with those abbreviations should not be expected of issuing authorities. Where the applicant has to explain terms used, this will slow the application process down.

4.116 For these reasons, we suggest that the CPRC consider amending the guidance notes in search warrant application forms to include:

(1) a reminder that the issuing authority may request additional information and that the applicant should be prepared to answer any questions asked; and

(2) a reminder that jargon or abbreviations should be avoided.

Confirming the applicant's detailed knowledge

4.117 All search warrant applications currently have to be authorised by a senior officer.[78] HM Council of District Judges (Magistrates' Courts) highlighted that this supervision is not as effective as it could be. They suggested that the authorising officer should be required to confirm not only that they have reviewed and authorised the application, but that the applicant has a detailed understanding of the information provided in the application. They also suggested that guidance on this "gatekeeping role" be provided by way of notes attached to the application form.

4.118 We see the value in these suggestions. The Independent Office for Police Conduct ("IOPC") has recently recommended that the CPRC consider amending search warrant applications to require the authorising officer to confirm:

(1) that all relevant information is contained within the warrant to the best of their knowledge and belief; and

(2) that the possibility there may be evidence, intelligence or other matters that might reasonably be considered capable of undermining the application has been considered, and relevant assurances have been sought from the applicant.[79]

4.119 In their response to the IOPC's recommendation, the CPRC considered a reformulation of the requirement imposed on an authorising officer by rule 47.26(5)(b) of the CrimPR and by the 21 application forms for search warrants and other investigatory orders. The Committee has made a recommendation to the Lord Chief Justice to amend the application forms along the lines suggested by the IOPC.

4.120 While this should assist in ensuring that applicants are able to answer questions adequately, there is an argument that more could be done. In particular, we note that none of the changes proposed to the application forms require an authorising officer to confirm that they

---

78 Code B of PACE (2013) para 3.4.

79 Independent Office for Police Conduct, *Operation Kentia: A report concerning matters related to the Metropolitan Police Service's Operation Midland and Operation Vincente* (October 2019), p 26.

are satisfied that the applicant has the ability to answer on oath any questions asked, as is required of an applicant under section 15(4) of PACE. For this reason, it may be considered desirable to amend the requirement imposed on an authorising officer by CrimPR, rule 47.26(5)(b) and by search warrant application forms to include a declaration that they are satisfied that the applicant has the ability to answer on oath any questions asked.

Recording the time taken to consider an application

4.121 The majority of consultees supported the introduction of a requirement to record the time that was spent considering an application on an application form. The main justification given was that it would help the issuing authority to demonstrate that it had scrutinised the application sufficiently. However, some consultees gave powerful reasons against introducing such a requirement.

(1) The CPRC considered that the different speeds at which different judges worked made it unlikely that such a record would assist and might provoke challenges to the decisions of those judges who work swiftly.

(2) HM Council of District Judges (Magistrates' Court) stated that the time taken to deal with an application is not, in its view, a reflection of the depth of consideration that was given to it.

(3) The CPS considered that it risks undue criticism of efficient decision-makers and undue endorsement of decisions which may have been reached inefficiently.

(4) The Senior District Judge (Chief Magistrate) observed that a magistrates' court's work is spread throughout the day and the judge may receive the application early but deal with it during a break in proceedings or when the applicant has arrived.

4.122 In the light of consultees' views, we no longer consider that an issuing authority should be required to record the time taken to consider an application.

Greater opportunity for the issuing authority to provide reasons

4.123 Search warrant application forms include space for the issuing authority to record both additional information given by the applicant during the hearing and the reasons for issuing, or refusing to issue, the warrant(s). A number of consultees expressed the view that application forms should provide more space for the recording of this information.[80] The reason for this suggestion was that application forms do not currently provide enough space. As a result, the issuing authority may need to append additional sheets.

4.124 We note that this will not be an issue when completing an application form on a computer as the boxes can easily be expanded, however, it may cause problems when an issuing authority has the application printed out.

[80] Magistrates Association; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate).

THE DRAFT SEARCH WARRANT

The current law

4.125 Section 15 of PACE provides detailed requirements for what a search warrant must contain. Under section 15(6)(a) the warrant must specify the name of the applicant; the date on which it is issued; the enactment under which it is issued; and each set of premises to be searched. Crucially, under section 15(6)(b), the warrant must also identify, so far as is practicable, the articles or persons sought. If the warrant authorises multiple entries it must also specify the maximum number of entries permitted, or state that it is for an unlimited number (see section 15(5A) of PACE).

The consultation paper

4.126 In our consultation paper we observed that particular police forces often use standardised forms but there is no central coordination. For this reason, we provisionally proposed[81] that the CPRC should prescribe a standard search warrant template to ensure compliance with section 15(5A) and (6) of PACE. We also sought consultees' views on whether this should be accompanied by non-statutory guidance about the level of detail required on the actual search warrant.

Consultation responses

4.127 Twenty-two consultees addressed this proposal: 19 agreed;[82] one disagreed;[83] and two expressed other views.[84]

4.128 The CPRC informed us that prescribed warrant templates do in fact exist for some types of warrant, but they are not available to the general public for security reasons. Further, the warrant template contains footnoted guidance on how it should be completed.

4.129 However, there is not a template for entry warrants, such as those issued under schedule 5 to the Consumer Rights Act 2015. Kent County Council Trading Standards considered that, ideally, there would also be a template for entry warrants. They shared with us an entry warrant template they have created for this purpose. The Association of Chief Trading Standards Officers also acknowledged that the lack of an entry warrant template was a problem.

4.130 The CMA can also apply for warrants under schedule 5 to the CRA. They pointed out that the Practice Directions for CMA warrants under the Competition Act 1998 and Enterprise Act

---

81 Consultation Question 13.

82 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; The Law Society; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Financial Conduct Authority; Association of Chief Trading Standards Officers.

83 Competition and Markets Authority.

84 Criminal Procedure Rule Committee; Serious Fraud Office.

2002 include a pro forma (standard format) for search warrants issued under those Acts.[85] They did not consider that a standardised approach to all warrants across the enforcement landscape, including the creation of a standard warrant, would be desirable.

Analysis

4.131 While search warrant templates may not be published for security reasons, we would point out that the template simply sets out the information required by statute. The presentation of a search warrant can be viewed by carrying out a simple Google search. Templates for other warrants can also be viewed online.[86] We are also concerned that not all investigators are aware of the existence of search warrant templates.

4.132 A separate concern we have is that investigators are modifying current templates when they are drafting the warrant to be approved by the magistrate, which increases the risk of errors in modification. For this reason, we consider that there should be an entry warrant template to promote consistency and reduce the scope for errors from applicants modifying their own forms.

4.133 We acknowledge the concerns of the CMA; however, their comments were made in the context of a standard search warrant template. We consider that an entry warrant template specifically designed with entry warrants in mind would address these concerns. Further, the template would not prevent them from presenting applications for warrants under the CRA by other means should they wish to do so.

Recommendation 12

4.134 We recommend that the Criminal Procedure Rule Committee consider prescribing a standard entry warrant template.

ONLINE APPLICATIONS PORTAL

The current law

4.135 At present, search warrant application forms are typically downloaded, completed on a computer, and then emailed to the relevant court centre. We discuss the procedure when arranging a search warrant application in detail at paragraphs 5.76 to 5.109 below.

The consultation paper

4.136 In the consultation paper,[87] we asked for consultees' views on whether greater use could be made of an online application portal, which enables applicants to fill in and submit forms

85 See https://www.justice.gov.uk/courts/procedure-rules/civil/rules/appforwarrant and https://www.justice.gov.uk/courts/procedure-rules/civil/rules/appforwarrant_comp_act2002.

86 See https://www.justice.gov.uk/courts/procedure-rules/civil/rules/appforwarrant.

87 Search Warrants (2018) Law Commission Consultation Paper No 235, para 4.35.

online. We invited consultees' views[88] on the value of interactive online application forms which guide the applicant through the relevant questions.

Consultation responses

4.137 Eighteen consultees answered this question: 16 agreed;[89] one disagreed;[90] and one expressed another view.[91] The vast majority of consultees who addressed this question supported an online applications portal.[92] The reasons for their support were summed up well by Dijen Basu QC, who stated:

> In twenty-first century Britain, it seems to me that it should be easy to design a single downloadable interactive form which contains drop down menus which expand/reveal or contract/hide parts of the form which are relevant or irrelevant to a given application. An interactive form could better prompt the applicant to ensure that the appropriate test has been met (e.g. reasonable grounds to suspect or to believe, etc). It could require the positive discharge of the duty of candour by requiring the applicant positively to state that there is nothing which it is necessary to disclose under this head. Such a form could more easily be transmitted to court electronically, triggering reminders to court staff to list the matter before a particular (level of) judge and ensuring that relevant information was readily available. This would also enable electronic monitoring of warrant applications for statistical purposes. The form could require a countersignature – to a suitable declaration – from a senior officer or manager, in order to ensure oversight and accountability.

4.138 The Law Society considered that a secure application portal would make better use of the limited resources available. In particular, it could provide for:

(1) all the necessary templates;

(2) early transmission to the authority considering the application;

(3) the ability to make the application at distance;

(4) the ability for the public to challenge warrants later; and

(5) the recording of reasons.

---

88 Consultation Question 9.

89 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); West London Magistrates' Bench; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; The Law Society; Southern Derbyshire Magistrates' Bench; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Members of the Senior Judiciary; Association of Chief Trading Standards Officers.

90 Financial Conduct Authority.

91 Serious Fraud Office.

92 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); West London Magistrates' Bench; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; The Law Society; Southern Derbyshire Magistrates' Bench; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Members of the Senior Judiciary.

4.139 The SFO had no objection to interactive online application forms but considered that the existing prescribed forms already meet the needs that an online portal would be designed to meet.

4.140 The FCA were not sure what we meant by an "online form that is interactive". Presently, they observed, the form is a structured document that is available to download and amend/populate for submission. The FCA are not presently connected to any shared system which would allow them to complete and submit an online form. They were concerned that many online forms have glitches or other issues, and given the detail and care required when filling out a search warrant application they suggested that a downloadable form is the most practical and safest method. They considered that filling out a structured downloadable template, as they currently do, is sufficiently practical.

Analysis

4.141 The support for online application forms among consultees was clear. However, the issues raised by the SFO and FCA merit further consideration.

4.142 By online application forms, we envisaged an application form that would be hosted and completed online by an investigator making the application. Submission of the form to the relevant court would be via the online portal on which the form was hosted. The online form would prompt applicants to give the relevant information and provide guidance on how to fill out each section. Another possible feature might be that the application form could not be submitted if certain sections were not completed.

4.143 On reflection, we consider that any such programme could also generate draft search warrants. For example, where a search warrant under section 8 of PACE search warrant was applied for, the search warrant template could automatically populate the field requiring the applicant to specify the legislation under which the warrant is sought with section 8 of PACE.

4.144 To give another example, it would be possible for an interactive form to state the expiry date of the warrant, with the precise date being automatically generated once the relevant statute has been selected. Again, if a warrant is sought under section 8 of PACE, then the search warrant template would automatically update itself to state that the warrant is valid for three months from the date of issue. The benefit of this would be more than simple convenience. We have spoken with police officers who have had to obtain legal advice on for how long search warrants under different provisions remain valid. This system could remove such errors and prevent particular defects on the face of the warrant.

4.145 The wider vision of search warrants operating within a digital end-to-end system reflects the broader aspiration of the digitisation of the criminal justice system.[93] One of the ways in which this has been implemented is through what is known as a two-way interface model, which allows the police and CPS to send and receive information from their respective case management systems. There is some evidence of such a system increasing efficiency.[94]

---

93 Ministry of Justice, *Criminal Justice System Digital Business Model* (2014).

94 Criminal Justice Joint Inspection, *Delivering Justice in a Digital Age: a Joint Inspection of Digital Case Preparation in the Criminal Justice System* (2016) para 5.24.

4.146 We have discussed the feasibility of including search warrants within this model with those involved in developing software for the police. We were informed that there is software currently being used by some constabularies which have a search warrants module.

4.147 For example, in their response to IOPC recommendations, the MPS stated that they are introducing a new integrated intelligence system called 'CONNECT' which will ensure a joined-up approach to the issuing of search warrants. It offers an interactive online programme which prompts officers to provide information which populates the relevant fields of a search warrant application form. Once the fields have been populated, however, an officer must "step out" of the system and email the document(s) to the court.

4.148 Therefore, it seems that the technology for online application form software exists and that there is the appetite for an online portal. However, inquiries would have to be made regarding extending the software to agencies other than the police.

4.149 There are also several reasons why it may be difficult to implement an online application portal. First, it is clear from the FCA's response that not every agency would wish to participate in a portal system. However, in our view, if a better and more efficient system can be designed and implemented, then this should be pursued.

4.150 Secondly, in cases of highly sensitive material or extreme urgency, it would likely be preferable for an application to be submitted in person. As to the sensitivity of material, any online applications portal should have adequate security features, including a means by which access is only available to court staff with an appropriate level of security clearance.

4.151 Thirdly, it is not the case that all of the material that is included in a warrant application will always be simple descriptive text: applicants may wish to upload maps or diagrams. However, any reasonably sophisticated system ought to be able to deal with uploading different types of documents.

4.152 We remain of the view that an online application portal would bring several benefits. It would reduce errors, allow better management of applications by court staff and enable the collection of data. The system, however, would require further consultation with relevant agencies and Her Majesty's Courts and Tribunals Service.

4.153 Given the potential for any work in this area to be a significant undertaking, we see an argument for it to be considered as part of a wider project aimed at digitising court applications generally. For example, there would be clear cross-over with applications for production orders and other investigative powers.

Recommendation 13

4.154 We recommend that Her Majesty's Courts and Tribunals Service consider the practicability of designing and implementing an interactive online search warrants application portal.

Chapter 5: Applying for a search warrant

INTRODUCTION

5.1 We considered reform to the content of the documents used when applying for a search warrant in the previous chapter. In this chapter, we consider reform to the wider framework governing the application process. In particular, we discuss the following areas:

(1) clarifying the scope of the duty of candour outside the application forms;

(2) arranging a search warrant application hearing;

(3) the level of knowledge required of an applicant when appearing at a hearing; and

(4) searching premises following arrest instead of applying for a search warrant.

5.2 As the Supreme Court has observed, the scheme for applying for a search warrant is designed to be operated speedily at an early stage in an investigation.[1] We remain of the view that the procedure governing applying for a search warrant ought to be reformed in order to improve procedural efficiency and application quality. Search warrants should be obtainable in a timely manner so that law enforcement agencies can respond quickly to intelligence, effectively investigate crime and protect the public. At the same time, reform must reduce the scope for serious errors, which on occasion have led to criminal investigations collapsing at a huge financial cost, and have caused significant reputational damage and stress to individuals who are the subject of a search.

5.3 The overarching aims of the recommendations in this chapter are therefore to ensure that search warrant applications are completed to a high standard and that the issuing authority is presented with an accurate and complete picture of the investigation. Search warrant application hearings should also be able to be arranged without inordinate delay.

5.4 In Chapter 4, we recommend that search warrant application forms be amended to include within the guidance notes an extensive (but non-exhaustive) list of factors which could be relevant to discharging the duty of candour. In this chapter, we recommend placing the common law duty of candour on a statutory footing to promote greater adherence to the duty of candour. We also recommend that the duty of candour is set out in greater detail in the Criminal Practice Directions ("CrimPD") and Code B of the Police and Criminal Evidence Act 1984 ("PACE").

5.5 We also recommend that all law enforcement agencies take steps to ensure that sufficient training is provided to officers involved in applying for and executing search warrants to ensure that applications are consistently completed to a high standard.

5.6 In addition, we recommend that Her Majesty's Courts and Tribunals Service ("HMCTS") consider the practicability of making more search warrant application hearing slots available,

---

1 *R (Haralambous) v Crown Court at St Albans* [2018] UKSC 1, [2018] AC 236 at [15]. Discussed in *R (Hafeez) v Southwark Crown Court* [2018] EWHC 954 (Admin), [2018] ACD 46 at [13].

or pursuing other measures which would decrease both the length of time it takes to obtain a search warrant and the disruption to other court business.

5.7 To ensure that a person applying for a search warrant has adequate knowledge to answer questions asked by the issuing authority, we also recommend that consideration be given to amending Code B of PACE to include such a requirement.

CLARIFYING THE SCOPE OF THE DUTY OF CANDOUR

The current law

5.8 As discussed in Chapter 4 of this report, when applying for a warrant, an applicant must make full and frank disclosure of all matters which may influence the court's decision. The duty of candour requires an applicant to disclose any circumstances that might undermine the application and therefore militate against the search warrant being issued.[2] Failure to comply with the duty of candour is a frequent ground of challenge to the lawfulness of a warrant.

5.9 As mentioned at paragraph 4.35 above, the duty of candour is a common law duty: it derives from a large body of case law but is not expressed in any statute. Search warrant application forms currently prompt the applicant to provide any information that might undermine the application. The Criminal Procedure Rules ("CrimPR") and CrimPD also reference the duty of candour.

(1) Rule 47.25(4) of the CrimPR provides that the court must not determine an application unless the applicant confirms, on oath or affirmation, that to the best of their knowledge and belief:

(a) the application discloses all the information that is material to what the court must decide, including any circumstances that might reasonably be considered capable of undermining any of the grounds of the application; and

(b) the content of the application is true.

(2) Rule 47.26(3) of the CrimPR provides that the application must disclose anything known or reported to the applicant that might reasonably be considered capable of undermining any of the grounds of the application.

(3) Paragraph 47A.3 of the CrimPD emphasises that applicants for warrants owe the issuing authority duties of candour and truthfulness. Therefore, the applicant must draw the court's attention to any information that is unfavourable to the application.

5.10 It is noteworthy that the duty of candour has been placed on a statutory footing in other settings. For example, a statutory duty of candour is found in paragraph 3(1)(b) of schedule 4 to the Terrorism Prevention and Investigation Measures Act 2011, which provides:

---

2 *R v Lewes Crown Court ex parte Hill* (1991) 93 Cr App R 60, 69 by Bingham LJ; *R (Energy Financing Team) v Bow Street Magistrates' Court* [2005] EWHC 1626 (Admin), [2006] 1 WLR 1316, 1325 by Kennedy LJ; *R (Rawlinson and Hunter Trustees) v Central Criminal Court* [2012] EWHC 2254 (Admin), [2013] 1 WLR 1634; *R (Golfrate Property Management Ltd) v Southwark Crown Court* [2014] EWHC 840 (Admin), [2014] 2 Cr App R 12 at [25]; Adam Craggs, "Golfrate Property Management: applicants for search warrants" (2014) 1237 *Tax Journal* 13.

(1) Rules of court relating to TPIM proceedings or appeal proceedings must secure that the Secretary of State is required to disclose—

(a) material on which the Secretary of State relies,

(b) material which adversely affects the Secretary of State's case, and

(c) material which supports the case of another party to the proceedings.

The consultation paper

5.11 Given that the failure to discharge the duty of candour remains a frequent ground of challenge to the lawfulness of a search warrant, to promote the duty of candour, we made a series of provisional proposals in the consultation paper which related to how the duty of candour is presented on search warrant application forms. We discussed these proposals in Chapter 4 above.

5.12 We also provisionally proposed[3] in our consultation paper that the scope of the duty of candour ought to be made clearer to ensure that investigators comply with their legal duty. We proposed that sources of law be amended to include the duty of candour (making it more accessible) and information be included explaining the scope of the duty (making it more comprehensible).

5.13 We did not propose a method by which the duty of candour should be set out. Instead, we invited[4] consultees' views on whether it ought to be set out in:

(1) primary legislation;

(2) rules of court; or

(3) Code B of PACE.

5.14 We identified several advantages and disadvantages to setting out the duty of candour in each of these ways, which we summarise briefly below. Further, in setting out these different sources, we did not necessarily consider that the duty should be set out only in one source.

5.15 Setting out the duty of candour in statute would demonstrate its fundamental importance when making an application. Section 15(2) of PACE sets out a number of categories of information which an applicant is required to disclose when applying for a search warrant. These include the grounds on which the application is made, the enactment under which the warrant would be issued and, so far as is practicable, the articles or persons sought.

5.16 On one view, the duty of candour is as important as the above categories of information and therefore ought to be in primary legislation. On the other hand, the above categories of information are specific and identifiable. The information which may fall within the duty of candour will be far broader and fact-specific, making it less suited to being set out in primary legislation.

---

3 Consultation Question 11.

4 Consultation Question 11.

5.17 Simply requiring disclosure of material which adversely affects the investigator's case or supports another party's case on the face of the statute would not necessarily make the law more accessible and easier to comply with. Equally, listing categories of information which should be disclosed would make the statute unwieldy. Notably, in the case of the Terrorism Prevention and Investigation Measures Act 2011 cited at paragraph 5.10 above, it is in rules of court that the statute envisages the duty being fully articulated. This lends weight to the view that primary legislation is ill-suited to laying out the scope of the duty of candour, or at least that the duty could only be articulated in general form.

5.18 In addition, enshrining the duty of candour in statute would not necessarily give the duty more force than it currently has as a common law duty. Taking into account the approach adopted by the courts when dealing with breaches of section 15 of PACE, it may make little difference to the conclusion reached by the court when considering a challenge. However, as we have said our aim is for the duty to be more accessible and comprehensible.

5.19 Another option would be to enshrine the duty of candour in the CrimPR, and also in the accompanying CrimPD and Code B of PACE.

5.20 Unlike primary legislation, rules of court and Code B of PACE allow greater flexibility for setting out the scope of the duty of candour. This is because they can be changed more easily and lend themselves better to a more narrative form. The CrimPR, CrimPD and Code B of PACE are also designed to be read by applicants. While the courts' powers to respond to breaches of rules of court or Code B are limited, the duty of candour is also a common law duty, breaches of which may result in the warrant being set aside.[5]

5.21 In addition to where the duty ought to be set out, we also invited[6] consultees' views on whether any text setting out the duty of candour ought to be accompanied by a list of the information which must always, if it exists, be disclosed. We did not attempt to set out exhaustively what this information might be.

5.22 As a result, within Consultation Question 11, there were in effect three sub-questions, namely:

(1) whether, in principle, the duty of candour needs to be made more accessible and comprehensible;

(2) if so, where the duty should be set out; and

(3) whether there should be an accompanying list of information which must be disclosed.

Consultation responses

5.23 Twenty-three consultees[7] answered this question.

---

5 *(Dulai) v Chelmsford Magistrates' Court* [2012] EWHC 1055 (Admin), [2013] 1 WLR 220 at [45] by Stanley Burnton LJ.

6 Consultation Question 11.

7 Criminal Procedure Rule Committee; Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Insolvency Service; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; The Law Society; Southern Derbyshire Magistrates' Bench;

The accessibility and comprehensibility of the duty of candour

5.24 In response to our provisional proposal that the duty of candour ought to be made more accessible and comprehensible:

(1) 21 consultees agreed;[8] and

(2) one disagreed.[9]

5.25 The Crown Prosecution Service ("CPS") considered that the duty of candour ought to be made more accessible so that investigators who comply with it in spirit ensure they do so in the letter of the application. Similarly, the Bar Council and the Criminal Bar Association ("CBA") agreed that steps should be taken to ensure that applicants understand and comply with the duty of candour when applying for a search warrant.

5.26 The Competition and Markets Authority ("CMA") was the only consultee to disagree. They pointed out that their warrant applications were subject to rigorous internal and external scrutiny and, as part of this, the CMA were conscious of the need to comply with the duty of full and frank disclosure.

Where should the duty of candour be set out?

5.27 On the question of where the duty of candour ought to be set out:

(1) eleven considered that it should be set out in primary legislation;[10]

(2) five considered that it should be set out in rules of court;[11] and

(3) eight considered that it should be set out in Code B of PACE.[12]

Enshrining the duty of candour in primary legislation

5.28 The following reasons were given by consultees for enshrining the duty of candour in legislation:

Independent Office for Police Conduct; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Serious Fraud Office; Competition and Markets Authority; Members of the Senior Judiciary; Financial Conduct Authority.

8 Criminal Procedure Rule Committee; Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Insolvency Service; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; The Law Society; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Serious Fraud Office; Members of the Senior Judiciary; Financial Conduct Authority.

9 Competition and Markets Authority.

10 Crown Prosecution Service; Criminal Procedure Rule Committee; HM Council of District Judges (Magistrates' Court); Insolvency Service; Birmingham Law Society; The Law Society; Southern Derbyshire Magistrates' Bench; Justices' Clerks' Society; Dijen Basu QC; Serious Fraud Office; Financial Conduct Authority.

11 Crown Prosecution Service; Senior District Judge (Chief Magistrate); Independent Office for Police Conduct; National Crime Agency; Serious Fraud Office.

12 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Council of Her Majesty's Circuit Judges; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Independent Office for Police Conduct; National Crime Agency; Bar Council and the Criminal Bar Association; Serious Fraud Office.

(1) as a duty of transparency and truthfulness, it is so central to the proper administration of justice that it should be set out in primary legislation;[13]

(2) it is just as important as other safeguards included in section 15 of PACE;[14]

(3) it might reduce the number of applications for search warrants as, on reflection, investigators may decide that a warrant is not necessary;[15] and

(4) the duty should not be "watered down" by secondary legislation.[16]

5.29 Some consultees considered that primary legislation should also include a list of information relevant to the duty of candour.[17] Others considered that primary legislation could be accompanied by guidance and examples in secondary legislation.[18]

5.30 The Serious Fraud Office ("SFO") queried whether statutory codification of the duty of candour would in fact make it more accessible or comprehensible to applicants. In particular, they noted that the statutory definition would have to be brief, meaning that detailed guidance for applicants would still be required elsewhere, particularly to explain the scope of the duty and potentially relevant factors.

5.31 The Financial Conduct Authority ("FCA") agreed that there would be benefits to enshrining the duty of candour in primary legislation provided an appropriately clear, practical and limited definition could be drafted to avoid encouraging inappropriate challenges. In its view, that definition should do no more than reflect the current law.

5.32 The Bar Council and the CBA doubted the need for primary legislation for several reasons. They observed that the issuing authority has to consider factors both for and against the granting of the warrant in relation to each of the statutory criteria. The general duty of the applicant to inform the court and not to mislead, thereby presenting a fair and balanced picture, would encompass the presentation of information that might undermine as well as that which would support the application.

5.33 The Bar Council and the CBA also observed that scenarios will arise where individuals disagree over whether certain information might undermine a case. Further, there will be cases where information not disclosed would have undermined the application but would not have made a material difference to the outcome. For example, the fact that a suspect in a serious organised crime network has no previous convictions is unlikely to make a material difference to the decision to issue a warrant. If this were not disclosed, it would likely be disproportionate to render the warrant unlawful and deem the material seized following execution unlawfully obtained, especially as this would give rise to admissibility arguments at trial.

---

13 Crown Prosecution Service; Insolvency Service; Birmingham Law Society; Law Society.

14 Crown Prosecution Service.

15 HM Council of District Judges (Magistrates' Court).

16 Birmingham Law Society.

17 Southern Derbyshire Magistrates' Bench; Dijen Basu QC.

18 Law Society.

Enshrining the duty of candour in rules of court

5.34 Other consultees made the case for including the duty of candour in rules of court. The Senior District Judge (Chief Magistrate) considered that rules of court could make the duty of candour clearer. The National Crime Agency ("NCA") considered that the duty of candour ought to be better defined where it currently appears in both the rules of court and Code B of PACE. They also suggested that the definition should be accompanied by guidance which includes a non-exhaustive list of examples.

5.35 The SFO was of the view that the duty of candour could helpfully appear in Part 47 of the CrimPR. It considered that even if the reference in the CrimPR were brief, it could be supplemented by detailed guidance in the CrimPD and prescribed forms. The SFO did not object to guidance being provided on the duty of candour in Code B of PACE but considered that the rules of court were a more suitable place to codify a duty which is owed to the court.

Enshrining the duty of candour in Code B of PACE

5.36 A number of consultees suggested that the duty of candour should be spelled out in Code B of PACE. HM Council of District Judges (Magistrates' Court) considered that in order to ensure that applicants (who are most frequently police officers) are aware of their duty of candour, amendments to Code B would be the most effective vehicle for reform. The Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate also considered that amending Code B of PACE would help those less experienced in applying for warrants to demonstrate full candour.

5.37 The Bar Council and the CBA considered that the duty of candour should be contained within Code B of PACE. This approach would reflect the fact that there exists a range of sanctions within the context of a criminal trial to address bad faith, negligence, incompetence or mistake and any resulting unfairness to a defendant, which allow the court to impose a sanction that is proportionate to the breach.

A list of information which must be disclosed

5.38 On the question of whether any amendments ought to include a list of the information which must always, if it exists, be disclosed:

(1) twelve agreed that such a list should be included;[19]

(2) one disagreed;[20] and

(3) two expressed other views.[21]

5.39 The overwhelming majority of consultees were persuaded that a list of information which must be disclosed would be beneficial. However, many also cautioned against the duty being reduced to a box-ticking exercise. The CPS and the Insolvency Service considered that the risk of a box-ticking exercise would be reduced if it were made clear that any list is non-exhaustive.

---

19 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Insolvency Service; Birmingham Law Society; Justices' Clerks' Society; Magistrates Association; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Financial Conduct Authority.

20 The Competition and Markets Authority.

21 Kent County Council Trading Standards; The Law Society.

5.40 The only consultee to disagree, the Competition and Markets Authority, sought to preserve its bespoke search warrants regime. They stated:

> Each application is fact specific and the CMA has concerns that, at least in respect of the regimes it enforces, prescribing a list of things which must be covered in the application may have the unintended consequence that relevant information falling outside the list is omitted or that the scrutiny applied by the courts becomes unduly focussed on whether the list has been complied with.

Analysis

5.41 In the light of consultees' responses, we remain of the view that steps ought to be taken to make the duty of candour more accessible and comprehensible. We remain concerned that failure to discharge the duty of candour is one of the most frequent grounds of challenge.

5.42 We accept that amending the law cannot, on its own, ensure that applicants make full and frank disclosure. We discuss the need for training at paragraphs 5.113 to 5.126 below. Responses from consultees indicate, however, a clear view that amending the law is likely to increase compliance with the duty of candour.

Enshrining the duty of candour in statute

5.43 We have considered whether the duty of candour should be codified in primary legislation, given the number of consultees who supported this. At the same time, we have taken into account the concerns of the Bar Council and the CBA relating to the existing duty not to mislead the court and the potentially disproportionate effect of breaching a statutory duty of candour.

5.44 As a matter of principle, we agree with consultees that the importance of the duty of candour justifies it being included in primary legislation. As we pointed out in our consultation paper, it is as important as those safeguards already found in section 15 of PACE. The fact that there is a common law duty not to mislead the court does not mean that there is no value to be found in enshrining the duty of candour in statute.

5.45 As we have repeatedly emphasised, failure to make appropriate disclosure is one of the most frequent grounds of challenge to the lawfulness of a search warrant. We consider that enshrining the duty of candour in statute may also contribute towards bringing about a cultural change in how applicants approach disclosure when applying for a search warrant.

5.46 We also agree with HM Council of District Judges (Magistrates' Court) that greater knowledge of the duty of candour may reduce the number of warrant applications, or at least the number of defective applications. However, we consider that this would not follow simply because the duty was set out in statute. Fewer defective search warrant applications could equally result from the duty of candour being spelled out in secondary legislation, namely Code B of PACE and rules of court. In addition, we accept the point made by the SFO that the duty of candour may have less impact if included in statute than it would if included in rules of court.

5.47 Despite this, we consider that statutory codification would have *some* impact, such that it would justify the duty being placed on statutory footing. We also note that codification of the duty of candour in primary legislation does not preclude the inclusion of the duty in rules of court or Code B of PACE.

5.48 We also agree that the duty of candour would only be worth enshrining in statute if it could be understood clearly, otherwise it would defeat the purpose of codification. Simply stating that the applicant owes a duty of candour does not promote clarity. As is clear, we also consider that the duty should be a codification of the current law.

5.49 With this in mind, we have given thought to how the duty could be defined within statute. Following discussions with the Office of the Parliamentary Counsel, we consider that wording along the following lines would be appropriate, which would reflect the wording of the Terrorism Prevention and Investigation Measures Act 2011:

> Where a constable applies for a warrant, the constable is under a duty to disclose—
>
> (a) material available to the constable which adversely affects the case for issuing a warrant; and
>
> (b) material available to the constable which supports the case of another party.[22]

5.50 Two advantages would flow from defining the duty of candour in one of these ways. First, the duty would be clear and understandable, as argued for by the SFO. Secondly, the formulation would do no more than reflect the current law, as argued for by the FCA.

5.51 A secondary question is which statute the duty should be included in. There are advantages to the wording being inserted in section 15 of PACE. It is the main provision which contains safeguards applicable to search warrant applications. It also already contains a number of disclosure requirements. Further amendments to primary and secondary legislation may be needed so that the duty applies where section 15 of PACE has been extended to other agencies and where comparable safeguards are contained in other pieces of legislation.

5.52 We have considered what the consequence of codifying the duty of candour in this way would be. Section 15(1) of PACE, and other regimes which replicate the effect of section 15(1), provide that entry onto or search of premises under a warrant is unlawful unless it complies with the safeguards.[23] The warrant itself is not rendered unlawful.[24] However, relief for a breach of the statutory safeguards is discretionary; the court will take into account the extent of the breach and its impact on the claimant.[25] As such, a breach of the statutory safeguards may still result in a warrant being quashed.[26]

5.53 The approach taken by the courts when determining a challenge, and the subsequent award of relief, is likely to be the same regardless of whether the duty remains solely a common law duty or is set out in statute. Under the current law, if an application is made for judicial review of the issue of a warrant on the basis that the application was inaccurate or insufficient, the court will quash the warrant where the correct or missing information, if supplied, might reasonably have led the magistrate to refuse to issue the warrant.[27] The

---

22 Reference to material "available to" a constable would make it clear that the duty of candour only extends to facts known to the constable at the time.

23 We discuss the operation of the Police and Criminal Evidence Act 1984, s 15(1) in detail in Chapter 2 above.

24 *Lees v Solihull Magistrates' Court* [2013] EWHC 3779 (Admin), [2014] Lloyd's Rep FC 23 at [43].

25 *R (Hicks) v Commissioner of the Metropolis* [2012] EWHC 1947 (Admin), [2012] ACD 102 at [247] by Richards LJ.

26 *R (Global Cash & Carry Ltd) v Birmingham Magistrates' Court* [2013] EWHC 528 (Admin), [2013] ACD 48 at [20].

27 *R (Hart) v Crown Court at Blackfriars* [2017] EWHC 3091 (Admin), [2018] Lloyd's Rep FC 98 at [19].

mere fact that the duty is replicated in statute would not alter this unless the statute so provides.

5.54 If the test were put on statutory footing in section 15 of PACE, an application for judicial review could be made on the grounds of breach of the provision in section 15 of PACE, rather than a breach of the duty of candour more generally. The court would then be entitled to quash the warrant. For these reasons, we are not persuaded by the concerns of the Bar Society and the CBA that including the duty in statute may result in a disproportionate number of warrants being rendered unlawful. Enshrining the duty in this way would only codify the current law and not affect the rights and remedies currently available.

Recommendation 14

5.55 We recommend that the duty of candour be codified in section 15 of the Police and Criminal Evidence Act 1984.

Enshrining the duty of candour in rules of court and Code B of PACE

5.56 As stated above, codification in statute does not preclude inclusion of the duty of candour in the CrimPR, CrimPD or Code B of PACE. We have therefore considered whether it would be desirable to include the duty of candour in these instruments too.

5.57 We observed at paragraph 5.19 above that the CrimPR and CrimPD already refer to the duty of candour. We are not persuaded that the duty of candour would benefit from further exposition in the CrimPR; given that the duty is already discussed, this may unnecessarily overburden the rules.

5.58 Instead, expansion of the duty of candour may be appropriate in the CrimPD. We note a recent amendment to the CrimPD which provides a non-exhaustive list of matters which might reasonably be thought capable of undermining the reliability of an expert's opinion, or detracting from the credibility or impartiality of an expert.[28] We consider that this may provide a useful precedent for a similar approach in respect of search warrants.

5.59 Turning to Code B of PACE, we note that there is little discussion of the duty of candour in the Code. Guidance note 3A states that an officer should be prepared to answer any questions that the issuing authority may have about the accuracy of previous information from a source or other related matters. In our view, this could usefully be expanded.

5.60 There are a number of advantages to including the duty of candour in both the CrimPD and PACE Code B, as well as in statute. The narrative format and adaptability of the CrimPD and Code B of PACE means that the duty can be spelled out more clearly and in a more narrative form. Of course, any description of the duty of candour in secondary legislation would have to be phrased so as to complement a statutory duty.

5.61 The CrimPD and Code B of PACE are also likely to be read by those who are involved in making search warrant applications. Therefore, including a description of the duty of candour in these sources of law is more likely to make applicants aware of what is required of them than if contained in statute alone. Combined with amendments to application forms, we

[28] Criminal Practice Directions, Division V 19A.7 (as amended 2019).

consider that this would make the duty of candour adequately accessible and comprehensible.

5.62 We note that the Independent Office for Police Conduct ("IOPC") has recently recommended that the PACE Strategy Board[29] amend Code B of PACE to include guidance to make the duty of disclosure clearer to investigators and assist them to comply with this duty.[30] In response, the PACE Strategy Board said that attention would be better focused on the CrimPR, as the statutory authority for including disclosure requirements in search warrant application forms arises from those rules and not Code B of PACE.

5.63 However, if, as we recommend above, the duty of candour were included in section 15 of PACE, we consider that that would create a strong justification for including a discussion of the duty in Code B of PACE.

5.64 It may also be argued that amending Code B of PACE or the CrimPD will have little effect on actual practice. We agree that training is fundamental if practice is to be changed and make a recommendation in relation to this below. We also recognise that there are other guidance sources which may be more readily referred to by investigators. For example, the College of Policing has stated that they will update their online information database, known as 'Authorised Professional Practice', to emphasise the importance of disclosing all information.

5.65 No amendment will be a silver bullet: there is no single document to which all investigators will always refer. But we believe that amending Code B of PACE would increase understanding of and compliance with the duty of candour.

5.66 Another issue that we have considered in the light of our conclusions is duplication. If amendments were made to the CrimPD and Code B of PACE, there is likely to be duplication across these sources and the application forms. However, we regard this better described as reiteration. A number of matters are already found across multiple sources, such as the duty to identify, so far as is practicable, the material sought.[31] The advantage of reiteration is that the duty is more likely to be read and followed. Given that failure to abide by the duty of candour is one of the most frequent grounds of challenge, and may lead to entire criminal investigations collapsing with huge reputational and cost implications, we consider that reiterating the duty in multiple sources is desirable.

5.67 We have also taken into account further concerns raised by consultees. First, that a list of information relevant to the duty of candour may reduce the duty to a box-ticking exercise. Secondly, that requiring that information on any list *must* be disclosed risks parties and the courts unduly focusing on whether the list has been complied with.

5.68 Each case which leads to a search warrant application will be fact specific. The list of information, as with our recommendation in respect of the application form, should be non-exhaustive. We agree with the CPS and the Insolvency Service that emphasising that the list is non-exhaustive would reduce the risk of the duty of candour becoming a box-ticking

---

29 The Strategy Board is merely advisory to the Home Secretary and cannot itself amend Code B. The Board can consider recommending whether or that Code B should be amended but cannot consider amending Code B.

30 Independent Office for Police Conduct, *Operation Kentia: A report concerning matters related to the Metropolitan Police Service's Operation Midland and Operation Vincente* (October 2019), p 26.

31 Police and Criminal Evidence Act 1984, s 15(6)(b); Criminal Procedure Rules, r 47.27(1)(c); PACE Code B (2013) para 3B.

exercise. In the light of the Competition and Markets Authority's concerns, we are hesitant to recommend that the information listed *must* be disclosed. The wording should do no more than draw to the applicant's attention the type of information which might influence the court's decision to issue a warrant.[32]

Recommendation 15

5.69 We recommend that the Criminal Procedure Rule Committee and the PACE Strategy Board consider amending the Criminal Practice Directions and Code B of the Police and Criminal Evidence Act 1984 to set out the duty of candour in greater detail. This should include consideration of the desirability of devising a non-exhaustive list of information which may be relevant to discharging the duty of candour.

ARRANGING A SEARCH WARRANTS APPLICATION HEARING

The current law

5.70 No search warrant can be granted without a private hearing in the presence of the applicant. An applicant need not be physically present: hearings may take place in person, by live link or over the telephone. These hearings will usually take place during court hours, but if the application is particularly urgent it can be heard outside court hours.

5.71 The way in which search warrant application hearings are arranged depends on the investigative body making the application, the nature of the application and the court procedures in place in the region concerned. Procedures also change regularly. The result is that, nationwide, there is no consistent practice.

The consultation paper

5.72 Stakeholders with whom we engaged prior to the consultation shared vastly different experiences. Many considered that improvements could be made to the process of applying for a warrant.

5.73 For this reason, we were interested in gathering wider evidence about consultees' experiences of arranging search warrant hearings. This was to assist us in identifying how the process under which applications are submitted, allocated and heard should be reformed. For example, we wanted to identify any potential obstacles to the arranging of application hearings. We therefore invited[33] consultees to share with us their experience of how search warrant hearings are arranged.

5.74 In the next chapter, we consider reform to the wider procedure for issuing a search warrant. For present purposes, we are concerned with the process by which search warrant hearings are arranged.

---

32 We discuss factors that may be relevant to discharging the duty of candour at paragraphs 4.49 to 4.109 above.

33 Consultation Question 14.

Consultation responses

5.75 Eighteen consultees[34] answered this question. Consultees' responses confirm that there is no standard procedure for arranging a search warrant application hearing. Here we set out how hearings are arranged, taking into account the differences consultees described.

Preparing an application

5.76 Typically, a search warrant application form will be completed electronically. Usually, this will involve either completing one of the CrimPR application forms or using a modified application form. Occasionally, it will involve presenting the application in narrative form. Some police forces have computer software with a search warrants module which guides them through completing a search warrant application. While this generates a completed application form, it does not automatically send it to the relevant court centre.

5.77 In some cases, the applicant will be seeking to obtain multiple search warrants. This is referred to informally as a "bulk" search warrant application. In complex criminal investigations, search warrants may be sought under different statutory provisions or by multiple agencies if there is a joint investigation.

5.78 The applicant will usually be a constable or other investigator involved in the criminal investigation. From the evidence we have been given, the level of training given to those who are empowered to apply for search warrants varies. In some agencies, applications must be made by an officer who has completed a search warrant application course. At the other end of the scale, we saw one example where a constable was completely unaware of the legislative provision under which they were applying for a search warrant.

5.79 Staffordshire Police explained their use of a "professional applicant" model. This involves a detective constable who specialises in applying for search warrants. In short, intelligence related to live investigations feeds into a central repository, which is reviewed by the professional applicant to assess whether there are grounds to apply for a warrant. We were told that this professional applicant model was streamlining the warrant application process, ensuring that applications are of a sufficiently high standard and saving police resources. In a similar vein, the NCA has established a dedicated group of search warrant applicants and carried out awareness training for officers authorising applications. This is the sole route for any applications for search warrants and production orders.[35]

5.80 In some cases, the applicant will not be involved directly in the investigation. As discussed in the next section, this may in some cases lead to difficulties at the application hearing where the applicant has insufficient knowledge to answer questions. In complex cases, more than one officer may attend the hearing. Additionally, external lawyers (such as barristers) may be enlisted to advise the agency in applying for a warrant. Experts, such as forensic experts, may also be asked to provide information alongside the applicant.

---

[34] HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; West London Magistrates' Bench; The Law Society; Southern Derbyshire Magistrates' Bench; Justices' Clerks' Society; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Serious Fraud Office; Competition and Markets Authority; Staffordshire Police; Financial Conduct Authority; DS Parminder Kang, Leicestershire Police.

[35] Criminal Justice Joint Inspection, *Delivering Justice in a Digital Age: a Joint Inspection of Digital Case Preparation in the Criminal Justice System* (2016) para 1.5.

5.81 The following factors may affect the approach taken by the applicant when arranging a search warrant application hearing:

(1) if the search warrant is sought non-urgently during court hours;

(2) if the search warrant is sought urgently during court hours; and

(3) if the search warrant is sought urgently out of court hours.

We consider each of these routes in turn.

Arranging a non-urgent search warrant application hearing

5.82 A search warrant application is usually understood to be urgent if the applicant intends to execute the warrant within the next 24 hours. However, we were informed by DS Parminder Kang, a Detective Sergeant with Leicestershire Police, that there is an inconsistent practice in terms of the criteria used for determining whether an application is urgent. An applicant may attend court in person when a warrant is sought urgently, as there is no time to wait for a hearing slot, which inevitably disrupts court business. It was therefore suggested that guidance on the criteria to determine whether a search warrant application is urgent would be beneficial and lead to a more consistent practice.

5.83 The majority of search warrants are not sought on an urgent basis. In these cases, applicants may arrange a hearing through a number of different channels. The available channels depend on the region in which the investigator is situated.

5.84 HM Council of District Judges (Magistrates' Court) stated that in some areas the court office controls the booking of applications sent in advance by way of an appointments system. This is run by the administrative branch of HMCTS and therefore without legal oversight. This may prevent anything but very urgent applications being dealt with quickly.[36]

5.85 Staffordshire Police explained that if the warrant is not sought urgently, they will email the relevant court centre to check the next available time and date in the court's diary. The hearing date will be confirmed and the relevant documents emailed to the legal adviser. The application form may be checked for defects by the legal adviser before the hearing.

5.86 Some areas were piloting a scheme allowing applications to be sent securely by email and a time allocated by the court office for telephone consultation and video link with the applicant. HM Council of District Judges (Magistrates' Court) encouraged the use of technology in this way.

5.87 The West London Magistrates' Bench informed us that West London has dedicated search warrant courts. A single magistrate hears applications from across London during 30-minute telephone slots which must be booked in advance. The magistrate will read emailed applications and question the applicant during a telephone conference in which a legal adviser also participates. The legal adviser can note additional information provided by the applicant and make minor amendments to the search warrant. If granted, an electronic signature is added to the warrant which is then sent electronically to the applicant. The West London Magistrates' Bench commended the dedicated search warrant court model for saving police and court time.

---

[36] We were not informed precisely why a lack of legal oversight reduced the speed of applications.

5.88 The Justices' Clerks' Society stated that in the South-East region applicants book themselves in for a hearing using an online diary and then email the application to the court. The application is then held by telephone with a justice supported by a legal adviser, who deal with no other types of business. We were informed that HMCTS intends to extend this model to the rest of England and Wales, but we do not know when.

5.89 In relation to the South-East model, the Law Society observed that the volume of applications is high with little scope to re-arrange hearings or accommodate applicants at other times. They considered that a central booking system that would allow applicants to seek telephone hearings in courts across the country would be preferable, and that this flexibility would mean courts could utilise "dead time" more effectively.

5.90 The Law Society also observed that that there are only 32 slots allocated per day under the South-East model, even though a number of counties are covered. They stated that HMCTS would need to put more resources into the scheme if it was to be more widely implemented.

5.91 HM Council of District Judges (Magistrates' Court) stated that in many areas applicants attend at court without notice and there is no system in place to establish urgency. An applicant may turn up even though a search warrant is not sought on an urgent basis. This may be in part owing to the problems applicants have with arranging hearing slots soon enough for the warrants to be executed.

5.92 The CPS observed that attendance without notice places the court under pressure to deal with warrant applications, which may encourage efficiency or may encourage undue haste. They also suggested that the fact that warrant applications must compete for court time with other important court business ought to be reviewed by the court service.

5.93 As can be seen, different procedures have developed and pilots have been tested in different court centres. HM Council of District Judges (Magistrates' Court) stated that a standard procedure applicable nationally would be beneficial. On the other hand, the Law Society observed that harmonisation may not always be achievable due to resource constraints at different court centres.

5.94 A recurring complaint from consultees concerned the lack of court availability to hear applications. We were informed that, in the Midlands, an applicant could be waiting between one week and 10 days for a slot to apply for a search warrant. This has significant consequences for the reliability of the intelligence: the longer it takes to organise a hearing, the more difficult it is to satisfy the statutory conditions that there is relevant material on the premises. Where courts offer 60 to 80 slots per week, these are rapidly filled.[37] As a result, applicants may feel that they have no choice but to attend a court without a hearing slot, a route otherwise used for urgent applications.

5.95 Some agencies may make an application to the Crown Court. Under certain search warrant provisions, this is a requirement.[38] In other instances, an applicant may decide to arrange a hearing in the Crown Court due to the complexity of the case.

---

[37] We have no evidence to indicate how many slots would be required to prevent a backlog.

[38] Police and Criminal Evidence Act 1984, sch 1 para 17; Drug Trafficking Act 1994, s 56; Terrorism Act 2000, sch 5, para 11; International Criminal Court Act 2001, s 37 and sch 5.

5.96 For Crown Court applications, we were informed that hearings are arranged very informally. An officer telephones the administrative office of the relevant court and requests a hearing. This may be done weeks in advance in the case of complex criminal investigations. The applicant will be told whether their application can be accommodated in the timescale requested and, if a suitable slot is found, will be given a listing. A full set of papers will often be served at least 24 hours in advance of a hearing so that the allocated judge can read them in advance. Counsel may also be instructed to appear at the hearing. It may be appropriate to file a short skeleton argument in advance of the hearing directing the issuing authority to the issues to be determined and relevant case law.[39]

5.97 Unusually, search warrant applications under the Competition Act 1998 and the Enterprise Act 2002 are made to the High Court. These are supported by an affidavit and exhibits, and the Court is given sufficient reading time in advance of the application.

Arranging an urgent search warrant application hearing during court hours

5.98 When seeking a search warrant application urgently, an applicant may attend a court in person to obtain a search warrant that day. This is typically because there are no telephone hearing slots available soon enough. We have heard examples of significant delays in some cases. One consultee reported that they were informed that the next available search warrant telephone hearing slot was 14 days away. In such circumstances, applicants may feel that they have no choice but to attend court in person, a route otherwise reserved for urgent applications.

5.99 Applications are dealt with at any time during a court day, including before the court sits or whenever there is a suitable break in proceedings. As stated above, there is rarely a system in place to determine how urgent an application is.

5.100 There are two main problems that arise when an applicant attends a court centre in person to obtain a warrant. We have heard that officers may have to drive, sometimes up to 50 miles, and then sit waiting in a court centre for more than two hours. Whether an application is heard may depend on the goodwill of court staff. We were informed that it is not unheard of for applicants to attend several court centres before finally being heard. This makes it difficult for law enforcement to respond quickly to evolving intelligence.

5.101 The second issue, as noted above, is the impact on the running of the courts. Court business may be disrupted and the courts may be put under pressure to deal with warrant applications with undue haste. There are also fewer facilities to amend applications where an application is made in person and greater difficulty is posed when gathering information in response to a query.

Arranging an urgent search warrant application hearing outside court hours

5.102 Sometimes an applicant will want to obtain a search warrant urgently but the court centres will be closed because it is out of normal sitting hours. In such cases, applications can be made out of court hours.

5.103 The Justices' Clerks' Society informed us that out of hours applications always begin with the applicant, or someone acting on their behalf, contacting a legal adviser who arranges the hearing. In most cases the legal adviser is on a rota, with a standard telephone number

---

39 *Ashbolt v HM Revenue and Customs* [2020] EWHC 1588 (Admin) at [72].

assigned to their mobile phone. In a few areas, applicants have to ring a list of legal advisers until one answers, however, this method of working is being phased out.

5.104 The Magistrates Association stated that magistrates also operate a rota system for out of hours availability. A legal adviser or clerk has to call magistrates listed as dealing with out of hours warrant applications to find someone who is available to hear the application. There are concerns that this process can be inefficient and very time-consuming for legal advisers and clerks.

5.105 In addition to speaking with the applicant, we were informed that in most cases the legal adviser will be sent the application before it is sent to the magistrate. It was considered that sight of the application form by a legal adviser made the process more efficient as advice could be given on specific issues.

5.106 In the South-East region, three magistrates are assigned every day, one for each half of the region and a reserve. The application is made by three-way telephone call, between the applicant, justice and legal adviser. The application is sent by email and the warrant completed and signed by the legal adviser in the same way. HMCTS aims to adopt the same system nationally. Outside the South-East region and some parts of Wales, there are no assigned justices. In these areas legal advisers have to telephone justices from a list until they find one who is available.

5.107 Apart from in the South-East region, hearings take place at the justice's home. Magistrates reported long delays between being called by the legal adviser and the applicant arriving at their home. Legal advisers give advice in advance and are available to give advice if the justice seeks it, but do not attend the actual application. Service of the application by email is common but not universal.

5.108 HM Council of District Judges (Magistrates' Court) stated that out of hours applications are also currently dealt with in many different ways across the police regions. It was argued that any reformed process must also include a single process for dealing with out of hours applications.

5.109 We were informed by Staffordshire Police that there have been recent changes to how out of hours applications are arranged in the Midlands. We were told that it can be difficult to apply for search warrants out of hours due to the lack of available magistrates, with the local justice area struggling to cope with demand for hearings. In some cases, the police have had to wait until the following morning and attend a court centre seeking an urgent hearing.

Analysis

5.110 The information provided by consultees in response to Consultation Question 14 has informed a number of our recommendations throughout this report. In the next chapter, we consider the desirability of introducing a standard national procedure for search warrant application hearings. It has also influenced our recommendation for an online search warrants portal at Recommendation 13,[40] which would streamline the application process and remove potential inconsistencies.

5.111 Based on consultees' experiences as described above, we are fortified in our view that there ought to be a standard procedure for search warrant application hearings nationally, which

[40] See paragraph 4.154 above.

maximises the use of technology to encourage remote hearings. We note that HMCTS intends to extend the dedicated search warrant court model and the remote out of hours model to the rest of England and Wales. We welcome these developments and discuss reform further at paragraphs 6.92 to 6.99 below in respect of out of hours applications and paragraphs 6.121 to 6.141 below in respect of in court hours applications.

5.112 There are two additional matters relating to the arranging of search warrant applications which require consideration irrespective of the model adopted: first, the training delivered to law enforcement agencies and, secondly, the availability of hearing slots.

Training delivered to law enforcement agencies

5.113 A retired senior police officer reported to us that if we want to get search warrants right, we need to start early in the "production line". It was said that insufficient training causes problems at all stages of the search warrants process, from defective applications to unlawful seizure.

5.114 In our consultation paper, we described an NCA review of all warrants and orders obtained from the courts in live pre-conviction criminal cases. The NCA legal department identified a need to introduce effective training for those making search warrant applications, together with a proper review process prior to applications being made. This led to a change of policy whereby only those officers who had received training could authorise applications for search warrants under PACE.

5.115 We note the recent report into changes made by the NCA in response to search warrant and production order deficiencies.[41] The findings were that:

> Overall, the standards of warrant applications were good. The effort that has been invested in training staff was evident. Applications were precise and explained the offences in sufficient detail; sufficient court time was allocated and intelligence managed appropriately.[42]

5.116 What this indicates is that training undoubtedly increases the quality of search warrant applications and creates cost savings. For this reason, in our view, training ought to be taken seriously by all law enforcement agencies involved in applying for or executing search warrants.

5.117 Recommendations for better training on search warrants have been made on a number of occasions in respect of specific agencies. Since the close of our consultation period, the IOPC has published a report with recommendations[43] regarding search warrants. This stemmed from a referral by the Metropolitan Police Service ("MPS") to the IOPC of five officers following criticisms made by Sir Richard Henriques relating to search warrant applications. Sir Richard Henriques was originally commissioned by the MPS to review the force's handling of a number of investigations. The IOPC made a series of recommendations relating to search warrants, two of which concerned learning and training.

---

41 HMCPSI and HMICFRS, *A joint inspection of search application and production order processes* (January 2019).

42 HMCPSI and HMICFRS, *A joint inspection of search application and production order processes* (January 2019) para 2.6.

43 Independent Office for Police Conduct, *Operation Kentia: A report concerning matters related to the Metropolitan Police Service's Operation Midland and Operation Vincente* (October 2019).

5.118 First, the IOPC recommended that the MPS take immediate steps to assure itself that appropriate measures (including training, guidance and oversight) are in place to ensure that warrants applied for by the MPS are consistently completed to a high standard.[44]

5.119 The MPS's response indicates that changes will be made to their search warrant guidance, online training material and training courses. A new governance structure will allow for clear oversight and performance on search warrants. The MPS has also committed to engaging with other police forces to support the College of Policing in the development of national standards for search warrant applications.

5.120 Secondly, the IOPC recommended that the National Police Chiefs' Council ("NPCC") and the College of Policing work together to consider what steps can be taken to ensure that warrant applications made by the police are consistently completed to a high standard.[45] As this work is undertaken, the IOPC also recommended that the NPCC and the College of Policing consider the lessons learned from an internal review of search warrants carried out by the NCA and its subsequent inspection to determine whether any of this learning is transferrable to the police service.[46]

5.121 Since the IOPC made this recommendation, the College of Policing has stated that they will update their online information database, known as 'Authorised Professional Practice', and the College of Policing curriculum, from which most police training is delivered.

5.122 Another recommendation made by the IOPC was that the MPS should issue an urgent reminder to officers of the requirements of this duty of disclosure and how important it is to make full disclosure in a search warrant application.[47]

5.123 The IOPC recommendations are directed at the MPS, one of 43 territorial police forces in England and Wales. As we stated at paragraph 9.72 of our consultation paper, the police no longer have a monopoly on the investigation of crime, and where other officials are performing similar functions they should be subject to the same safeguards as the police. We agree that training ought to be in place to ensure that search warrant applications are completed to a high standard, however, this must apply to all law enforcement agencies who apply for warrants.

5.124 We have seen that institutional reform is often prompted by highly-publicised and significant failings in individual cases. Where improvements are necessary, it should not take such failings to effect institutional change. Accordingly, we recommend that *all* law enforcement agencies involved in applying for and executing search warrants take steps to ensure that appropriate measures are in place so that search warrant applications are consistently completed to a high standard.

---

44 Independent Office for Police Conduct, *Operation Kentia: A report concerning matters related to the Metropolitan Police Service's Operation Midland and Operation Vincente* (October 2019) p 23.

45 Independent Office for Police Conduct, *Operation Kentia: A report concerning matters related to the Metropolitan Police Service's Operation Midland and Operation Vincente* (October 2019) p 24.

46 Independent Office for Police Conduct, *Operation Kentia: A report concerning matters related to the Metropolitan Police Service's Operation Midland and Operation Vincente* (October 2019) p 24.

47 Independent Office for Police Conduct, *Operation Kentia: A report concerning matters related to the Metropolitan Police Service's Operation Midland and Operation Vincente* (October 2019) p 26.

5.125 Consideration will have to be given to the form, content and breadth of training. For example, whether it should be a requirement that only those officers who have undertaken training be permitted to apply, or authorise an application, for a search warrant. It is not for us to dictate these matters. Further, training must be tailored to each law enforcement agency, taking into account their size, structure and the nature of their enforcement powers. We agree that the lessons learned by the NCA following their internal review could be usefully reflected upon by other agencies.

Recommendation 16

5.126 We recommend that all law enforcement agencies take steps to ensure that sufficient training is provided to officers involved in applying for and executing search warrants to ensure that applications are consistently completed to a high standard.

The availability of hearing slots

5.127 Several law enforcement consultees and the Law Society expressed concerns over the availability of hearing slots. Discussions with police forces in July 2020 confirmed that there remains in some cases a three-week waiting time to have search warrant applications heard.

5.128 There are two main reasons why, in our view, more hearing slots should be made available, which have been touched on above. First, search warrants applications must be dealt with in a timely manner, irrespective of whether they are especially urgent. The longer the delay, the greater the likelihood of intelligence becoming out of date and the statutory conditions not being satisfied.

5.129 Anecdotal evidence from speaking with several police forces suggests that the majority of investigations in which search warrants are obtained concern the supply of drugs. Other investigations often concern firearms, offences against persons, theft and related offences. In all these cases, the longer it takes to obtain and execute a search warrant, the higher the risk of evidence being lost and the longer the period of potential offending and therefore harm being caused to members of the public.

5.130 Secondly, where slots are unavailable, applicants may be left with little choice but to attend court in person. As identified above, this may waste police and court time, disrupt court business and put pressure on courts to deal with search warrant applications immediately. It is therefore in the interests of all those involved in the criminal justice system, and the wider public, that search warrants can be obtained without undue delay.

5.131 In the light of concerns raised by several law enforcement agencies, we consider that more search warrant application hearing slots should be made available. This would decrease the length of time it takes to obtain a search warrant. We accept that court availability is limited, however, creating more slots would reduce disruption to court business, including reducing delays to trials.

5.132 We also accept that more hearing slots would not resolve all problems in the application process; formalising and streamlining the application process is also extremely important. However, regardless of the model adopted, there must be sufficient hearing slots.

Recommendation 17

5.133 We recommend that Her Majesty's Courts and Tribunals Service consider the practicability of making more search warrant application hearing slots available or pursuing other measures which would decrease both the length of time it takes to obtain a search warrant and the disruption to other court business.

THE LEVEL OF KNOWLEDGE REQUIRED WHEN APPEARING AT A HEARING

The current law

5.134 Section 15(4) of PACE provides that the constable applying for a search warrant constable shall answer on oath any question that the justice of the peace or judge hearing the application asks them. At present, there is no requirement that the applicant be involved in the criminal investigation to which the warrant relates, or that an adequate level of knowledge regarding the investigation must be held. Nor do Code B or rules of court impress the importance of having sufficient knowledge to answer questions on oath. However, clearly the less knowledgeable an applicant is, the lesser the chance that a warrant will be issued.

The consultation paper

5.135 In the consultation paper, we made clear our desire to improve the way that applicants provide information at search warrant hearings. We were informed anecdotally by one magistrate that it is not uncommon for officers who know very little about the case to apply for search warrants. This often leads to the application being refused and another hearing being arranged, wasting both the court and the investigator's time.

5.136 For this reason, we invited[48] consultees' views on whether problems commonly arise because applicants for search warrants do not have sufficient knowledge to answer the questions on oath. If so, we asked whether consultees consider that reform is needed. We also invited consultees' views on whether there ought to be more detail in rules of court or Code B of PACE on what is required from an applicant at a search warrant hearing.

Consultation responses

5.137 Twenty consultees[49] answered this question.

Insufficient knowledge of the case

5.138 Several consultees[50] stated that applicants lacking a detailed knowledge of the case frequently causes problems. This is often only revealed when additional information is

---

48 Consultation Question 15.

49 Robert Della-Sala JP; Department for Work and Pensions; Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; West London Magistrates' Bench; The Law Society; Southern Derbyshire Magistrates' Bench; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Serious Fraud Office; Competition and Markets Authority; Financial Conduct Authority.

50 Council of Her Majesty's Circuit Judges, HM Council of District Judges (Magistrates' Court); West London Magistrates' Bench; Robert Della-Sala JP.

requested and the applicant explains that they cannot provide any answers. The Magistrates Association surveyed their members and 60% of respondents said that they had experienced cases where applicants did not know enough about the case to answer detailed questions.

5.139 One serving magistrate informed us that there is a tendency for inexperienced officers to be applying for warrants. This inexperience extends to both unfamiliarity with the statutory conditions for issuing a warrant and the powers which the warrant confers. This will often lead to warrants being refused which otherwise might not have been, wasting time and resources.

5.140 Responses suggest that police forces are most likely to send junior officers to obtain search warrants.[51] However, the specialist law enforcement agencies who responded to this question all indicated that this problem does not arise in respect of their investigations.

More detail on what is required from an applicant

5.141 On the question of whether reform is needed to increase the likelihood that applicants will have sufficient knowledge to answer questions asked:

(1) eight agreed;[52] and

(2) three expressed other views.[53]

5.142 The majority of consultees considered that amendments to Code B of PACE may be more effective than amendments to rules of court in ensuring that applicants understand their duties.[54]

5.143 The FCA stated that some non-statutory guidance as to who should swear and give evidence in relation to the warrant application would be beneficial.

Analysis

5.144 What emerged from consultees' responses was the view that there is a tendency for junior officers with very limited knowledge of the investigation to be tasked with seeking search warrants. It should always be the case that the person applying for a search warrant has adequate knowledge of the investigation. However, this need not be someone directly involved in the investigation. There are several reasons why the person applying for a search warrant may not be an investigator involved in the investigation:

(1) police forces adopting a "professional applicant model"[55] will invariably have an officer who is not directly involved in the application but nonetheless adequately apprised of the facts;

---

51 Law Society; Justices' Clerks' Society.

52 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); The Law Society; Southern Derbyshire Magistrates' Bench; Magistrates Association; Financial Conduct Authority.

53 Crown Prosecution Service; National Crime Agency; Bar Council and the Criminal Bar Association.

54 Magistrates Association; HM Council of District Judges (Magistrates' Court); Council of Her Majesty's Circuit Judges; National Crime Agency.

(2) some agencies may instruct external lawyers to assist with applying for their search warrants; and

(3) for various reasons, it may simply not be practical for an officer directly involved in the investigation to apply for the warrant.

5.145 What is necessary is that the officer who makes the application has adequate knowledge of the investigation to answer questions asked by the issuing authority. In the light of consultees' responses, we remain of the view that it would be beneficial to give this requirement greater prominence.

5.146 Consultees preferred that the requirement that a person have adequate knowledge to answer questions asked at a search warrant hearing be inserted into Code B of PACE. We note in Chapter 4 at paragraph 4.119 above that the Criminal Procedure Rule Committee has made a recommendation to the Lord Chief Justice to amend application forms to require an authorising officer to confirm a number of additional details. We write at paragraph 4.120 above that it may be considered desirable to amend search warrant application forms further to include a declaration that the authorising officer is satisfied that the applicant has the ability to answer on oath any questions asked, as is required of an applicant under section 15(4) of PACE.

5.147 Notwithstanding the potential value to amending the applications forms authorised for use with the CrimPR, we agree with consultees that it would be desirable to amend Code B of PACE for several reasons. First, the requirement may need to be set out in narrative form and Code B of PACE lends itself to the adoption of a more narrative format. Secondly, we regard the current detail in guidance note 3A of Code B of PACE as capable of expansion, as it simply states that:

> the officer should be prepared to answer any questions the magistrate or judge may have about:
>
> (1) the accuracy of previous information from that source; and
>
> (2) any other related matters.

5.148 Thirdly, while conscious of the fact that Code B of PACE should not be overburdened, we also consider that any amendment to Code B of PACE could be expanded to include guidance related to who should swear and give evidence in relation to the warrant application, as suggested by the FCA. For example, such guidance could usefully state that in complex cases specialist information might be best provided by someone other than the applicant officer.

---

[55] Discussed at paragraph 5.95 above.

Recommendation 18

5.149 We recommend that the PACE Strategy Board consider amending Code B of the Police and Criminal Evidence Act 1984 to include the requirement that a person applying for a search warrant has adequate knowledge to answer questions asked by the issuing authority.

SEARCHING PREMISES FOLLOWING ARREST INSTEAD OF APPLYING FOR A WARRANT

The current law

5.150 Not all searches of premises require a warrant.[56] Section 18 of PACE provides that a constable may enter and search any premises occupied or controlled by a person who is under arrest for an indictable offence. Section 32 of PACE also gives the police the power to enter and search any premises where the person was located when arrested (or immediately before being arrested) for an indictable offence.

5.151 Sections 18 and 32 of PACE are both triggered by lawful arrest. The power to arrest without a warrant is found in section 24 of PACE. There are, in effect, two conditions for lawful arrest, both of which must be satisfied.

(1) Under section 24(1) to (3) of PACE, that the person arrested is about to commit, is committing or has committed an offence or the police officer has reasonable grounds for suspecting this to be so.

(2) Under section 24(4) of PACE, that the arresting officer has reasonable grounds for believing that the arrest is necessary for any of the reasons identified in section 24(5) of PACE. One of those reasons, in section 24(5)(e) of PACE, is that the constable has reasonable grounds for believing that arrest is necessary to allow the prompt and effective investigation of the offence or of the conduct of the person in question.

5.152 The issue with which we are concerned here is whether the police, or other officers who have powers of arrest, *can* arrest an individual solely to activate the power to search premises in preference to securing a search warrant.

The consultation paper

5.153 Stakeholders who defend and represent the interests of individuals affected by a warrant expressed concern regarding the interplay between sections 18, 32 and the search warrant procedure. First, they were concerned that there may be a tendency to sidestep the warrant procedure by arresting individuals under section 24 of PACE and then searching their premises under section 18 or 32 of PACE. In effect, this allows the investigator to avoid the higher threshold for securing a search warrant and the time it takes to apply for one. Secondly, they were concerned that where premises are searched under section 18 or 32 of PACE, the protection afforded to journalistic material does not apply. This is because the

[56] See Search Warrants (2018) Law Commission Consultation Paper No 235 paras 4.100 to 4.110.

only restriction on the categories of material that can be searched for and seized under sections 18 and 32 of PACE is for legally privileged material.[57]

5.154 The question we sought to answer in our consultation paper was whether the ground for arrest under section 24(5)(e) of PACE, namely the need to allow the prompt and effective investigation of an alleged offence, includes a need to search premises. If it does, then assuming that one of the conditions in section 24(1) to (3) of PACE is satisfied, is it justifiable to arrest a suspect solely in order to search their premises, or is this an illegitimate way of circumventing the need for a search warrant?

5.155 The Divisional Court has considered whether the intention to carry out a search pursuant to section 18 of PACE could, on its own, justify arresting a suspect under section 24(5)(e) of PACE.[58] The Court held that no conclusive answer could be drawn from the authorities and that it was both unnecessary and undesirable to resolve the issue of principle in that particular case.[59] That said, the court did observe that precluding the police from ever using section 18 of PACE as the sole justification for an arrest under section 24(5)(e) of PACE would have far-reaching consequences.[60]

5.156 The powers of arrest and related search powers are important powers, which are routinely used. It is unsatisfactory that no definitive answer can be gleaned from the current law as to their relationship to the search warrant powers. We therefore considered that this ambiguity should be resolved.

5.157 In the consultation paper, we provisionally proposed[61] that, where the sole intention of arrest is to search premises, this should satisfy the necessity criteria for arrest provided that there are reasonable grounds for believing that it is not practicable to obtain the evidence through other means.

5.158 Under this test, consideration would therefore have to be given by an officer to whether voluntary production of the items could be sought, or a search warrant obtained. Arrest would therefore be lawful if, objectively viewed, there was a reasonable basis for believing that voluntary production would not be given or that it would not be practicable to obtain a search warrant.

Consultation responses

5.159 Fifteen consultees addressed this provisional proposal: seven agreed;[62] four disagreed;[63] and four expressed other views.[64]

---

57 See Police and Criminal Evidence Act 1984, ss 18(1), 18(2), 32(2)(b) and 19(6).

58 *R (L) v Chief Constable of Surrey Police* [2017] EWHC 129 (Admin), [2017] 1 WLR 2047.

59 *R (L) v Chief Constable of Surrey Police* [2017] EWHC 129 (Admin), [2017] 1 WLR 2047 at [66].

60 *R (L) v Chief Constable of Surrey Police* [2017] EWHC 129 (Admin), [2017] 1 WLR 2047 at [71].

61 Consultation Question 16.

62 Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Southern Derbyshire Magistrates' Bench; Justices' Clerks' Society; Metropolitan Police Service; Serious Fraud Office; Financial Conduct Authority.

63 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); The Law Society; Dijen Basu QC.

64 Crown Prosecution Service; Independent Office for Police Conduct; Magistrates Association; National Crime Agency.

5.160 A number of consultees agreed it should be made clear that the necessity criterion for arrest can be satisfied where the sole purpose of arrest is to search premises for evidence. Many also agreed with the introduction of a requirement that there are reasonable grounds for believing that it is not practicable to obtain the evidence through other means.

5.161 The Southern Derbyshire Magistrates' Bench considered that the proposal tightened up what was clearly a loophole that potentially undermines the PACE safeguards. Our proposal, they considered, would ensure that arrest is not used as a short cut to normal evidence gathering.

5.162 The SFO considered that guidance would suffice on this point. In their view, an intention to search premises under section 18 of PACE should satisfy the arrest criteria provided that:

(1) there is an immediate need to do so; and

(2) there are reasonable grounds for believing that it is not practicable to apply for a search warrant or use other less obtrusive means such as voluntary or compelled production.

5.163 Several consultees did not agree with our proposal. For some, the proposal was perceived as extending police powers, whereas for others the proposal was seen as restricting them.

5.164 Professor Richard Stone considered that the proposed change ignored the strength of section 18 of PACE, which permits the search for and seizure of protected categories of material without prior judicial oversight. The Law Society argued that the proposal would effectively condone what they perceived as a police practice of arresting in order to carry out a search. It would also remove the possibility of remedy by a claim for wrongful arrest in such cases.

5.165 The Law Society opposed any extension of arrest powers, and submitted that powers to search should be kept separate from powers to arrest. It noted the potential for arrest to have long lasting consequences for an individual in a way that a search warrant might not. The Law Society also pointed out that the effect of this change could be the arrest of a person who is unconnected with the offence under investigation, but who is in control of the relevant property.

5.166 The Law Society further argued that the proposal would have the consequence of circumventing judicial oversight in relation to decryption notices issued under section 49 of the Regulation of Investigatory Powers Act 2000. This is because, where the police are exercising a statutory power to seize material, a senior police officer rather than a judge may authorise a section 49 notice.

5.167 Dijen Basu QC was of the view that arrest of a person should never be made purely in order to search premises which the arrestee controls. To include section 18 PACE searches as part of the necessity criteria would encourage arrests which were intended purely to enable a search of a person's premises. The Bar Council and the CBA also cautioned that the proposal may encourage arrest for the purpose of search.

5.168 HM Council of District Judges (Magistrates' Court) cautioned that the proposal may bring about a fundamental change to police powers, the consequences of which could be wide-ranging. The CPS expressed similar concerns and argued that further analysis ought to be undertaken before recommending fundamental changes to police powers of arrest.

Analysis

5.169 In the light of consultees' views, we are hesitant to recommend reform in this area. We accept that any change may have a wide-ranging impact on police powers of arrest. As the Law Society points out, there are many consequences which may flow from such a change, however, we disagree that our provisional proposal could lead to the arrest of a person who is unconnected with the offence under investigation: under section 24(1) to (3) of PACE, a constable can only arrest a person who is about to commit, is committing or has committed an offence, or the constable has reasonable grounds for suspecting this to be so.

5.170 We have come to the conclusion that reform of this nature would therefore only be justified on the basis of evidence secured from more detailed and extensive consultation. Consultation responses indicate that reform would have far reaching consequences for police powers not within our terms of reference, and requires more detailed consideration. Given that this was a peripheral issue as far as our terms of reference are concerned, we do not consider that it is necessary for us to seek to resolve it in a report concerning search warrants.

Chapter 6: Issuing a search warrant

INTRODUCTION

6.1 In this chapter we look at how warrants are issued from the perspective of the issuing authority, which will be either a magistrate or judge. We consider possible reform to the following areas:

(1) the circumstances in which a search warrant application ought to be heard by a judge as opposed to a magistrate;

(2) whether magistrates should have specialist training to hear search warrant applications;

(3) formalising the practice of magistrates being advised by a legal adviser;

(4) the number of magistrates who ought to hear a search warrant application;

(5) the procedure governing out of hours search warrant applications;

(6) formalising the application procedure in court hours;

(7) the filtering of search warrant applications made to the Crown Court by a legal adviser;

(8) recording additional material provided during search warrant hearings;

(9) providing written reasons for issuing a search warrant; and

(10) record keeping and statistics concerning search warrants.

6.2 Our focus remains on how procedures can be improved to ensure that the legal requirements are fully adhered to and there is adequate judicial oversight. To that end, we recommend that only those magistrates who have undergone specialist training should have the power to issue a search warrant. We also recommend formalising the practice of magistrates being advised by a legal adviser in the Criminal Procedure Rules ("CrimPR").

6.3 Additionally, we recommend formalising the procedures by which search warrants are issued both during and outside court hours and examining the practicability of audio recording search warrant hearings. These recommendations aim to make the procedures by which a search warrant is issued simpler and more efficient, while also reducing the scope for error.

6.4 We also consider that the use of search warrants ought to be more transparent. Therefore, we recommend a requirement to record and publish statistics on the use of search warrants. In addition to improving transparency, collecting and publishing search warrants data would increase the likelihood of understanding key trends, and being able to respond to them.

DISTRIBUTION BETWEEN JUDGES AND MAGISTRATES

The current law

6.5 Most search warrants are issued by a magistrate (also known as a "justice of the peace"). These are volunteer judicial office holders who sit in a magistrates' court on criminal (and family) matters. No legal training or qualifications are required to become a magistrate. However, magistrates undertake mandatory training and are supported in court by a qualified legal adviser. Magistrates are assigned to a local justice area (also known as a "bench").[1]

6.6 Search warrants are also issued by professional judges in the magistrates' courts by District Judges (Magistrates' Courts) or Deputy District Judges (Magistrates' Courts) and in the Crown Court by recorders, Circuit judges and High Court judges. Although the majority of search warrants are issued by a justice of the peace, other judges have the powers of a justice of the peace.[2] They can therefore grant any application which could be granted by a magistrate.

6.7 Unless specified in the statutory provision, the investigator has complete discretion over which court to apply to. However, the vast majority of search warrant applications are made to a magistrates' court and issued by magistrates or District Judges (Magistrates' Courts) or deputies. The decision about which magistrates are to hear the application, or whether to put the application before a District Judge (Magistrates' Courts) or a magistrate, is made by a legal adviser delegated by the justices' clerk in accordance with the Judicial Deployment Protocol.[3]

6.8 As discussed in the previous chapter, some types of search warrant can only be issued by a Circuit judge. Even where a search warrant can be issued by a magistrate, an applicant may apply to the Crown Court in cases of particular complexity. In *R (Chatwani) v National Crime Agency*, Hickinbottom J, as he then was, observed that, in cases involving money laundering or other financially complex matters, a magistrate may "be less able [than in other types of case] to consider and question applications with the same experience and informed rigour as would (e.g.) a Circuit judge".[4]

The consultation paper

6.9 In early discussions, stakeholders indicated that law enforcement agencies take differing views as to the appropriate circumstances in which to make an application to the Crown Court. We considered that the adoption of a more consistent practice may result in a greater proportion of search warrants receiving the appropriate level of oversight. Therefore, in the consultation paper, we invited[5] consultees' views on whether, in certain cases, it ought to be

---

1 For more information about magistrates, see Courts and Tribunals Judiciary, *Magistrates*, https://www.judiciary.uk/about-the-judiciary/who-are-the-judiciary/judicial-roles/magistrates/.

2 Courts Act 2003, ss 25 and 66.

3 *Protocol to support judicial deployment in the Magistrates' Courts* (November 2012), https://www.judiciary.gov.uk/wp-content/uploads/JCO/Documents/Protocols/support-judicial-deployment-in-magistrates-court.pdf .

4 *R (Chatwani) v National Crime Agency* [2015] EWHC 1283 (Admin), [2015] ACD 110 at [105].

5 Consultation Question 17.

compulsory for a search warrant application to be made to the Crown Court or District Judges (Magistrates' Courts) rather than the lay magistracy. If so, we welcomed views on:

(1) the types of cases to which this rule ought to apply; and

(2) whether the distinction between such cases and routine cases should be in legislation.

Consultation responses

6.10 Twenty-two consultees answered this question: 14 consultees disagreed with introducing more formal rules that would allocate complex search warrant applications to the Crown Court;[6] and eight consultees expressed other views.[7]

6.11 No consultees supported the proposal for a class of cases in which applications must be made to the Crown Court. On the whole, the proposal was viewed as likely to lead to fewer magistrates hearing search warrant applications. Consultees were not persuaded that this was a desirable outcome.

6.12 It was pointed out by a number of consultees that there is no clear evidential basis to suggest that warrants issued by magistrates are more likely to be challenged than those issued by a District Judge (Magistrates' Courts).[8] Where errors are identified, they are usually attributable to mistakes made by the applicant.[9] Additionally, it is often search warrants issued by a Crown Court judge that are challenged as these are often complex criminal investigations in which occupiers have the resources to challenge the lawfulness of a warrant.

6.13 It was also suggested that the consultation question failed to appreciate that magistrates are used to dealing with complex cases and making important judicial decisions, often based on imperfect information.[10] Magistrates are therefore more than capable of dealing with complex search warrant applications.[11] Further, magistrates are assisted by legal advisers and therefore should be properly advised.[12] As a result, applications will benefit from legal expertise irrespective of whether they come before a magistrate or a judge.

6.14 In addition, the cost of an application being heard before a District Judge (Magistrates' Courts) is greater than that of a magistrate and legal adviser. As a result, sending more applications to professional judges would come at a greater cost.[13] There would also be the risk of impacting quite severely on court sittings given the limited number of professional

---

6 Robert Della-Sala JP; Nigel Shock JP; Siân Jones; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Birmingham Law Society; West London Magistrates' Bench; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; Justices' Clerks' Society; Magistrates Association; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Serious Fraud Office.

7 Professor Richard Stone; Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; The Law Society; National Crime Agency; Competition and Markets Authority; Financial Conduct Authority; Dijen Basu QC.

8 West London Magistrates' Bench.

9 Dijen Basu QC.

10 West London Magistrates' Bench; Justices' Clerks' Society.

11 Senior District Judge (Chief Magistrate).

12 Birmingham Law Society.

13 Independent Office for Police Conduct.

judges.[14] Similarly, there is a risk that professional judges would simply not be available given the pressures on their time.[15] These risks were not seen as justifiable given that there is no evidence that the scrutiny being applied by magistrates under the present regime is inferior to that which would be applied by professional judges.

6.15 Concern was also raised regarding the risk of overly prescriptive rules being created to differentiate between complex and other cases. It is notoriously difficult to identify a "complex" case[16] and there is a risk that any definition might operate arbitrarily in practice.[17] For these reasons, change was argued to be unnecessary and at risk of imposing undue rigidity.[18] The numerous factors that may be relevant in any given case would mean that there had to be exceptions, which might undermine the rationale behind having a single test.[19] For example, it was pointed out that the Court of Appeal has held that where a search warrant application is linked with other orders, they should be made before the same judge.[20]

6.16 It was also pointed out that the Judicial Deployment Protocol successfully assists with allocation to District Judges (Magistrates' Courts).[21] Legal advisers are also trained in the vetting of applications and how to allocate them.[22] Law enforcement agencies are also well-placed to decide to which level of judge to apply.[23]

6.17 There was a concern that law enforcement agencies might be impeded by a more formal arrangement.[24] An example was given where a complex and urgent case was dealt with very well by a magistrate. Were it the case that a feature of the application required the application to be made before a professional judge, this may have made it far more difficult to list the application quickly and may have jeopardised the investigation. Flexibility for the investigator is important as they are well-placed to determine to which level of judge the application should be made,[25] especially in urgent cases.[26] Further, a formal requirement for a certain category of case to be dealt with by a Crown Court judge might open up a new avenue of challenge.[27]

---

14 Justices' Clerks' Society.

15 Law Society.

16 Council of Her Majesty's Circuit Judges.

17 Magistrates Association.

18 HM Council of District Judges (Magistrates' Court)

19 Justices' Clerks' Society.

20 Financial Conduct Authority. See *Windsor v Crown Prosecution Service* [2011] EWCA Crim 143, [2011] 1 WLR 1519 at [62].

21 West London Magistrates' Bench; Southern Derbyshire Magistrates' Bench.

22 Law Society.

23 National Crime Agency; Serious Fraud Office.

24 Metropolitan Police Service; Serious Fraud Office; Kent County Council Trading Standards.

25 Competition and Markets Authority; Serious Fraud Office; Financial Conduct Authority.

26 Serious Fraud Office.

27 Kent County Council Trading Standards.

6.18 The Bar Council and the Criminal Bar Association considered that a better solution would be to ensure that magistrates receive adequate training and that they are afforded adequate time to consider applications.

6.19 Two consultees formed a different view. The Financial Conduct Authority ("FCA") queried whether our analysis of the overall number of professional judges in the High Court, Crown Court and magistrates' courts included recorders in the Crown Court and Deputy District Judges (Magistrates' Courts) in magistrate courts. Given that there is likely to be a wider pool of professional judges than we envisaged, they invited us to consider whether it might be realistic for warrant applications to be heard by legally qualified tribunals only. Dijen Basu QC considered that the power to issue a search warrant should be limited to District Judges (Magistrates' Court) given their inherent complexity and the level of intrusion caused.

Analysis

6.20 By seeking views on whether, in certain cases, it should be compulsory for a search warrant application to be made to the Crown Court or District Judges (Magistrates' Courts), it was not our intention to exclude magistrates from the search warrants process. The lay magistracy plays a vital role in the criminal justice system and receives expert legal advice. Properly advised magistrates are clearly capable of dealing with search warrant applications, as they are with a range of other decisions which affect individuals' civil liberties. Nor does it follow that applications to lay magistrates are necessarily to the disadvantage of those against whom the warrant is sought. For example, McCowan LJ observed that a lay magistrate may be more sympathetic to the disruption and distress caused by a dawn raid than a Circuit judge.[28]

6.21 Our intention in seeking views was to gauge appetite for a more formal set of rules concerning the allocation of complex search warrant applications. We do not consider that search warrant applications should *always* be heard by a professional judge. This position was nonetheless advocated for by some consultees. We acknowledge the point made by the FCA that there is likely to be a larger pool of professional judges than we identified in the consultation paper. For this reason, it may be feasible to operate search warrant tribunals where applications are only heard by legally qualified judges. Similarly, as noted by Dijen Basu QC, search warrant applications are often complex and authorise significant intrusion.

6.22 On balance, however, we do not consider that a professional tribunal would be either necessary or desirable. Even were we to ignore the fact that magistrates are capable of handling search warrants applications, based on discussions with stakeholders, we consider that the volume of search warrants would still outstrip the number of available judges. We note in particular that recorders in crime have had their minimum sittings reduced from 30 days to 15; this is despite huge trial backlogs prior to COVID-19. Deputy District Judges (Magistrates' Courts) have also had reduced sittings since COVID-19. There would also be significant cost implications of moving to this model.

6.23 Therefore, we have considered whether there ought to be a more formal set of rules concerning the allocation of complex search warrant applications. We agree with consultees that requiring applications to be made before judges may have unintended consequences for the criminal justice system. Any problems with the existing scheme can be overcome by ensuring adequate training, which we discuss further below.

---

[28] *R v Customs and Excise Commissioners, ex parte X Ltd* [1997] BVC 440.

6.24 In addition, devising an overarching test of "complexity" may be impractical. Questions of complexity are highly fact-specific. We therefore accept that it is unlikely that a sufficiently flexible test could be devised to identify reliably those cases which would be better decided by a professional judge. Current mechanisms which afford a degree of latitude, namely the applicant's choice of court and HMCTS protocol, seem to ensure that search warrant applications are appropriately allocated.

6.25 For the above reasons, other than where already required by statute, we do not consider that it ought to be compulsory for those seeking search warrants to apply to a professional judge in complex cases.

SPECIALIST TRAINING FOR THE MAGISTRACY

The current law

6.26 The current training undertaken by magistrates in relation to search warrants varies considerably.

The consultation paper

6.27 During our discussions with stakeholders before publishing the consultation paper, we were informed that magistrates who deal with search warrants out of hours are specialists who receive additional training. We were also told that in much of the country the same is true of magistrates dealing with applications during court hours. Other stakeholders suggested that magistrates should nonetheless receive training on how to apply the law of search warrants before being able to issue warrants. It was suggested that magistrates need such training in order to apply the relevant statutory tests for each warrant and to scrutinise warrant applications properly.

6.28 Three ways in which this training could be delivered to magistrates were proposed.

(1) One suggestion was "ticketed" magistrates; in other words, a cadre of magistrates with appropriate training who would hear all search warrant applications. However, we did not consider this to be practicable given the element of randomness regarding the availability of magistrates and the substantial volume of work that would likely be needed to set up such a system.

(2) Another suggestion was that there could be a requirement for all bench chairs[29] to undergo specialist search warrants' training as part of the extra training they receive in order to become a bench chair. The advantage of delivering training in this way is that, in the case of an application heard by a full bench under the normal procedure, there will invariably be a bench chair present. The problem, however, is that applications are usually heard by a single magistrate under the "Single Justice Procedure".

(3) The final suggestion was that *all* magistrates should receive appropriate training.

[29] For information on magistrates' bench chairs, see Courts and Tribunals Judiciary, *Bench Chairs*, https://www.judiciary.gov.uk/about-the-judiciary/who-are-the-judiciary/judicial-roles/magistrates/bench-chairmen/.

6.29 Without expressing a view on which course to take, we provisionally proposed[30] that only those magistrates who have received specialist training should have the power to issue a search warrant.

Consultation responses

6.30 Twenty-two consultees answered this question: 19 agreed;[31] one disagreed;[32] and five expressed other views, which included consultees who either agreed or disagreed with the proposal in the main.[33]

6.31 The overwhelming majority of consultees agreed. Their reasons for doing so centred around ensuring that magistrates are equipped with the necessary knowledge and skills to ask questions and make appropriate decisions regarding whether to grant a warrant. All search warrant applications must be thoroughly scrutinised, which magistrates cannot do without training.[34]

6.32 A number of consultees pointed out that training already takes place in certain regions, although improvements could be made to ensure that this is effective. One serving magistrate[35] stated that training comes from two sources. First, training came from observing more experienced colleagues; however, the transition to the single justice procedure was said to have diminished this opportunity. Secondly, ad hoc advice was provided by legal advisers; however, this advice may be varied and appear inconsistent due to the lack of centralised training. A more formal training requirement was described as "essential".[36]

6.33 We received a number of suggestions regarding both the extent to which training should be undertaken and its content.

Extent of training

6.34 One serving magistrate[37] considered that trained bench chairs should be the only magistrates allowed to hear search warrant applications. That consultee accepted, however, that this may not be strictly necessary if there was formal training along with regular updates on procedures and processes that were more widely distributed.

6.35 The Justices' Clerks' Society proposed that there be a national trained panel of magistrates to deal with search warrants. The Society anticipated that HMCTS intends to recommend a national trained panel of magistrates to the Senior Presiding Judge. Such magistrates can

---

30 Consultation Question 18.

31 Robert Della-Sala JP; Nigel Shock JP; Siân Jones; Professor Richard Stone; Crown Prosecution Service; Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Birmingham Law Society; West London Magistrates' Bench; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; The Law Society; Magistrates Association; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Financial Conduct Authority.

32 Senior District Judge (Chief Magistrate).

33 HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); West London Magistrates' Bench; Competition and Markets Authority; Financial Conduct Authority.

34 West London Magistrates' Bench.

35 Robert Della-Sala JP.

36 Southern Derbyshire Magistrates' Bench.

37 Robert Della-Sala JP.

be assigned as required, with other members of the panel available as back up where necessary. Training all chairs, or all magistrates would not be necessary; if all magistrates, or even chairs, were trained, individual justices would hear applications so infrequently that the training would lose most of its effect.

6.36 One consultee, who had sought the opinion of magistrates within their local justice area before responding to the consultation, identified support for more training on search warrants being provided to all magistrates, as an integral part of core training. This would ensure that all magistrates would be better prepared to consider search warrant applications.[38]

6.37 The Magistrates Association acknowledged that specialist training could be regarded as no less necessary for those magistrates who deal with out of hours applications. This is because legal advisers will not be physically present while the application is considered. It was regarded as important that magistrates have sufficient training to be able to identify possible legal queries to raise with the legal adviser.

6.38 The Magistrates Association also suggested that a list should be kept within a Local Justice Area of those magistrates who have completed the necessary training.

Content of training

6.39 We received a number of views on this issue. Emphasis was placed in equal measure on skills and knowledge. In terms of skills, consultees suggested that magistrates need to have the ability to ask appropriate questions of the applicant for the warrant in order to establish whether the statutory criteria are met or not. In terms of knowledge, one point raised was the need to distinguish between the statutory tests of "reasonably believe" and "reasonably suspect".[39]

6.40 It was considered unnecessary to train magistrates in respect of every single warrant that they may encounter.[40] In particular, it was pointed out that it is unrealistic to expect magistrates to carry out the research necessary to identify the legislative criteria they must apply to the application before them.[41] This, it was said, falls more appropriately under the role of the legal adviser. The Senior District Judge (Chief Magistrate) was also hesitant about requiring specialist training given that magistrates should receive search warrants training as part of their initial training and are assisted by trained legal advisers.

6.41 It was suggested that training could be conducted in part online (at least as regards the theory) and in part as practical training.[42] The search warrants' training currently received was described to us as broadly "on-the-job" training. Newer magistrates learn from observing more experienced colleagues in court, from guidance documentation provided (for example, that published by the Justices' Clerks' Society), and from ad hoc advice provided by legal advisers.

6.42 Several consultees suggested that newly appointed magistrates should be required to observe at least two applications being dealt with before being able to deal with applications

---

38 West London Magistrates' Bench.

39 West London Magistrates' Bench; National Crime Agency.

40 Law Society.

41 HM Council of District Judges (Magistrates' Court).

42 West London Magistrates' Bench.

themselves.[43] This was regarded as an important safeguard given that search warrants are usually dealt with by a single justice. There is, therefore, less opportunity for magistrates to observe hearings being conducted by others.

6.43 Consultees also considered that there should be a review of the new appraisal process for magistrates. It does not currently include any assessment for magistrates involved in warrant applications, such as their competence in hearing and issuing search warrants.[44] It was also said that thought would need to be given to whether training should be updated and, if so, how regularly.[45]

Analysis

6.44 While consultees' responses indicate clear support for the requirement of training in principle, it is equally clear that the extent and content of any training could take many forms.

6.45 There are arguments for a training programme to be introduced for all magistrates. There are also good arguments for limiting the training to a specified pool of magistrates who would conduct search warrant application hearings. It is difficult for us to form a definitive view as to the best approach given that the answer would depend in part on whether a specialist panel model is adopted.

6.46 Nor do we consider it necessary to seek to prescribe the exact form any such training should take. We agree with the West London Magistrates' Bench that training could usefully be part theory and part practical. As the Justices' Clerks' Society states, a shadowing scheme would be sensible given that applications are typically dealt with by a single justice. We agree that particular emphasis should be placed on the skills required by magistrates, such as how to conduct effective questioning of those applying for search warrants. We also agree that detailed knowledge of legal provisions is unnecessary in light of the assistance of trained legal advisers who will be advising in every case.

6.47 Putting the practicalities to one side, we are fortified by consultees' responses in our view that, in principle, the power to issue a search warrant should be restricted to those magistrates who have undergone specialist training. We agree that all search warrant applications need a robust assessment and so magistrates must be trained to provide this.

---

43 Justices' Clerks' Society; Magistrates Association.

44 Robert Della-Sala JP; West London Magistrates' Bench.

45 Magistrates Association; National Crime Agency.

Recommendation 19

6.48 We recommend that only those magistrates who have undergone specialist training should have the power to issue a search warrant.

FORMALISING THE REQUIREMENT FOR A MAGISTRATE TO BE ADVISED BY A LEGAL ADVISER

The current law

6.49 At present there is no legal requirement that a magistrate deciding a warrant application should be advised by a legal adviser (a justices' clerk). This contrasts with decisions made by magistrates in criminal trials and sentencing, where the CrimPR require a clerk to be present, unless the magistrate is a District Judge and directs otherwise.[46]

The consultation paper

6.50 There was consensus among stakeholders with whom we discussed this matter that a magistrate hearing a search warrant application should be advised by a legal adviser. The legal adviser enables the magistrate to understand relevant legislative provisions and to assess whether each requirement has been met.

6.51 During working hours, the availability of a legal adviser to assist a magistrate hearing an application for a warrant would rarely pose a problem. We were informed by stakeholders that it would be almost unheard of for a magistrate to deal with a search warrant application without it being scrutinised in advance at some level by a legal adviser. Further, magistrates should always have access to a legal adviser should they wish to obtain advice.

6.52 Some stakeholders suggested nevertheless formalising the requirement for a magistrate hearing an application for a search warrant in court to be advised by a legal adviser. This could be achieved by inserting a requirement into the CrimPR. The reason consultees gave in favour of formalising this requirement was the importance of the availability of legal advice to maximise the prospects of search warrants being issued correctly.

6.53 We invited views[47] on whether, in order to improve judicial scrutiny, there should be a requirement, when a search warrant application is made in court, for a magistrate to be advised by a legal adviser. If so, we asked whether this requirement should also apply to a magistrate who is a District Judge (Magistrates' Courts).

Consultation responses

6.54 Twenty-three consultees answered this question. On the question of whether, when a search warrant application is made in court, there should be a requirement for a magistrate to be advised by a legal adviser: 16 agreed;[48] and seven expressed other views.[49]

---

46 Criminal Procedure Rules, r 24.15.

47 Consultation Question 19.

48 Nigel Shock JP; Professor Richard Stone; Crown Prosecution Service; Council of Her Majesty's Circuit Judges; Birmingham Law Society; West London Magistrates' Bench; Southern Derbyshire Magistrates' Bench; Independent

6.55 On the question of whether there should be a requirement for a District Judge (Magistrates' Courts) to be advised by a legal adviser: one considered that such a requirement should exist, with the option for it to be dispensed with;[50] and 17 considered that such a requirement should not exist.[51]

Requirement for a legal adviser

6.56 Every consultee agreed that a magistrate should be advised by a legal adviser. It was pointed out that assistance should be provided irrespective of whether the application is made in court hours or otherwise.[52] Further, it was accepted that a legal adviser need not be physically present to provide assistance to a magistrate when considering an out of hours application.[53] Consultees also made clear that what already invariably happens in practice is that a legal adviser provides assistance to the magistrate.[54]

6.57 Although there was widespread acceptance that assistance should be, and invariably is, provided, there were very few consultees who addressed whether this arrangement should be formalised. The Serious Fraud Office saw sense in there being a formal requirement. The Financial Conduct Authority also welcomed this suggestion.

Requirement for a legal adviser for District Judges (Magistrates' Courts)

6.58 Virtually every consultee considered that there is no need for a requirement for District Judges (Magistrates' Courts) to be assisted by a legal adviser given that they are legally trained judges. The only consultee who saw merit in District Judges (Magistrates' Courts) being advised by a legal adviser accepted that there should be a power to dispense with the requirement.

Analysis

6.59 In our view, there should always be a legal adviser available to advise a magistrate in respect of search warrant applications. A search warrant involves a serious intrusion of privacy and home rights. If a lay magistrate is issuing a search warrant, they must have legal advice. The question, however, is whether there should be a formal requirement. If there were a formal requirement, we consider that the CrimPR would be the most suitable mechanism for stipulating that requirement.

6.60 There are two possible views that could be taken. The first is that the requirement need not be placed on a more formal footing given that it is firmly established practice. The second is

---

Office for Police Conduct; The Law Society; Justices' Clerks' Society; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Serious Fraud Office; Financial Conduct Authority.

49 Robert Della-Sala JP; Siân Jones; Criminal Procedure Rule Committee; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Kent County Council Trading Standards; Magistrates Association.

50 The Law Society.

51 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Birmingham Law Society; West London Magistrates' Bench; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; Justices' Clerks' Society; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Serious Fraud Office; Financial Conduct Authority.

52 Birmingham Law Society; Law Society.

53 Law Society.

54 West London Magistrates' Bench; Criminal Procedure Rule Committee; Senior District Judge (Chief Magistrate); Magistrates Association.

that it should be formalised given that it is an important safeguard which provides an additional layer of scrutiny. It may also be said that, given it is firmly established practice, there is no harm in putting the requirement in the CrimPR.

6.61 On balance, we take the view that the requirement should be formalised in the CrimPR. The prevailing view is that a magistrate should be advised by a legal adviser. Given that this invariably happens in practice, there is nothing to be lost by formalising the requirement. We are also persuaded by consultees that it is unnecessary for District Judges (Magistrates' Courts) and deputies to be so advised: District Judges (Magistrates' Courts) also very rarely sit with a legal adviser, meaning that this would be unworkable in practice.

Recommendation 20

6.62 We recommend that the requirement for a magistrate hearing a search warrant application to be advised by a legal adviser be formalised in the Criminal Procedure Rules.

A MINIMUM NUMBER OF MAGISTRATES HEARING AN APPLICATION

The current law

6.63 When a search warrant application is made in court it is usually considered by a single magistrate.

The consultation paper

6.64 Given that the execution of a search warrant involves a serious intrusion into privacy rights, some stakeholders we spoke to suggested that such a decision was too important to be taken by a single magistrate.

6.65 In the consultation paper we therefore invited[55] consultees' views on whether, when a search warrant application is made in court to a magistrate, there ought to be a minimum of two magistrates on a bench to consider the application in order to improve judicial scrutiny.

Consultation responses

6.66 Twenty consultees answered this question: none agreed; 18 disagreed;[56] and 2 expressed other views.[57] Therefore, virtually every consultee disagreed with this suggestion. They did so for a number of reasons.

6.67 It was considered that there is no need for there to be two magistrates if there is to be a legal adviser present.[58] Further, it was questioned why, if a single properly advised

---

55 Consultation Question 19.

56 Robert Della-Sala JP; Nigel Shock JP; Siân Jones; Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; West London Magistrates' Bench; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; The Law Society; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Serious Fraud Office.

57 Birmingham Law Society; Financial Conduct Authority.

magistrate is not trusted to do the work on their own, they are on the bench at all.[59] A single magistrate was viewed as the most efficient method of dealing with in hours applications.[60] If the concern was to ensure proper scrutiny of warrant applications, there were more effective ways of achieving that without requiring two magistrates to hear every application. Key mechanisms to ensure adequate scrutiny were seen as training and assistance from a legal adviser.[61]

6.68 Practically speaking, a number of consultees pointed out that both magistrates may reach a different conclusion, creating a split decision.[62] As a consequence, having a bench of two could slow down the procedure for issuing a warrant. To prevent a split decision, three magistrates would be required, incurring even greater cost.

6.69 The cost implications and potential impact on court business was raised as a concern.[63] It was said that the practical impact of requiring two magistrates would, in some cases, be that courts needed to be disbanded for a lack of available magistrates. In addition, the length of time for search warrant applications would generally be increased.

6.70 It was also pointed out that this would create an unprincipled distinction with the out of hours procedure where a single magistrate is entrusted to hear search warrant applications.[64]

Analysis

6.71 For the reasons given by consultees set out above, we agree that it would be unnecessary and undesirable to require a minimum of two magistrates on a bench when hearing search warrant applications. We share the view of the Metropolitan Police Service that effective decision-making by a single magistrate can be secured by training, which we recommend above, and access to a legal adviser, which occurs as a matter of course, and which we recommend be required by the CrimPR.

ISSUING A SEARCH WARRANT DURING OUT OF COURT HOURS

The current law

6.72 Applications for search warrants can be made to a magistrate out of hours at the magistrate's home address. We discuss this procedure in detail at paragraphs 5.102 to 5.109 above.

The consultation paper

6.73 We were keen to understand from consultees' experiences whether the out of hours application procedure created problems in practice. In the consultation paper, we therefore

---

58 Magistrates Association; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Robert Della-Sala JP; The Law Society.

59 Nigel Shock JP.

60 Magistrates Association.

61 Metropolitan Police Service.

62 Robert Della-Sala JP; Nigel Shock JP; Siân Jones; Justices' Clerks' Society;

63 Law Society.

64 Justices' Clerks' Society; Financial Conduct Authority.

invited[65] consultees' views on whether, when applications for search warrants are made to a magistrate out of court sitting hours, the magistrate is always able to obtain the legal advice they need.

6.74 Stakeholders indicated that different practices were adopted across different geographical regions. We therefore also invited[66] consultees' views on the desirability of formalising the magistrates' courts' out of hours procedure for hearing search warrant applications. In particular, we asked whether warrant applications should be:

(1) submitted and heard remotely, unless otherwise directed; and

(2) always made to a legally qualified judge on a regional rota system.

Consultation responses

6.75 Ten consultees[67] answered the question regarding the ability of magistrates to obtain the legal advice they need. In response to the question of formalising the out of hours procedure, 22 consultees answered this question.

(1) In respect of whether search warrant applications ought to be submitted and heard remotely, unless otherwise directed: 14 agreed;[68] and three expressed other views.[69]

(2) As regards the question of whether search warrant applications should always be made to a legally qualified judge on a regional rota system: six agreed;[70] 13 disagreed;[71] and two expressed other views.[72]

Obtaining legal advice

6.76 All those consultees who work within the court system were of the view that legal advisers are currently available to advise magistrates when out of hours applications are made. It was pointed out that legal advisers will make initial contact with the magistrate via telephone to confirm availability to hear the application. At this point legal advisers will provide an outline

---

65 Consultation Question 21.

66 Consultation Question 22.

67 Siân Jones; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Birmingham Law Society; West London Magistrates' Bench; Southern Derbyshire Magistrates' Bench; The Law Society; Justices' Clerks' Society; Magistrates Association; National Crime Agency.

68 Professor Richard Stone; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; West London Magistrates' Bench; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; The Law Society; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Financial Conduct Authority.

69 HM Council of District Judges (Magistrates' Court); National Crime Agency; Birmingham Law Society.

70 Professor Richard Stone; Council of Her Majesty's Circuit Judges; Dijen Basu QC; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Financial Conduct Authority.

71 Robert Della-Sala JP; Siân Jones; Nigel Shock JP; Criminal Procedure Rule Committee; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Birmingham Law Society; West London Magistrates' Bench; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; The Law Society; Justices' Clerks' Society; Serious Fraud Office.

72 National Crime Agency; DS Parminder Kang, Leicestershire Police.

of the application and advise the magistrate. The legal adviser is available by telephone should the magistrate need to speak to the legal adviser again during the hearing.

Remote submissions and hearings

6.77 Every consultee agreed that out of hours search warrant applications ought to be submitted and heard remotely, unless otherwise directed. What was meant by this was that the applicant would send the application by email and the hearing would take place by telephone or video-link. It was considered that this would streamline and improve existing paper-based processes[73] as well as increase consistency and transparency.[74] Further, legal advisers have the technology to be able to advise magistrates appropriately.[75] It was acknowledged that magistrates would require a secure laptop.[76]

6.78 From a law enforcement perspective, it was agreed that remote hearings would reduce travelling time and costs.[77] As a consequence, remote hearings would speed up the process for obtaining urgent search warrants.[78]

6.79 One consultee expressed hesitation on the grounds that there is already a formalised system in place in each region where an "on call" legal adviser is the first point of contact.[79] As discussed in in the chapter above, consultees informed us that remote submissions and hearings for out of hours warrants occur only in the South-East region. In all other regions, applicants have to attend the justice at their home. It was stated that any reformed process must be one that is consistently applied nationally.[80]

6.80 In terms of practicalities, it was suggested that applications should be submitted electronically to a secure mailbox at a minimum.[81] Applications could then be checked by legal advisers before a magistrate deals with them.[82] A telephone conference could be set up as appropriate between the applicant, legal adviser and magistrate.[83]

6.81 It was also suggested that live video link might be preferable to ensure sufficient scrutiny.[84] Stakeholders have repeatedly stated throughout the life of this project just how important it is for the magistrate to be able to see the applicant, even if only virtually. If such a system were adopted, security and reliability of the system would also be important.[85] A dedicated secure

---

73 West London Magistrates' Bench.

74 Magistrates Association.

75 Senior District Judge (Chief Magistrate).

76 National Crime Agency.

77 Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate.

78 Law Society.

79 HM Council of District Judges (Magistrates' Court).

80 HM Council of District Judges (Magistrates' Court).

81 Justices' Clerks' Society; Bar Council and the Criminal Bar Association.

82 Magistrates Association.

83 Justices' Clerks' Society.

84 Magistrates Association.

85 Magistrates Association.

email should have limited access by court staff in order to militate against the risk of tip offs or inadvertent disclosure.[86]

6.82 A separate question is whether, if online out of hours application hearings were to be introduced, it would be preferable for applications to be heard by a magistrate in the same local region as the property to be searched. One consultee considered that there is merit in applications being heard by magistrates who are based locally to the site of a potential search.[87] It was suggested that this local knowledge enables the issuing authority to ask pertinent questions and speeds up the process. In their view, it was regrettable that in many areas arrangements for considering search warrant applications are now centralised. Accordingly, they argued that local courts should be allowed to make their own appropriate arrangements.

Rota system of legally qualified judges

6.83 A small number of consultees agreed with the idea of introducing a national rota system of legally qualified judges to hear out of hours applications remotely. The only consultee who provided reasons for their agreement did so on the grounds that there should be sufficient availability and because out of court emergency applications work well in the High Court.[88] To this end, a similar model could be adopted.

6.84 The point was also made that there is no means at present of applying for a warrant under schedule 1 to PACE, which can only be issued by a Circuit judge, urgently out of hours.[89] It was said to not always be appropriate to apply in court hours, given the potential urgent need to obtain such warrants.

6.85 The majority of consultees disagreed with this suggestion, raising a number of objections. It was pointed out that there is no evidence that, or research into whether, the quality of decision making is affected by whether an application is made in or out of core business hours.[90] Magistrates hear applications outside court hours on other business. It was therefore seen as illogical to hold that magistrates are capable of rational decision making in respect of certain functions but not in relation to search warrants.

6.86 It was also doubted whether out of hours applications were often likely to be of such complexity as to require allocation to a judge.[91] The magistracy is able to undertake this important role.[92] The point was also made that access to a legal adviser ensures that magistrates are able to consider out of court applications on the same basis as in court hours.[93]

6.87 Another issue was raised regarding recruitment. It was suggested that additional District Judges (Magistrates' Courts) would need to be recruited to cover all out of hours

---

86 Financial Conduct Authority.

87 Birmingham Law Society.

88 Bar Council and the Criminal Bar Association.

89 DS Parminder Kang, Leicestershire Police.

90 Robert Della-Sala JP.

91 Criminal Procedure Rule Committee.

92 Senior District Judge (Chief Magistrate).

93 Senior District Judge (Chief Magistrate).

applications.[94] It was doubted that there are sufficient judges available to participate in such a rota, which would have to operate out of hours seven days per week and 365 days a year.[95] Similarly, where work is taken away from other sources, additional magistrates may be required. In addition, introducing a rota system of legally qualified judges would incur large costs.[96]

6.88 It was also suggested that it would be difficult to get support from District Judges (Magistrates' Courts) to participate in an out of hours rota system.[97] District Judges (Magistrates' Courts) would be unlikely to be willing to deal with search warrant applications out of hours after a full day's work, or at the weekend. Participation would be in addition to judges' daily workload which already significantly impinges on their private and leisure time.[98] It was also pointed out that administrative processes may need to be completed after the hearing, including amendment and signature, which the single professional judge would have to complete.[99]

6.89 It was pointed out that there would have to be a backup system in place where a District Judge (Magistrates' Courts) is not available: that backup system is the magistracy.[100]

Analysis

6.90 We agree with the weight of consultees that a rota system of only legally qualified judges is both unnecessary and impractical. We reiterate here our comments at paragraph 6.20 above: with appropriate training and the availability of a legal adviser, a magistrate is clearly capable of dealing with out of hours applications.

6.91 We accept that there may nonetheless be a problem of public perception about the rigour of a system when an investigator visits a person's house out of hours to seek permission to enter premises and make a serious intrusion into another individual's private life. This is particularly so if there is no legal adviser present and no proper recording of the questions asked. In the light of the current pandemic resulting from COVID-19, there is even more reason to reduce in person contact.

6.92 We therefore see merit in formalising a nationwide procedure where applications are submitted and heard remotely. It is clear from consultees' responses that this would save time and money for law enforcement and the courts. Although this may already be occurring in the South-East region, we agree with HM Council of District Judges (Magistrates' Court) that there should be a single process applied consistently across all regions.

6.93 We agree that the general approach to be adopted should reflect the procedures which are being developed in the South-East region. We have set this out in detail at paragraph 5.106 above. We understand that HMCTS is considering implementing this as a national system,

---

94 Nigel Shock JP.

95 HM Council of District Judges (Magistrates' Court); Law Society.

96 HM Council of District Judges (Magistrates' Court).

97 Siân Jones.

98 HM Council of District Judges (Magistrates' Court).

99 West London Magistrates' Bench.

100 Siân Jones.

which we would encourage. In light of consultees' responses, we make a series of further observations.

6.94 It is clear that during court hours remote hearings take place more often by telephone rather than by live link. We are not aware of any out of hours applications being conducted by live link. We agree that live link is to be preferred in principle in out of hours hearings as the magistrate will be able to see the applicant as they are questioned. At the same time, we recognise that it may be preferable for the video link to show only the applicant, with audio for the magistrate who may have been awoken at 2am in their home.

6.95 We do not agree that applications should necessarily be heard remotely by a court local to the premises to be searched. Although local knowledge may assist the magistrate, it cannot be assumed that they will have knowledge of the particular area or premises. Even if they do possess such knowledge, it does not follow that their questions will be more pertinent or the process will be quicker. On the contrary, it may be that fewer questions are asked in respect of areas which are known to be crime hotspots. Nor do we see how it follows that proximity to a local court will influence the degree of candour.

6.96 We also anticipate that the likely success of a remote hearing procedure will be dependent on ensuring that there are an adequate number of available hearing slots. As discussed at paragraphs 5.107 to 5.109 above, we were informed that there can be lengthy delays when arranging out of hours applications. This increases the risk that evidence will be lost and may cause applicants to travel to court at the next available time during court hours to seek an urgent hearing, impacting on court business. As we recommend in the chapter above in respect of in court hours applications, for any out of hours procedure there must be adequate availability.

6.97 While we regard a rota system of *only* legally qualified judges as unnecessary and impractical, there may be merit in having some judges participating in a remote hearing system. This would enable applications for warrants that can only be issued by a particular seniority of judge, such as schedule 1 to PACE warrants, to be capable of being heard urgently out of hours.

6.98 Where the application is urgent, search warrant applications are made immediately at court or, if the courts are closed, outside court hours. However, we were informed that there is an inconsistent practice in terms of the criteria used for determining whether an application is urgent. A nationwide application procedure should permit the urgency of applications to be assessed accurately and consistently, so that urgent applications can be allocated and heard expeditiously.

Recommendation 21

6.99 We recommend that Her Majesty's Courts and Tribunals Service review the current magistrates' courts' out of hours search warrant application procedures across all regions to ensure that:

(1) proper use is being made of technology to increase the efficiency of out of hours applications; and

(2) there are sufficient resources to hear out of hours applications urgently and without undue delay.

FORMALISING THE APPLICATION PROCEDURE DURING NORMAL COURT HOURS

The current law

6.100 We discuss in detail how search warrant applications are heard at paragraphs 5.75 to 5.109 above. We note the varying practice across different regions. The CrimPR sets out a general framework pertaining to the exercise of the court's powers to issue a search warrant. For example, the court must determine an application for a warrant at a hearing.[101] An applicant must confirm, on oath or affirmation, several matters regarding the application,[102] and give answers to questions on oath or affirmation.[103]

The consultation paper

6.101 The courts have repeatedly emphasised the importance of proper judicial scrutiny of search warrants. Given that search powers represent a serious imposition on the privacy of the individual, issuing a warrant should never be treated as a formality. Sufficient time must be made available for the issuing authority to consider the application. Effective scrutiny is needed not only to check that the statutory conditions are satisfied, but also to ensure that the search power is used in a way which is compatible with European Convention rights.

6.102 Stakeholders made several suggestions to embed this principle further and heighten the level of judicial scrutiny. Drawing on their suggestions, we provisionally proposed[104] that the following application process should be put on a more formal basis. Our core aims in devising the procedure were to provide sufficient time to consider applications, heighten judicial scrutiny and improve the overall efficiency of search warrant applications:

(1) applications for a search warrant to a magistrates' court or the Crown Court should be submitted electronically, unless it is not practicable in the circumstances to do so; and

(2) applications to a magistrates' court should be screened by legal advisers who would:

---

101 Criminal Procedure Rules, r 47.25(1)(a).

102 Criminal Procedure Rules, r 47.25(4).

103 Police and Criminal Evidence Act 1984, s 15(4); Criminal Procedure Rules, r 47.25(5)(a).

104 Consultation Question 23.

(a) return applications that obviously do not comply with statutory criteria or contain obvious errors;

(b) forward straightforward applications to the magistrate or judge, to be decided on the documents alone; or

(c) list other cases for a hearing by video link, telephone, or in court, to be arranged with sufficient notice to read the documents in advance and sufficient time at the hearing for adequate scrutiny.

Consultation responses

6.103 Twenty-five consultees responded to our proposals. In respect of whether search warrant applications ought to be submitted electronically, unless not practicable to do so: 18 agreed;[105] and one expressed another view.[106] In respect of whether search warrant applications ought to be screened by a legal adviser, with defective applications returned to the applicant: 15 agreed;[107] one disagreed;[108] and eight expressed other views.[109] As to whether simple search warrant applications ought to be considered and decided on the documents alone: seven agreed;[110] eight disagreed;[111] and two expressed other views.[112] In respect of whether search warrant applications ought to be heard via live link, telephone or in person: 16 agreed;[113] and one expressed another view.[114]

---

105 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; West London Magistrates' Bench; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Independent Office for Police Conduct; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Serious Fraud Office; Financial Conduct Authority.

106 HM Council of District Judges (Magistrates' Court).

107 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Birmingham Law Society; West London Magistrates' Bench; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; National Crime Agency.

108 Metropolitan Police Service.

109 Siân Jones; Kent County Council Trading Standards; Southern Derbyshire Magistrates' Bench; The Law Society; Competition and Markets Authority; Serious Fraud Office; Members of the Senior Judiciary.

110 Professor Richard Stone; Crown Prosecution Service; Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Independent Office for Police Conduct; Bar Council and the Criminal Bar Association.

111 HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Birmingham Law Society; Southern Derbyshire Magistrates' Bench; Justices' Clerks' Society; Dijen Basu QC; National Crime Agency; Metropolitan Police Service.

112 The Law Society; Financial Conduct Authority.

113 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; The Law Society; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; Bar Council and the Criminal Bar Association; Metropolitan Police Service.

114 National Crime Agency.

Submitting applications electronically

6.104 Virtually all consultees agreed with this proposal. Reasons for agreeing included that it would result in a more consistent and efficient process.[115] There were three reasons identified which might impact on the ability of an applicant to submit an application electronically, those were instances where the application:

(1) includes highly sensitive material;

(2) is of such urgency that it is not practicable to arrange a hearing electronically; and

(3) involves maps, diagrams or other material which cannot be easily sent in electronic form.

6.105 A number of consultees made observations about applications involving sensitive material. It was said that applications will need to be transferred on an appropriate secure IT system and, in some cases, delivered by hand.[116] It was suggested that the subsequent storage of warrants and any requests by occupiers to get copies of them should be overseen by a District Judge (Magistrates' Courts), particularly if a sensitive schedule of material has been given to the magistrates.[117]

Screening applications by legal adviser

6.106 The majority of consultees agreed that applications should, in the first instance, be screened by legal advisers. The benefits identified were that it would save court time and improve the quality of applications since there would be greater opportunity for defective applications to be rectified earlier in the process.[118]

6.107 Several consultees observed that filtering already occurs in some court centres. A useful common practice has developed, in courts which do receive digital applications in advance, whereby the legal adviser can return defective applications.[119]

6.108 Some consultees queried what was meant by "filtering" applications. It was generally understood that this would involve vetting applications to reject those that were obviously flawed or which clearly did not contain the rudimentary information to constitute a valid application. This would require the applicant to resubmit an application before it could be pursued.[120]

6.109 One consultee informed us that there are two issues which arise in practice.[121] First, there are some defects, such as the wrong address, which can be easily corrected. The second is the quality of information provided. We were told that some applications have such low prospects of being granted that they will be returned. Others are weak in respect of the

---

115 Magistrates Association.

116 Independent Office for Police Conduct; Bar Council and the Criminal Bar Association.

117 National Crime Agency.

118 Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate.

119 Justices' Clerks' Society.

120 HM Council of District Judges (Magistrates' Court).

121 Siân Jones.

underlying information, but not so weak that the application would not be put before a magistrate.

6.110 One consultee expressed concern that the introduction of a triage system might encourage the issuing authority to assume that the relevant criteria are met.[122] The point was also made that this might in fact create an additional layer of unnecessary bureaucracy and delay.[123]

6.111 Some consultees raised practical considerations. It was observed that, while all warrants used to be vetted by legal advisers, there are not enough legal advisers in some regions.[124] It was also pointed out that for filtering to take place by the legal adviser the applications will need to be received at least 24 hours in advance rather than the morning of the hearing.[125] Legal advisers will need desk time to complete this task.

Dealing with simple applications on the documents alone

6.112 Several consultees were concerned about this proposal. One consultee questioned what was meant by a "simple" application.[126] There was a concern that this could lead to a common practice of granting warrants on the papers alone.

6.113 Several other consultees expressed the view that search warrant applications should always be sworn.[127] To hold otherwise was said to remove a long-established safeguard.[128] There is plenty of case law to the effect that the issuing of warrants should never be a formality and so permitting a paper-based decision process would be a retrograde step.[129]

6.114 Oral hearings also emphasise the gravity of the application and the care required when making it.[130] Paper-based hearings may therefore increase the risk of error.[131]

6.115 It was also pointed out that even seemingly simple applications often benefit from questioning under oath.[132] Search warrant applications often contain missing information, which would prevent them being issued without questioning.[133] The point was also made that the vast majority of hearings will involve questioning.[134]

---

122 Metropolitan Police Service.

123 Metropolitan Police Service; Bar Council and the Criminal Bar Association; Competition and Markets Authority.

124 HM Council of District Judges (Magistrates' Court).

125 Southern Derbyshire Magistrates' Bench.

126 Professor Richard Stone.

127 HM Council of District Judges (Magistrates' Court); Birmingham Law Society, Southern Derbyshire Magistrates' Bench, Justices' Clerks' Society; Dijen Basu QC; National Crime Agency.

128 HM Council of District Judges (Magistrates' Court).

129 Dijen Basu QC.

130 Justices' Clerks' Society.

131 Dijen Basu QC.

132 Southern Derbyshire Magistrates' Bench.

133 Law Society.

134 National Crime Agency.

Arrange hearing via live link, telephone or in person

6.116 The majority of consultees agreed that all search warrant hearings should be listed for a remote hearing by video link, telephone or, if not desirable, be held in person. Consultees saw no reason why technology could not be utilised in this way.[135] Where applications are made remotely, applicants may be in their office where they will have access to additional material relevant to the investigation, thereby making the hearing more efficient.[136]

6.117 It was suggested that video link applications are preferable to telephone applications.[137] This is because there is something more personal about being able to see the applicant, who may also show their warrant card and be seen taking the oath or affirming. One consultee also reported instances of applicants being caught attempting to coach each other's evidence when appearing over video link, which would be more difficult to identify on the telephone.[138]

6.118 Some search warrant applications may still need to be heard in person where the matter is complex or sensitive material is relied upon.[139] It was also said that it must always remain open for applicants to attend a hearing in person and be asked questions on oath.[140]

6.119 There may be practical problems in listing remote hearings.[141] Court centres vary in size. Applications may be squeezed into already crowded lists if there is not a court with dedicated times for applications where hearing slots can be booked in advance.

6.120 Even in the case of a court with dedicated time for search warrant applications, it was emphasised that the procedure must be sufficiently flexible and properly resourced.[142] These were two aspects identified as deficient in existing arrangements. Applications may be sought, or dropped, at short notice and hearings may overrun. It was pointed out that the South-East system had no built-in time for advance reading and screening of applications; slots were limited; and, there was no time available in the scheme for applicants to renew an application.[143] It was said to be imperative that a realistic time frame for reading and hearing the application is put in place.[144]

Analysis

General observations

6.121 We remain of the view that, to the maximum extent possible, there should be regional consistency in relation to the procedure for applying for search warrants. We acknowledge that different court centres will vary in their size and staffing, which may make the

---

135 HM Council of District Judges (Magistrates' Court).

136 Magistrates Association.

137 HM Council of District Judges (Magistrates' Court); Birmingham Law Society.

138 Birmingham Law Society.

139 HM Council of District Judges (Magistrates' Court).

140 Birmingham Law Society.

141 HM Council of District Judges (Magistrates' Court).

142 Law Society.

143 Law Society.

144 National Crime Agency.

introduction of a nationwide unitary procedure difficult. That said, there is clear benefit in a consistent approach to issuing a search warrant.

6.122 We also consider that there ought to be a greater utilisation of technology as a means for making and hearing applications. We see no reason why search warrants should not move to a fully electronic system, with appropriate security measures, to save time and expense. We do not understand why sending maps and diagrams in electronic form need be any more difficult than text.

6.123 At the time of writing, we are in the midst of a pandemic resulting from COVID-19. In the UK alone, tens of thousands of people have lost their lives to the virus, including magistrates and others working in the criminal justice system. We see this as further justifying the implementation of an electronic system (a conclusion that we reached prior to the pandemic), which would remove the need for face to face contact.

6.124 As we discussed at paragraph 6.95 above in the context of formalising an out of hours search warrants procedure, we do not consider that applications should necessarily involve an application by live link to a court centre with geographical proximity to the premises to be searched. We adopt a similar view in respect of applications made during court hours. There may in fact be good reasons for applications *not* being allocated to local courts where there may be a small but appreciable risk that court staff may know an occupier.

Submitting applications electronically

6.125 We consider that applications should be sent electronically, unless impracticable to do so. This should be the case irrespective of whether the application is sent to the magistrates' court or Crown Court.

6.126 We accept that certain applications may need to be made in person for reasons of urgency or security, however, as a general principle electronic submission is clearly to be preferred because of the opportunity for time and cost savings it offers (and, in light of COVID-19, for public health reasons). Although this may already be occurring in practice, we consider that steps could be taken to promote the consistent electronic submission of search warrant applications.

6.127 At Recommendation 13 above, we recommend that HMCTS consider the practicability of an online application portal. This could enable not only the electronic completion of forms, but also electronic submission. In addition to speeding up the process for issuing a warrant, this would bring additional possibilities for attaching other forms of material, listing applications and notifying applicants.

6.128 Even if an online application portal were considered impracticable, or particular agencies were unable to participate in the system, other arrangements could be made to encourage electronic submission. For example, dedicated secure email addresses could be set up to ensure security is maintained.

Filtering applications by legal adviser

6.129 We consider that legal advisers should review search warrant applications sent to the magistrates' court whenever practicable. We understand that this used to be standard practice under a duty clerk scheme, whereby legal advisers would take turns being the duty clerk and review applications before they went to court. We were informed by a former legal adviser that this was a good scheme which stopped owing to staff shortages.

6.130 In our view, the filtering of applications by a legal adviser would save court time and improve the quality of applications by rectifying defective applications early, and so should occur whenever possible.[145] The legal adviser's review should involve vetting the application form for obvious defects. We agree that there are various types of defects, some of which may be more significant. Guidance could helpfully be provided to assist with the difference between defective applications and those which are weak, but not too weak to be put before a magistrate.

6.131 However, we acknowledge the concerns raised by consultees. Given the fact-specific nature of application forms and the fact that the resources to vet all applications cannot be guaranteed, we have concluded that the review by a legal adviser should not be a mandatory requirement. For example, an application may be of such urgency that it should go straight before a judge. Additionally, a legal adviser may not have the desk time to vet the application. It is therefore desirable for legal advisers to review search warrant applications whenever practicable, but we do not consider that it should be a mandatory requirement in all cases to give flexibility to deal with urgent applications and resource constraints.

6.132 On the whole, we do not think that discretionary filtering will lead to unnecessary bureaucracy and delay. Anecdotal evidence from consultees suggests that filtering already happens in some instances and successfully identifies defective applications. Additionally, as indicated at paragraph 6.130, this practice used to occur and operated well.

6.133 Nor do we agree that a more general scheme of filtering would be likely to encourage the issuing authority to assume that the relevant criteria are met. Any issuing authority should know that they must be personally satisfied that there is before them sufficient material on which it is proper to grant the warrant.[146]

Dealing with simple applications on the documents alone

6.134 We agree with the weight of opinion of consultees that any formalised application system should not require search warrant applications to be decided on the documents alone, whether the case is simple or not. This would erode an important safeguard and risk treating search warrant applications as a formality. Additionally, even simple applications may require questions to be put to the applicant.

6.135 We note that the issuing authority may determine an application for a production order[147] in the applicant's absence in the circumstances set out in the CrimPR, r 47.5(2), which too is usually applied for without notice. When permitted by the rules, and where the application has been sufficiently completed and submitted on the correct form, there is a presumption that the application will be dealt with without a hearing. We accept that a similar set of rules would be inappropriate in the search warrants context.

Arrange hearing via live link, telephone or in person

6.136 In the light of the strong support by consultees, we remain of the view that all search warrant hearings should be listed for a remote hearing by video link, telephone or, if desirable, be

---

145 We discuss the position in respect of applications sent to the Crown Court in the next section.

146 *R (Rawlinson and Hunter Trustees) v Central Criminal Court* [2012] EWHC 2254 (Admin), [2013] 1 WLR 1634 at [83]; *R (Hart) v Crown Court at Blackfriars* [2017] EWHC 3091 (Admin), [2018] Lloyd's Rep FC 98 at [18].

147 An investigative power requiring the production of, or access being given to, specified material. See Police and Criminal Evidence Act 1984, sch 1.

held in person. Therefore, the presumption should be that hearings are held remotely, unless there are compelling reasons for a hearing in person. We consider that this would bring a host of benefits: increasing the overall efficiency of the process by saving time, money and making it easier for applicants to provide information in support of the application. We also agree with consultees that this should be technologically feasible. We also note that an applicant can be sworn in over video link proceedings.

6.137 We agree that video link hearings would be preferable where possible as the applicant can be seen by the issuing authority. We visited a virtual courtroom in one police station which had video link facilities and holy books to take the oath or affirm. We can see, however, that this may be more difficult to organise than a conference call in some cases.

6.138 We also see that search warrant applications may still need to be heard in person where the matter is complex or sensitive material is relied upon. Therefore, it must remain open for an applicant to attend a hearing in person at a court centre. We do not seek to attempt to prescribe on what criteria this should occur as it will involve a fact-specific assessment in each case.

6.139 There is also the matter of signing the warrant. In our view, the issuing authority ought to be able to manuscript sign on screen,[148] and there should be a court stamp, albeit digital. While a typed signature may be deemed sufficient, it is much easier to forge and potentially opens the door to fabricated documents. Security must therefore be considered carefully, as with greater digitalisation comes greater possibilities for fraud.[149]

6.140 We agree with the observations made by the Law Society that the procedure must be sufficiently flexible and properly resourced. Even though a system currently operates in certain regions for applications during court hours, there are clearly flaws which are impinging on its successful operation. We would hope that in the intervening time since making this comment, given the greater experience of remote hearings, technical issues can be easily resolved. However, putting these to one side, it remains imperative that there are enough application slots which also provide sufficient time for applications to be read by the issuing authority.

[148] Manuscript signing means that a signatory may use a stylus or finger to inscribe an image approximating to their usual manuscript signature. See Electronic Execution of Documents (2019) Law Com No 386, para A2.3.

[149] We were informed by one senior judge that she has been sent several documents from various jurisdiction in order to confirm whether she had in fact signed them, which she had not.

Recommendation 22

6.141 We recommend that an application system for court hours applications be formalised nationwide to provide that:

(1) applications for a search warrant to a magistrates' court or the Crown Court should be submitted electronically, unless it is not practicable in the circumstances to do so; and

(2) unless it is not practicable in the circumstances to do so, applications to a magistrates' court should be screened by legal advisers, who would:

(a) return applications that obviously do not comply with statutory criteria or contain obvious errors; and

(b) list other cases for a hearing by video link, telephone, or in court, to be arranged with sufficient notice to read the documents in advance and sufficient time at the hearing for adequate scrutiny. There should be a presumption for remote hearings unless there are compelling reasons to hold a hearing in person.

CROWN COURT APPLICATIONS SCREENED BY A LEGAL ADVISER

The current law

6.142 All search warrants which can be issued by a justice of the peace can be issued by judges in the magistrates' court or Crown Court. Certain agencies may apply to the Crown Court either because a statute requires it or because they would prefer the scrutiny of a professional judge. Section 47B of the Criminal Practice Directions discusses several principles to be borne in mind regarding the selection of Crown Court centres for the purposes of an application.

The consultation paper

6.143 Under the search warrants application procedure recommended above, applications sent to the magistrates' court would be screened by a legal adviser unless not practicable in the circumstances to do so. In the Crown Court, however, there are no equivalently qualified court staff who could sift the application before it was considered by a judge. As a result, our recommendation would create a mismatch whereby search warrant applications made before the Crown Court would not be screened for defects.

6.144 We considered whether screening could form part of a wider operation of allocation between court centres. In addition to screening applications, a legal adviser could determine which court would be the most appropriate forum to hear the application. This could lead to cost savings by taking some search warrant applications out of the Crown Court where adequate scrutiny can be given by a magistrate.

6.145 At the same time, we recognised that compulsory filtering might disrupt the practice of law enforcement agencies who often apply to the Crown Court, and might also generate additional work for legal advisers.

6.146 Without reaching a definitive view, we invited[150] consultees' views on whether all search warrant applications should in the first instance be sent to a magistrates' court legal adviser who would:

(1) determine whether the application meets the statutory criteria; and

(2) send on those which do comply to a Circuit judge or District Judge (Magistrates' Courts) or justices as appropriate given the complexity of the case.

Consultation responses

6.147 Twenty-one consultees answered this question:14 agreed;[151] five disagreed;[152] and two expressed other views.[153]

6.148 The majority of consultees agreed with our suggestion, albeit tentatively. The reasons given in support were that it would provide consistency in approach and the potential to divert work away from the Crown Court.[154] Support was also expressed for allowing an applicant to be entitled to state their preferred tribunal.[155]

6.149 However, all respondents, whether agreeing or not, made a number of observations indicating that the procedure would be undesirable.

6.150 Some investigative agencies considered that the requirement would undermine the established and successful practice of submitting applications to particular Crown Courts.[156] For example, Southwark Crown Court has a specialism in considering economic crime cases and is therefore most suited to deal with the unique demands of certain warrant applications.

6.151 It was also said that a system which mandates filtering for applications that are in any event eminently suitable for the Crown Court would be unnecessarily bureaucratic and an inefficient use of the legal adviser's time.[157] Additionally, it would prevent the practice of applicants advising the Crown Court of prospective applications weeks in advance, as the application may, subject to the decision of the adviser, eventually end up in the magistrates' court.[158] The practice of advising the Crown Court of prospective applications was said to be

---

150 Consultation Question 24.

151 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Birmingham Law Society; West London Magistrates' Bench; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; Justices' Clerks' Society; Magistrates Association; Competition and Markets Authority.

152 Dijen Basu QC; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Serious Fraud Office; Financial Conduct Authority.

153 The Law Society; National Crime Agency.

154 West London Magistrates' Bench.

155 Justices' Clerks' Society.

156 Serious Fraud Office; Financial Conduct Authority; National Crime Agency.

157 Serious Fraud Office.

158 Serious Fraud Office.

particularly useful for courts determining the amount of pre-reading and court time required for an application.

6.152 There were also concerns about the capacity of legal advisers being available to fulfil this role.[159] It would stretch the limited resources of legal advisers even further.[160] Allocation decisions might be made based on capacity rather than which court is most appropriate. Submissions might be made to the legal adviser regarding the venue to which it should go.

6.153 Consultees were not aware of Crown Courts being burdened by straightforward warrant applications.[161] They considered it to be the applicant's responsibility to recognise whether their application is sufficiently complex to be better suited to the Crown Court.

Analysis

6.154 Further discussions with the judiciary indicate that it is relatively rare for Crown Court judges to hear search warrant applications. Of those courts that do regularly hear search warrant applications, such as Southwark Crown Court and the Central Criminal Court, applications are typically made by those agencies investigating complex crime. These agencies will have made a reasoned judgment to apply to the Crown Court and will invariably submit long and complex applications, often liaising with the Court well in advance.

6.155 We consider that there is a more fundamental problem with requiring applications to be screened and allocated by a magistrates' court legal adviser in the first instance. In the section above, we recognise that filtering must be optional given that some warrant applications will be urgent and, in some cases, there will not be the resources to vet the application. This creates an issue for allocation if the decision of a legal adviser was to become the only route to an application going before a Crown Court judge. This might cause significant delays or prevent applications ever making it before a Crown Court due to a lack of time to filter the application.

6.156 A workaround for the above issue would be to permit the applicant to indicate a specific court before which the application should be heard. We agree, however, that this might result in applicants making additional submissions and would create an additional layer of work in what is meant to be a speedy process. Further, it would undermine the purpose of the proposal if applications were inevitably to be forwarded to the Crown Court based on the applicant's indication.

6.157 From further discussions with consultees, it has become clear that those who make the considered decision to apply to the Crown Court for a search warrant do so rarely and for sensible reasons. The quality of applications is high and significant amounts of time can be spent on the application. The problems associated with requiring allocation by a legal adviser will outweigh any perceived merits. We acknowledge in particular that a requirement would disrupt the successful practice of specialist agencies.

6.158 In light of these conclusions, we do not consider that search warrant applications made to the Crown Court should be screened by a magistrates' court legal adviser. The investigator should retain discretion to make an application to either court.

---

159 Financial Conduct Authority.

160 Law Society.

161 Bar Council and the Criminal Bar Association.

RECORDING ADDITIONAL MATERIAL PROVIDED DURING HEARINGS

The current law

6.159 During a search warrant hearing, additional information is often provided by applicants in response to questions asked by the issuing authority. These questions are typically asked so that the issuing authority can satisfy themselves that the statutory conditions for the granting of a warrant are met.

6.160 Additional information provided by the applicant during the hearing of a search warrant application should be recorded. This will be done by the judge or legal adviser. Recording ensures that there can be no dispute about what was or was not said to and by the issuing authority. A detailed record also enables a person affected by the warrant and its execution to understand the basis and extent of the interference and facilitates review by the courts.

6.161 The CrimPR require the issuing authority to arrange for a record of the gist of any questions asked and the reply.[162] The accompanying application forms also prompt the issuing authority to summarise any questions and answers raised at the hearing.

The consultation paper

6.162 An inadequate record of the applicant's answers to questions is a frequent complaint and has occasionally led to warrants being held unlawful. Although there is a requirement to provide the "gist" of additional issues which arise during a warrant application hearing, stakeholders have argued that this does not go far enough: instead, hearings should be recorded, either by an audio recording or a verbatim note.

6.163 Our initial analysis led us provisionally to propose[163] that:

(1) there ought to be a standard procedure for audio recording search warrant hearings; and

(2) this should only be transcribed and made available to the occupier in the same way, and on the same conditions, as the information sworn in support of the warrant under the CrimPR, which we set out at paragraph 9.12 below.

Consultation responses

6.164 Twenty-four consultees answered this question. In respect of whether there ought to be a standard procedure for audio recording search warrant hearings: 14 agreed;[164] three disagreed;[165] and seven expressed other views.[166] On the question of whether search

---

162 Criminal Procedure Rules, r 47.25(5)(b).

163 Consultation Question 25.

164 One member of the public; Professor Richard Stone; Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Birmingham Law Society; West London Magistrates' Bench; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Magistrates Association; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Competition and Markets Authority; Financial Conduct Authority.

165 HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate).

warrant hearing transcripts should only be transcribed and made available to the occupier in the same manner as the information sworn in support of the warrant under the CrimPR: 11 agreed;[167] and two expressed other views.[168]

6.165 The majority of consultees agreed that search warrant proceedings should be recorded. The Council of Her Majesty's Circuit Judges noted that it is difficult to find any justification for not recording hearings in the twenty-first century. The Magistrates Association welcomed the proposal to record hearings, which would improve fairness and transparency. Another consultee emphasised to us that the proposal was technically feasible.[169]

6.166 Three consultees disagreed with the proposal. It was pointed out that recording search warrant hearings when no other aspect of a magistrates' court work was recorded (as it is not a court of record) would create a disparate and anomalous practice in the magistrates' court.[170] It was suggested that this could not be justified on the basis of intrusion to property as the magistrates' court frequently imposes orders that involve the loss of liberty and these are not recorded.[171]

6.167 The cost of implementing a secure audio recording and storage system would also be significant.[172] Additionally, there would be difficulties in respect of out of hours applications which occur at a magistrate's home.[173] Adding to this the fact that the failure to record information was rare and that a verbatim transcript rather than a summary would make little difference, it was suggested that the proposal was disproportionate.[174] The better focus was said to be in ensuring that the application fully and properly set out the basis of the application and additional information and findings were recorded.[175]

6.168 Additional concerns were raised by those who supported the proposal. It was pointed out that, if sensitive material is mentioned, there may be a need to ensure that there is limited access to the recording and that any disclosure of an audio recording or transcript is redacted.[176] Storage would have to be secure and take into account data protection safeguards.[177]

---

166 Criminal Procedure Rule Committee; Siân Jones; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; The Law Society; Justices' Clerks' Society; Serious Fraud Office.

167 One member of the public; Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Magistrates Association; Dijen Basu QC; Bar Council and the Criminal Bar Association; Metropolitan Police Service.

168 Serious Fraud Office; Financial Conduct Authority.

169 Dijen Basu QC.

170 HM Council of District Judges (Magistrates' Court); Crown Prosecution Service.

171 Crown Prosecution Service.

172 HM Council of District Judges (Magistrates' Court); Crown Prosecution Service.

173 Senior District Judge (Chief Magistrate).

174 Crown Prosecution Service.

175 Crown Prosecution Service.

176 National Crime Agency.

177 Criminal Procedure Rule Committee.

6.169 It was also indicated that thought would have to be given to the fact that, as the magistrates' courts are not currently a court of record, this may open the door to other proceedings being recorded.[178]

Analysis

6.170 We remain of the view that, in principle, search warrant applications should be recorded. We note that the Independent Office for Police Conduct ("IOPC") has since recommended that HMCTS consider the costs and benefits of implementing audio recording of search warrant application hearings and whether this should form part of the hearing process.[179] In their view, the recording of the search warrant application process would increase public confidence by improving transparency and providing a clear audit trail.[180]

6.171 In response to the IOPC recommendation, HMCTS stated that it would only be possible to introduce recording if there were either a statutory requirement or a judicial direction, neither of which are in place. As a consequence, it was said that reform is a matter for Ministry of Justice policy.

6.172 We agree with the observations made by the IOPC. We acknowledge consultees' concerns, including the cost of implementing a standard audio recording procedure. The practicability of these matters would have to be further considered. We do, however, consider that this may nonetheless be outweighed by the benefit of having such a procedure. For example, audio recordings may assist with bringing and defending civil claims and judicial review applications, and making and defending applications to exclude evidence or to stay proceedings in a criminal context. Equally, the challenges provided by out of hours applications are not insurmountable with technology and with legal advisers involved.

6.173 We agree that care would have to be taken around sensitive material, which may need to be redacted. To this end, we observe that such redaction and considerations of public interest immunity already take place in respect of legal advisers' notes. We consider that proper arrangements can be made to address matters of security surrounding storage.

6.174 Audio recording search warrant applications may open the door to other proceedings being recorded. To some, this may be welcomed. The county court, like the magistrates' courts, is an "inferior court" and yet proceedings are recorded. To take another example, the tribunal responsible for adjudicating on traffic penalty charge notices records its hearings. We express no firm view on this as it is not within our terms of reference; however, we acknowledge that it does mean that the topic of audio recording will likely involve considerations outside the sphere of search warrants.

6.175 If a standard audio recording procedure were to be introduced, we consider that audio recordings should only be transcribed and made available to the occupier in the same way, and on the same conditions, as the information sworn in support of the warrant under the

---

178 Bar Council and the Criminal Bar Association.

179 Independent Office for Police Conduct, *Operation Kentia: A report concerning matters related to the Metropolitan Police Service's Operation Midland and Operation Vincente* (October 2019), p 25.

180 Independent Office for Police Conduct, *Operation Kentia: A report concerning matters related to the Metropolitan Police Service's Operation Midland and Operation Vincente* (October 2019), p 25.

Criminal Procedure Rules. In addition, we observe that in the Crown Court transcripts of search warrant hearings can be ordered to be prepared at the claimant's cost.[181]

Recommendation 23

6.176 We recommend that the Ministry of Justice examines the practicability of audio recording search warrants hearings in the magistrates' courts and out of hours. Should such facilities be available, we consider that audio recordings should only be transcribed and made available to the occupier in the same way, and on the same conditions, as the information sworn in support of the warrant under the Criminal Procedure Rules.

PROVIDING WRITTEN REASONS FOR ISSUING THE SEARCH WARRANT

The current law

6.177 As they stand, neither PACE nor the CrimPR contain an explicit requirement for an issuing authority to produce a written record of their decision to grant or refuse a search warrant. Search warrant application forms do, however, invite the issuing authority to give their reasons.

6.178 Repeated judicial observations indicate that reasons for issuing a search warrant ought to be given.[182] The Divisional Court in *R (Newcastle United Football Club) v Revenue and Customs Commissioners* confirmed that there is a common law duty on courts to give reasons.[183] Importantly, however, the absence of reasons will not necessarily render a warrant unlawful.[184] The ultimate question is whether the statutory test has been properly applied: if the court is still able to discern a sufficient basis for the decision to issue the warrant, the challenge will fail.[185]

The consultation paper

6.179 Following a review of the case law and arguments for and against codification, we provisionally proposed[186] that the requirement for the issuing authority to provide written reasons for issuing or refusing a search warrant should be set out in statute. To retain the current position, we also provisionally proposed that the requirement should not displace the current position in law that a failure to give reasons does not necessarily invalidate a search warrant if it is clear that the court was presented with evidence of sufficient grounds to issue the warrant.

---

181 *Fitzgerald v Preston Crown Court* [2018] EWHC 804 (Admin) at [8].

182 *R v Southwark Crown Court ex parte Sorsky Defries* [1996] COD 117.

183 *R (Newcastle United Football Club) v Revenue and Customs Commissioners* [2017] EWHC 2402 (Admin), [2017] 4 WLR 187 at [51].

184 *R (Newcastle United Football Club) v Revenue and Customs Commissioners* [2017] EWHC 2402 (Admin), [2017] 4 WLR 187 at [51].

185 *R (Newcastle United Football Club) v Revenue and Customs Commissioners* [2017] EWHC 2402 (Admin), [2017] 4 WLR 187 at [56].

186 Consultation Question 26.

6.180 If consultees did not agree, we invited views on other means by which the issuing authority ought to be encouraged to give reasons.

Consultation responses

6.181 Twenty-six consultees answered this question: 17 agreed;[187] six disagreed;[188] and four expressed other views.[189]

6.182 The majority of consultees agreed for the reasons given in our consultation paper. A number of those who did agree were of the view that the rule that failure to give reasons for issuing a search warrant does not automatically invalidate it should remain. Of those who disagreed, a number of different views were expressed.

6.183 It was considered that creating a statutory duty is unnecessary given that application forms already require that reasons must be given.[190] The common law duty to give reasons sufficed, without codification in primary legislation.[191] Another consultee agreed that there was not an issue: a dip sample audit of search warrant applications carried out by HMCTS in the South-East region revealed that reasons were routinely given.[192]

6.184 Warrant decisions should be made on the basis of the warrant application submitted.[193] If provided with a satisfactory application, the court should not detain itself with repeating or rehearsing every conceivable element of the decision-making process.[194]

6.185 Dijen Basu QC considered that there should not be a statutory duty given that the absence of reasons is not necessarily fatal to the lawfulness of the grant of a warrant so long as a sufficient basis to issue the warrant is discernible.

Analysis

6.186 As stated above, the majority of consultees agreed. However, we see particular force in the arguments made by those who disagreed with the provisional proposal. To make clear, we remain of the view that the duty should remain qualified: a failure to give reasons should not necessarily invalidate a search warrant if it is clear that the court was presented with evidence of sufficient grounds to issue the warrant.

---

187 One member of the public; Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; The Law Society; Justices' Clerks' Society; Magistrates Association; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service.

188 Nigel Shock JP; Siân Jones; Criminal Procedure Rule Committee; Crown Prosecution Service; Dijen Basu QC; Serious Fraud Office.

189 Crown Prosecution Service; West London Magistrates' Bench; Competition and Markets Authority; Financial Conduct Authority.

190 Criminal Procedure Rule Committee.

191 Criminal Procedure Rule Committee.

192 Siân Jones.

193 Crown Prosecution Service.

194 Crown Prosecution Service.

6.187 Firstly, as a matter of practicality, in light of discussions with the judiciary and HMCTS, we are not persuaded that putting the requirement to give reasons when issuing a search warrant on a statutory footing would materially affect current practice. Discussions with consultees suggest that reasons are now invariably given. The encouragement of giving reasons also seems a matter more suitably dealt with by training.

6.188 Secondly, we do not consider that the duty would lend itself well to drafting given that it is a qualified duty. As indicated by the *Newcastle United* case, the duty is perhaps best understood not as a duty to give reasons, but to ensure that there is sufficient information to justify the grant of a warrant, which may require reasons where not sufficiently clear.

6.189 For the above reasons, we do not consider that the duty that exists at common law should be set out in primary legislation.

REQUIREMENT TO KEEP RECORDS AND STATISTICS

The current law

6.190 There have been many complaints about the lack of statistical information on search warrants. It has been said that there is little research and insight into search warrants[195] and that records would provide useful information for individuals.[196] Although detailed data is collected and published on detentions, road checks, intimate searches, detention warrants and stop and search, the same is not true of search warrants.

The consultation paper

6.191 In the consultation paper, we suggested that the benefits of collecting and publishing data included greater transparency and higher likelihood of understanding key trends, and responding to them. We also indicated that HMCTS now has software from which relevant data on search warrants can be extrapolated.

6.192 For these reasons, we provisionally proposed[197] that data should be collected and published on the number of search warrant applications received under each statutory basis, together with the number of warrants granted and refused, gathered for each court centre. We also invited consultees' views on what other data ought to be collected.

Consultation responses

6.193 Nineteen consultees answered this question. On the question of whether data should be collected and published on search warrant application numbers, the statutory basis and whether the application was granted or refused: 15 agreed;[198] two disagreed;[199] and three expressed other views.[200]

---

195 K Ewing, *Bonfire of the Liberties: New Labour, Human Rights, and the Rule of Law* (2010) p 41.

196 H Snook, *Crossing the Threshold: 266 ways the State can enter your home* (2007) p 59.

197 Consultation Question 27.

198 Professor Richard Stone; Council of Her Majesty's Circuit Judges; Guardian News and Media; Birmingham Law Society; West London Magistrates' Bench; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Privacy International; Financial Conduct Authority.

6.194 The majority of consultees agreed for the reasons identified in our consultation paper. Siân Jones, Head of Legal and Professional Services at HMCTS, confirmed that HMCTS may potentially have the facilities through the "Applications Register"[201] system to record and report search warrants data. The Southern Derbyshire Magistrates' Bench noted that useful data collection should become a simple task once electronic submission of search warrants applications become the norm.

6.195 The Magistrates Association agreed with our analysis of the potential benefits of data collection. However, they considered it important that necessary resources and structures are put into place to ensure the data is used and disseminated correctly to ensure those benefits identified are achieved.

6.196 The two reasons given by those consultees who disagreed were that it is not clear what purpose such data, collated site by site, would serve and that there is a risk that such data could be misread, misconstrued and then misapplied.

6.197 In addition to the number of search warrant applications received under each statutory power and the number of warrants granted and refused, it was suggested that the following data should be collected:

(1) the identity of the issuing authority, the applicant officer and force;

(2) the number of warrants which are:

(a) successful;

(b) refused and later renewed;

(c) granted after an unsuccessful or amended application;

(d) not executed and the reason why; and

(e) subsequently overturned or quashed (including by consent) together with the reasons for the decision.

Analysis

6.198 Addressing, first, the arguments given by consultees that it was not clear what purpose such data would serve, we consider the purposes are clear: greater scrutiny, transparency in the use of intrusive state powers and the opportunity to understand key trends in the application for, and execution of, search warrants. For example, the data could assist in identifying potentially obsolete search warrant provisions. Additionally, the collection of data may assist with the proper allocation of court resources and identifying areas for training and development.

6.199 We also note that similar recommendations have been made in other jurisdictions. The Victorian Commonwealth Senate Scrutiny of Bills Committee recommended that each agency which exercises entry and search powers should maintain a centralised record of all

---

199 HM Council of District Judges (Magistrates' Court); Crown Prosecution Service.

200 Siân Jones; Crown Prosecution Service; The Law Society.

201 See Search Warrants (2018) Law Commission Consultation Paper No 235, para 5.104.

occasions on which those powers are exercised, and should report those figures annually to Parliament.[202] The New Zealand Law Commission identified several benefits that may arise from the introduction of reporting requirements regarding search powers, including the shedding of light on the value and appropriateness of law enforcement powers, together with the need for changes in substance or procedure.[203]

6.200 As for the risk of data being misconstrued, this relates to how the data is presented. The data would be likely to be handled by experienced individuals, meaning that it could be scrutinised beforehand. Further, any limits or issues with the data could be flagged to prevent misreading. Judicial involvement might also be required.

6.201 We therefore remain of the view that data gathering and reporting would serve a useful purpose, a view with which the majority of consultees agreed.

6.202 Considering what other data ought to be collected, we agree that data by court centre would be important. This should include out of hours applications. Equally, the number of searches pursuant to a warrant in which material is successfully recovered would be useful information. This should not be too significant a burden given that an endorsed copy of the warrant, stating whether the articles or person sought were found, must be returned to the court.[204]

6.203 The remaining suggestions, however, do not seem to serve a clear purpose. We can see how the number of warrants which are subsequently overturned or quashed (including by consent) together with the reasons for the decision could be used to learn lessons to improve the quality of future applications and the decision-making process. However, this suggestion, along with the number of warrants not executed (including the reasons why), would be very time consuming and resource intensive to compile given that it would require detailed investigation and liaising with law enforcement.

---

202 Senate Standing Committee for the Scrutiny of Bills, *Entry and Search Provisions in Commonwealth Legislation*, Fourth Report of 2000, p 80. The Victorian Parliament Law Reform Committee also considered that agencies should report their entry and search activities to Parliament, as a way to ensure that the process is open to public scrutiny. See Victorian Parliament Law Reform Committee, *The Powers of Entry, Search, Seizure, Questioning and Detention by Authorised Persons: Discussion Paper* (2001) p 25.

203 Law Commission Search and Surveillance Powers (NZLC R97, 2007) paras 15.7 to 15.8.

204 Police and Criminal Evidence Act 1984, s 16(9) and (10).

Recommendation 24

6.204 We recommend that the following warrants data be collected and published by Her Majesty's Courts and Tribunals Service, with the assistance of law enforcement agencies where possible:

(1) the number of warrant applications received under each statutory power and by which agency (by court centre, including out of hours);

(2) the number of warrants granted and refused (by court centre, including out of hours); and

(3) the number of searches pursuant to a warrant in which material is successfully recovered.

Chapter 7: The conduct of a search under warrant

INTRODUCTION

7.1 In this chapter, we examine possible reform to various procedural aspects of the execution of a search warrant. We consider reform to the following areas:

(1) specifying who may accompany the person conducting a search under a warrant;

(2) for how long a search warrant should remain valid;

(3) the number of visits to premises that may be authorised under a single search warrant;

(4) accessing all premises occupied or controlled by an individual;

(5) the search of persons on premises during the execution of a warrant;

(6) the time at which the search is conducted;

(7) the information provided to the occupier during the search;

(8) the provision of an authoritative guide to search warrants for occupiers;

(9) informing an occupier how to apply for the underlying information sworn in support of a search warrant application; and

(10) the presence of legal representatives.

7.2 Individual search warrant provisions differ in respect of several of the above matters. In the consultation paper, we concluded that several of these differences could not be justified by the different purposes of the search warrant provisions. In fact, in a number of instances, we were concerned that search warrant provisions do not provide law enforcement agencies with the powers necessary to investigate crime effectively.

7.3 To address these deficiencies,[1] we recommend amending search warrant provisions under several statutes to provide for the authority to enter and search premises on more than one occasion ("multiple entry warrants") and any premises occupied or controlled by a specified person ("all premises warrants"). In order to fill a gap in enforcement powers we also recommend that, where specific conditions are met, a constable be permitted to search a person found on premises where executing a warrant under the Police and Criminal Evidence Act 1984 ("PACE"). To resolve an area of confusion, we also recommend clarifying in a number of Acts that an applicant need only specify the function or description of a person to accompany the officer executing the warrant rather than their name.

7.4 We also concluded in our consultation paper that greater safeguards should be provided to those whose premises are searched. We placed particular emphasis on increasing

[1] Several deficiencies in the powers granted under search warrants concern the application of search warrants legislation to electronic material. We discuss these issues in detail in Chapters 14, 15, 16, 17 and 18 of this report.

transparency in decision-making, clarifying matters which are relevant to executing a warrant in a proportionate manner and improving the information to be provided to occupiers to assist in understanding the extent of the state's powers and their rights.

7.5 We recommend several amendments to Code B of PACE. First, we recommend that it is amended to provide guidance as to what constitutes a reasonable hour when deciding when to execute a search warrant. Secondly, we recommend amending Code B of PACE to clarify when and in what form a search warrant must be provided to an occupier. Thirdly, we recommend amending Code B of PACE to state that an occupier has a right to ask for a legal representative to observe the execution of a warrant.

7.6 We also recommend introducing a statutory requirement for law enforcement agencies executing search warrants to provide an occupier with a notice of powers and rights. In addition, we recommend the introduction of a specific search warrants "your rights and the law" webpage on the Government website. Finally, we recommend that application forms are amended to invite the issuing authority to record their reasons for granting a warrant which may be executed outside usual hours.

SPECIFYING WHO MAY ACCOMPANY A PERSON EXECUTING A WARRANT

The current law

7.7 When a search warrant is issued, it confers lawful authority on a specified official, or officials, to execute the warrant. By "execute the warrant" we mean authority to enter, and invariably search, the premises. For example, under section 8 of PACE, Constable A may apply for a search warrant authorising Constable B and Constable C to execute the search warrant. There is no statutory limit to the number of specified officials who may be authorised to execute a search warrant, subject of course to the principle of proportionality.

7.8 Other individuals may accompany the specified official when executing the search warrant. For example, a digital forensics officer or interpreter may be required. An individual may only accompany the specified official onto the premises if they are authorised to do so. Depending on the statutory provision under which the warrant is sought, a person may be authorised to accompany an investigator by the warrant itself or the investigator may be empowered by statute to choose an individual to accompany them.

7.9 An example where authority for a person to accompany a searcher emanates from the warrant itself is section 16(2) of PACE. This provision provides that a warrant to enter and search premises may authorise persons to accompany any constable who is executing it. In other words, the person accompanying the constable must be specified in the warrant, rather than chosen after the search warrant has been issued.

7.10 This can be contrasted with section 2(7)(b) of the Criminal Justice Act 1987 ("CJA"), which empowers the Director of the Serious Fraud Office ("SFO") to authorise persons to accompany the constable executing the warrant.

The consultation paper

7.11 Stakeholders reported that there is some uncertainty over whether the person accompanying a constable must be a named individual ("Jane Smith") or whether it is sufficient to refer to the role that person will perform in the course of the execution ("a locksmith").

7.12 In policy terms, we did not consider that the law should require a named individual to be identified. Requiring a named individual risks being unnecessarily restrictive, especially as some search warrants are valid for three months; a named locksmith may not be available on a given date chosen to execute the search warrant. It is the function of the individual in the warrant execution process that is relevant, not their name. Specifying a function rather than an individual would reflect the fact that the court issuing the warrant should focus on whether there is a need for that function to be performed. Search records should also document the name of those who attend a search should a name be required at a later date.

7.13 In response, we provisionally proposed[2] that section 16(2) of PACE should permit a search warrant relating to a criminal investigation to authorise the agency executing the warrant to be accompanied either by a named individual or by a person exercising the role specified in the warrant. In addition, we provisionally proposed that this should not displace current statutory provisions which enable persons executing a warrant to have others accompany them in the execution of the warrant without being specified in the warrant.

7.14 While our proposal was limited to section 16(2) of PACE, we intended that section to apply to all warrants sought for the purpose of a criminal investigation. Our underlying policy was therefore that all criminal investigation search warrants should permit an investigator to specify either a named individual or a particular role or position in the warrant.

Consultation responses

7.15 Twenty consultees addressed these issues.

(1) On the question of whether section 16(2) of PACE should permit specification of either a named individual or a particular role or position in the warrant: 16 agreed;[3] one disagreed;[4] and three expressed other views.[5]

(2) As regards whether the above proposal should not displace current statutory provisions which enable persons executing a warrant to take others with them without this being specified in the warrant: 14 agreed;[6] and one disagreed.[7]

7.16 The overwhelming number of consultees agreed with both proposals. It was recognised that requiring a named person might be too restrictive and limit the viability of the search.[8] For example, a person exercising a particular role may be ill on the day of the search.[9]

---

2 Consultation Question 29.

3 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Insolvency Service; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; The Law Society; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Serious Fraud Office.

4 One member of the public.

5 Kent County Council Trading Standards; Competition and Markets Authority; Financial Conduct Authority.

6 HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; The Law Society; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Competition and Markets Authority; Serious Fraud Office.

7 Professor Richard Stone.

7.17 Consultation responses revealed different approaches across law enforcement agencies. One force explained that they set out in their applications for a warrant what type of person would be accompanying the police and their specific expertise and the reason for their attendance. We were informed that in some cases where names are specified, the police have had to make a further application to amend the warrant where a person named on the warrant was unavailable at the date of its execution.

7.18 Given the intrusive nature of search powers exercised under a warrant, it was considered that a warrant should still be required to state the role and number of people accompanying the officer executing the warrant.[10] Proof of that role should still be provided to the occupier.[11]

7.19 Several consultees, while broadly supportive of the proposal, observed that the operational benefits would be limited if it was confined to warrants to which section 16(2) of PACE applies.

7.20 The SFO stated that, in its view, any doubts that exist under section 16(2) of PACE 1984 must also apply to the equivalent power of the Director of the SFO in section 2(7)(b) of the CJA. It submitted that this section should also be amended to clarify that it is permissible to refer to a role rather than a named individual. The SFO explained that this would allow for greater operational flexibility and would obviate the need to revert to the director, where, for example, someone is unavailable at the date of execution.

7.21 The Competition and Markets Authority ("CMA") has found that the current requirement to name officers in warrants issued under the Competition Act 1998 ("CA") and Enterprise Act 2002 ("EA") can present operational difficulties where officers become unavailable at short notice.[12]

7.22 The Financial Conduct Authority ("FCA") pointed out that they can execute a search warrant under the Financial Services and Markets Act 2000 ("FSMA") without the need for a criminal investigation. Therefore, they would need clarification as to whether any change related solely to criminal investigations, otherwise they would have to adopt two different approaches depending on the purpose of their investigation. At present, they specify on their warrants "any investigator from the FCA" and would not want to have to be more specific than that.

Analysis

What should the position be?

7.23 We remain of the view that search warrants should only be required to state the agency or role of the individual who is to accompany the person executing the warrant. This is for several reasons. First, it is the function of the individual that is relevant, not their name, subject to the need to be able to identify them from search records for the purposes of giving

---

8 Magistrates Association.

9 Kent County Council Trading Standards.

10 Magistrates Association.

11 HM Council of District Judges (Magistrates' Court); Dijen Basu QC.

12 See Competition Act 1998, ss 28(2) and 28A(2); Enterprise Act 2002, s 194(2).

evidence at a later date. Secondly, the focus of the issuing authority should be on whether there is a need for that function, be it a locksmith or digital forensics expert.

7.24 Thirdly, we consider that there is no inherent public interest in knowing the name of the person(s) accompanying the person executing the warrant. Nor do we see how a search could be regarded as involving a greater infringement of privacy where a person's role is specified rather than their name. Should either the lawfulness of the warrant, or the way in which it was executed, be challenged, it will be possible to ascertain from search records who accompanied a person on a search if such individuals are needed to give evidence.

7.25 Fourthly, we agree with consultees that to require the name of every individual who may accompany a person executing a warrant risks wasting time and money if new warrants must be obtained where that person is unavailable. This is particularly so given that the name of an individual who may accompany a person executing a warrant is unlikely to influence the granting of a warrant.

7.26 While we regard the reasons justifying this rule as clear, we acknowledge the concerns of consultees regarding the extent to which this rule ought to apply. We agree that the rule should not be limited to the current instances in which section 16(2) of PACE applies. As discussed above, our intention was for the rule to apply to all search warrants relating to a criminal investigation.

7.27 At the same time, as emphasised to us by the FCA, restricting the rule to criminal investigation warrants may create an unprincipled position whereby authorities would be able to specify the function of an individual rather than their name only when carrying out a criminal investigation and not when seeking a warrant for other purposes. Thought should be given to whether the rule should be restricted to search warrants or also include warrants which concern entry and inspection.

7.28 In addition, our proposal was directed at providing clarity as to what information is to be specified on the warrant. It was therefore limited to those instances where authority for a person to accompany a searcher emanates from the warrant. We accept the SFO's concern that the proposal would provide no elucidation of the position for provisions such as section 2(7)(b) of the CJA, which empowers the director of the SFO to authorise persons to accompany the constable executing the warrant, rather than specifying names on the face of the warrant.

What does the current law permit?

7.29 As we stated in the consultation paper, the current law is not clear. Consultation responses reveal a divergence in practice. However, after careful reflection on the position under the current law, we are of the view that the current law *does* permit an individual's role, rather than their name, to be specified by the warrant or an investigator.

7.30 We begin with the wording of the provisions concerned:

(1) sections 16(2) of PACE and 176(5B) of FSMA state that a warrant "may authorise persons to accompany any constable who is executing it";

(2) section 2(7)(b) of the CJA provides that an appropriate person means a "person who is not a member of that office but whom the director has authorised to accompany the constable"; and

(3) the CA and EA are somewhat anomalous given that warrants under the Acts are governed by Practice Directions to the Civil Procedure Rules, which specify that the name of each accompanying person must be given.[13]

7.31 In respect of PACE, FSMA and the CJA, we consider, on a proper construction, that an applicant need only specify the function or description of the person to accompany the officer executing the warrant. Therefore, both specifying a named individual and specifying a description of a person are lawful. In contrast, the CA and EA clearly do require the name, rather than the role, of an accompanying person.

7.32 In reaching this conclusion, we have taken into account the long-established and important canon of legislative construction that statutes permitting interference with the rights of citizens are to be strictly construed.[14] The issuing and execution of search warrants represent a serious intrusion on a fundamental right. On one view, it may be said that the provisions cited above should be strictly construed and require the names of persons accompanying those executing a warrant to be specified.

7.33 We do not see, however, that such an interpretation would accord with Parliament's intention, nor would it achieve just outcomes in practice. The Divisional Court has observed that the provisions of section 15 and 16 of PACE must be applied in a manner which takes careful account of the practical realities of investigations, in that case of running large-scale fraud investigations.[15] In a similar vein, we consider that a pragmatic construction of section 16(2) of PACE and similarly worded provisions leads to the conclusion that an officer need only specify the role of the person intended to accompany the officer executing the warrant.

7.34 In reaching this conclusion, we have taken into account the fact that there is no inherent public interest in knowing the name of the persons accompanying a constable or other investigator. Should a challenge be initiated, the persons accompanying a warrant will be identifiable after the search and therefore will be answerable to their actions.

7.35 We are fortified in our view by the fact that the search warrant application forms authorised for use with the Criminal Procedure Rules ("CrimPR"), in prompting the question which other persons the applicant wants to take part in the search, states: "identify those people by function or description (e.g. scientists, IT experts, accountants)". Guidance note 3C of Code B of PACE also gives the example of "any suitably qualified or skilled person or an expert in a particular field", which also focuses on the function of the individual.

7.36 We reach this view in respect of section 2 of the CJA notwithstanding that it takes a slightly different approach by referring to a person who is not a member of that office but *whom* the director has authorised to accompany the constable. While the reference to a person *whom* the director has authorised to accompany the constable might be read as requiring the authorisation to be of a named individual rather than of a description of a person, we consider that the better view is that section 2(7)(b) should be interpreted in the same way as PACE and FSMA.

---

13 Practice Direction – Application for a Warrant under the Competition Act 1998, para 4.3(7); Practice Direction – Application for a Warrant under the Enterprise Act 2002, para 4.3(9).

14 D Bailey and L Norbury, *Bennion on Statutory Interpretation* (8th ed 2020) paras 27.2 and 27.9.

15 *R (Superior Import / Export Ltd) v Revenue and Customs Commissioners* [2017] EWHC 3172 (Admin), [2018] Lloyd's Rep FC 115 at [85].

Should the current law be amended?

7.37 On one view, the law ought not to be amended: the current law does, in most instances,[16] permit an individual's role, rather than their name, to be specified by the warrant or an investigator. Any statutory amendment would therefore be purely clarificatory, and would therefore require strong justification. Further, a hazard of amending PACE, CJA and FSMA is that it might cause problems for the interpretation of other provisions on the statute book about those accompanying persons exercising warrants.

7.38 We have concluded that there is strong justification for clarifying the law: in particular, PACE, the CJA, FSMA, the CA and EA. Given that the current law in PACE, the CJA and FSMA is ambiguous, it would put the matter beyond doubt in respect of these statutes. The current law is also misunderstood in practice, which leads to procedural inefficiency and has cost implications, further justifying clarificatory amendment. An amendment would also likely be needed to the practice directions governing CA and EA given that they currently require the name, rather than the role, of an individual to be specified.

7.39 In reaching this conclusion, we have formed the view that an amendment to Code B of PACE or other instruments would not put the matter beyond doubt and effect a change in practice in the same way that a clarificatory amendment to a statute would. To the extent that amendment to Code B of PACE would be of benefit, we consider that statutory amendment would prompt this.

Recommendation 25

7.40 We recommend that the following statutes be amended to make clear that an applicant need only specify the function or description of the person to accompany the officer executing the warrant rather than their name:

(1) the Police and Criminal Evidence Act 1984;

(2) the Criminal Justice Act 1987;

(3) the Competition Act 1998;

(4) the Financial Services and Markets Act 2000; and

(5) the Enterprise Act 2002.

THE PERIOD FOR WHICH A SEARCH WARRANT REMAINS VALID

The current law

7.41 Section 16(3) of PACE provides that entry and search under a warrant must be within three months from the date of its issue. This provision provides a general backstop where the specific search warrant provision does not specify the warrant's expiry date. For example, section 46 of the Firearms Act 1968 does not specify for how long the search warrant

[16] As indicated at paragraph 7.30(3) above, the Competition Act 1998 and Enterprise Act 2002 clearly do require the name, rather than the role, of an accompanying person by virtue of the practice directions.

remains valid. The effect of section 16(3) of PACE is therefore that a search warrant under the Firearms Act 1968 is valid for three months.

7.42 Other search warrant powers provide for different periods: for example, a search warrant under section 23(3) of the Misuse of Drugs Act 1971 or section 28(6) of the CA must be executed within one month. A search warrant under paragraph 1(1) of schedule 15 to the Data Protection Act 2018 is valid for seven days from the date of the warrant.

The consultation paper

7.43 In the consultation paper we invited[17] consultees' views on whether there should be uniformity in relation to the period for which a search warrant remains valid. If consultees did not consider that it is necessary to have complete uniformity, we invited views on whether the period of validity for any particular search warrant provision ought to be altered.

Consultation responses

7.44 Twenty consultees[18] answered this question. A wide range of views were expressed. A number of consultees did not see any inherent benefit in uniformity.[19] The Law Society considered it would be inappropriate to amend time limits to create uniformity without a body of evidence supporting the need for uniform time limits. The Birmingham Law Society pointed out that different time limits will reflect different operational requirements.

7.45 Other consultees considered that there should be uniformity.[20] A popular period of validity suggested was one month.[21] The main reasons put forward were to avoid errors, reduce the infringement of rights and because of the risk of changing circumstances over the passage of time. It was also queried why a warrant would need to remain valid for a period as long as three months.

7.46 The National Crime Agency, on the other hand, considered that a uniform period of three months would be desirable. Law enforcement agencies emphasised that many of their operations require numerous warrants and coordination with external agencies and other jurisdictions.[22] As a result, there have been occasions where investigators are pushed close to the three-month limit. The Bar Council and the Criminal Bar Association ("CBA") also saw no reason to decrease the period from three months in respect of those warrants which have such a limit.

---

17 Consultation Question 30.

18 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Guardian News and Media; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; The Law Society; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Competition and Markets Authority; Serious Fraud Office; Financial Conduct Authority.

19 Birmingham Law Society; The Law Society; Independent Office for Police Conduct; The Bar Council and the Criminal Bar Association.

20 National Crime Agency; Dijen Basu QC; Guardian News and Media.

21 HM Council of District Judges (Magistrates' Court); The Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Southern Derbyshire Magistrates' Bench; Justices' Clerks' Society.

22 Financial Conduct Authority; Serious Fraud Office; Competition and Markets Authority; Metropolitan Police Service.

7.47 Another popular view was for the period of validity to be fixed by the issuing authority.[23] This could be subject to a maximum period of validity of three months and feature the option to apply for an extension.

Analysis

7.48 We do not consider that uniformity should be pursued for its own sake. Each provision governs its own subject-matter, within its own enforcement regime, thereby justifying different periods of validity. While uniformity may assist in reducing the risk of errors, applicants operating within particular regimes will be familiar with the time limits which are relevant to them. We have not come across, nor been made aware of, an out of date warrant being executed in error. There is therefore insufficient evidence for us to conclude that provisions should be altered to achieve a uniform period of validity.

7.49 The question remains whether the period of validity provided for under any particular search warrant provision ought to be changed. We recognise the merits of a model where the period of validity is fixed by the judge. In particular, it may be seen as providing greater specificity by aligning the period of validity more closely with that which is necessary in the circumstances.

7.50 On the other hand, there is a risk that investigators will be unduly restricted by a short time frame which is controlled by the practices of the particular issuing authority. Additional submissions would also need to be made regarding the period of validity, slowing down the application process. Circumstances may also change following the issuing of the warrant meaning that it would be preferable to execute the warrant at a later date.

7.51 For these reasons, we consider it better for the investigator to work within the bounds of a fixed statutory time-limit and make the operational decision when to execute the warrant. Often there will be an incentive to execute the warrant as soon as practicable to ensure the preservation of evidence.

7.52 We are not persuaded that a uniform period for execution within one month would be satisfactory, nor that reducing the period of validity of any particular provision to one month would be desirable. Consultation responses from law enforcement agencies suggest that a three-month time-limit may be necessary in complex investigations. A longer period of validity, as is found under the current law, provides greater opportunity for the search to be carried out at a reasonable hour, coordinated with other search teams and arranged with appropriate support to assist with the search.

7.53 It was said by one consultee that any warrant should only be valid for the least amount of time necessary to execute it. In our view, it does not follow that the shorter the period between obtaining and executing a warrant, the more likely the search will be proportionate. Searches should be carried out as expeditiously as possible, however, they must also be carried out safely and with as little negative impact on others as possible.

7.54 In the light of our conclusions above, we do not recommend reforming any of the time limits in respect of search warrant provisions.

---

[23] Professor Richard Stone; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate

THE NUMBER OF TIMES PREMISES CAN BE ENTERED

The current law

7.55 The general rule is that once an investigator has executed a warrant its authority is spent. Therefore, once the investigator leaves the premises that are the subject of the warrant, the only way to re-enter lawfully is to obtain another warrant or the consent of the occupier. The Serious Organised Crime and Police Act 2005 amended sections 8 and 15(5) of PACE to state that a warrant may authorise entry to and search of premises on more than one occasion.

7.56 For multiple entries to premises to be authorised, the issuing authority must be satisfied that it is necessary in order to achieve the purpose of the warrant. The number of entries may be either limited to a maximum or unlimited. If the warrant authorises multiple entries, a police officer of at least the rank of inspector must authorise in writing any subsequent entries.

7.57 A number of other search warrant provisions include a specific power to apply for a warrant authorising multiple entries.[24]

The consultation paper

7.58 Stakeholders informed us that the power to apply for multiple entries remains a useful provision and consideration should be given to extending it across search warrant powers in other Acts.

7.59 In the consultation paper we noted that multiple entry warrants provide clear operational and cost benefits. Against this, we acknowledged the greater interference caused by multiple entry warrants. However, we observed that the current statutory test for authorising multiple entry warrants requires the issuing authority to consider the necessity and proportionality of the measure.

7.60 As this is a finely balanced matter, we invited[25] consultees' views on whether the issuing authority should have the power to authorise multiple searches for all search warrants relating to a criminal investigation. If not, we asked whether there are particular search warrant provisions that should allow for multiple entry warrants.

Consultation responses

7.61 Eighteen consultees addressed these issues: 12 agreed that the power of a judge to authorise multiple entries to premises should be extended to all search warrants relating to a criminal investigation;[26] and six disagreed.[27]

---

24 Immigration Act 1971, s 28FB; Sexual Offences Act 2003, s 96B; UK Borders Act 2007, s 45(2); Serious Crime Act 2015, s 52 and sch 2; Psychoactive Substances Act 2016, s 39.

25 Consultation Question 32.

26 HM Council of District Judges (Magistrates' Court); The Senior District Judge (Chief Magistrate); Guardian News and Media; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Justices' Clerks' Society; Magistrates Association; National Crime Agency; Bar Council and the Criminal Bar Association; Competition and Markets Authority; Serious Fraud Office; Financial Conduct Authority.

27 The Council of Her Majesty's Circuit Judges; Southern Derbyshire Magistrates' Bench; The Law Society; Dijen Basu QC; Metropolitan Police Service.

7.62 The majority of consultees acknowledged the benefits of extending the availability of multiple entry warrants. A number of consultees emphasised that the availability of such warrants should only be extended provided that they are properly authorised and have the necessary safeguards. Further, any extension should only be made where the case has been properly made out.

7.63 Those consultees who did not think that the availability of multiple entry warrants should be extended argued that it was sufficient that section 8 of PACE permits multiple entries. It was also argued that, without evidence of a need for such a power, it would be a disproportionate interference with individuals' rights. Concern was also raised that extending the power may reduce the incentive for investigators to complete the search promptly.

7.64 The SFO considered that extending the availability of multiple entry warrants to warrants under section 2 of the CJA and section 352 of the Proceeds of Crime Act 2002 ("POCA") would be useful. It said that it was not uncommon for their searches to last in excess of a day, and that in such circumstances members of the search team require an overnight rest period during which the warrant must be kept "open" by a constable or member of the SFO (depending on the statutory power) remaining at the premises throughout the night.

7.65 The FCA requested that the option for authorised multiple entry searches should be available under section 176 of FSMA. Given that many of the individuals investigated by the FCA frequently travel, search warrants become useless if the person and their digital devices are not present on the premises, resulting in wasted effort.

Analysis

7.66 We do not consider that an issuing authority should have the power to authorise multiple searches for *all* search warrants relating to a criminal investigation. As Liberty noted during the Home Office's consultation on extending the PACE framework for the issue of a search warrant for all offences, significant privacy issues are engaged by extending multiple entry warrants.[28] Therefore, the power to authorise multiple entry warrants should only be extended where the case for doing so has been properly made out.

7.67 Under the current law, judicial authorisation is granted once, and any further entries are authorised by a police officer of at least the rank of inspector. Searches authorised only by a senior police officer pursuant to a multiple entry warrant represent a greater interference with the right to respect for private and family life of an occupier under article 8 of the European Convention on Human Rights ("ECHR") than searches authorised by an independent judge. Although the European Court of Human Rights ("ECtHR") has observed on a number of occasions that judicial authorisation is not necessary to ensure compliance with article 8 of the ECHR in this context, it is important that counterbalancing safeguards apply which place strict limits on the use of such powers.[29]

---

[28] Liberty, *Response to the Home Office consultation to the Government proposals in response to the Review of the Police and Criminal Evidence Act 1984* (November 2018) para 9.

[29] *Camenzind v Switzerland* (1997) 28 EHRR 458 (App No 21353/93) at [42] and [45]; *Klass v Germany* (1978) 2 EHRR 214 (App No 5029/71) at [55]; *Amarandei v Romania* (2016) App No 1443/10 at [224].

7.68 With the above in mind, we consider that the power to apply for multiple entry warrants is justified in respect of search warrants under section 2 of the CJA, section 352 of POCA,[30] and section 176 of FSMA, for the reasons given at paragraphs 7.64 and 7.65 above.

7.69 The power to apply for multiple entry warrants would provide clear operational benefits. Those agencies which carry out investigations under the CJA, POCA and FSMA deal with complex crime.[31] We consider the extension of multiple entry warrants to these regimes to be both appropriate and desirable to ensure that the provisions are equipped to deal with the realities of modern digital investigations and document-heavy cases.

7.70 In reaching this conclusion, we have also taken into account the fact that the power to apply for a search warrant under PACE has been extended to other investigators. A number of organisations can already apply for multiple entry warrants in respect of their investigations under PACE. These include Welsh Revenue Authority officers;[32] an officer of Revenue and Customs;[33] immigration officers and designated customs officials;[34] officers of the department for Business, Energy and Industrial Strategy;[35] and labour abuse prevention officers.[36]

7.71 It is important that strong safeguards apply. We consider that comparable safeguards to those found in PACE should apply so that multiple entry warrants are only issued and executed where it is necessary and proportionate to do so. As stated by Lord Woolf CJ, sections 15 and 16 of PACE help ensure that a search complies with article 8 of the ECHR.[37]

7.72 Section 15(2)(a)(iii) of PACE requires a constable to state the ground on which they apply for a multiple entry warrant and the number of entries desired. Section 15(5A) of PACE requires a warrant to specify the number of entries authorised. Section 16(3B) of PACE provides that, once premises have been searched for the first time, no premises may be entered or searched any subsequent time unless a police officer of at least the rank of inspector has in writing authorised that entry to those premises. Amendments would also have to be made to the CrimPR application forms accordingly.

7.73 One final point to note is that the legislation that we are recommending be amended extends beyond England and Wales. Section 2 of the CJA and section 176 of FSMA extend to the whole of the UK, while section 352 of POCA extends to Northern Ireland as well as to

---

30 The Law Commission are currently undertaking a project in respect of the confiscation regime under part 2 of the Proceeds of Crime Act 2002. See https://www.lawcom.gov.uk/project/confiscation-under-part-2-of-the-proceeds-of-crime-act-2002/.

31 *R (KBR) v Director of the Serious Fraud Office* [2018] EWHC 2368 (Admin), [2019] QB 675 at [69].

32 Welsh Revenue Authority (Powers to Investigate Criminal Offences) Regulations 2018 (SI 2018 No 400), sch 1, para 1.

33 Police and Criminal Evidence Act 1984 (Application to Revenue and Customs) Order 2015 (SI 2015 No 1783), sch 1.

34 Police and Criminal Evidence Act 1984 (Application to immigration officers and designated customs officials in England and Wales) Order 2013 (SI 2013 No 1542), schs 1 and 2.

35 Police and Criminal Evidence Act 1984 (Department of Trade and Industry Investigations) Order 2002 (SI 2002 No 2326), art 3.

36 Police and Criminal Evidence Act 1984 (Application to Labour Abuse Prevention Officers) Regulations 2017 (SI 2017 No 520), reg 3.

37 *Kent Pharmaceuticals v Director of the Serious Fraud Office* [2002] EWHC 3023 (QB) at [30] by Lord Woolf CJ.

England and Wales. The geographical scope of this project applies to the law of England and Wales. We are not proposing changes that would extend beyond England and Wales.

Recommendation 26

7.74 We recommend that the following search warrant provisions be amended to provide for the authority to enter and search premises on more than one occasion (a "multiple entry warrant"):

(1) section 2 of the Criminal Justice Act 1987;

(2) section 352 of the Proceeds of Crime Act 2002; and

(3) section 176 of the Financial Services and Markets Act 2000.

7.75 The statutory condition for granting such a warrant should be that the issuing authority is satisfied that it is necessary to authorise multiple entries in order to achieve the purpose for which they issue the warrant.

7.76 We also recommend that comparable safeguards to those under the Police and Criminal Evidence Act 1984 should apply.

ACCESSING ALL PREMISES OCCUPIED OR CONTROLLED BY AN INDIVIDUAL

The current law

7.77 All premises warrants allow access to all premises occupied or controlled by a person, both those which are specified in the application and those which are not. An investigator is typically able to apply for this type of warrant when it is necessary to search all premises occupied or controlled by an individual, but it is not reasonably practicable to specify all such premises at the time of applying for the warrant.

7.78 All premises warrants were introduced by amendment to section 8 of PACE by section 113 of the Serious Organised Crime and Police Act 2005. Their introduction was aimed at addressing high level fraud or organised crime where evidence may be moved between locations but where the details of the addresses may only come to light after initial searches of other premises.[38]

7.79 A number of organisations which have the power to apply for a search warrant under PACE can apply for an all premises warrant in respect of their investigations. As with multiple entry warrants, these include Welsh Revenue Authority officers, HM Revenue and Customs ("HMRC") officers, immigration officers and designated customs officials, the Insolvency Service and labour abuse prevention officers. All premises warrants are also available under several other statutory regimes.[39]

---

[38] Home Office, *Policing: Modernising Police Powers to Meet Community Needs – Summary of Responses* (January 2005) p 6.

[39] Immigration Act 1971; Terrorism Act 2000; Terrorism Act 2006; UK Borders Act 2007; Armed Forces Act 2011; Serious Crime Act 2015; Immigration Act 2016; Psychoactive Substances Act 2016; Ivory Act 2018.

The consultation paper

7.80 We did not invite consultees' views on the availability of all premises warrants in our consultation paper. However, consultees raised an issue regarding the availability of all premises warrants

Consultation responses

7.81 Two consultees[40] responded with comments regarding the availability of all premises warrants. All premises warrants are currently not available under section 2 of the CJA, section 176 of FSMA or section 352 of POCA. The SFO argued that it would benefit from the ability to apply for all premises warrants under section 2 of the CJA and section 352 of POCA. The SFO stated that the current requirement to apply for specific premises warrants poses operational challenges where the existence of a previously unknown set of premises is discovered during the course of a search and access is needed without delay to guard against material being destroyed.

7.82 The FCA also stated that it would welcome consideration being given to legislative development to enable courts to issue all premises warrants under section 176 of FSMA and section 352 of POCA. The FCA pointed out that a significant amount of effort is expended in identifying all relevant premises, however, there are instances where the identification of all premises, including storage facilities, used or controlled by the subject is not possible until searches themselves are being conducted. It can be very difficult to establish the locations at which relevant material is likely to be held where an individual operates a transient work or personal lifestyle.

Analysis

7.83 Although we did not directly consult on the matter of all premises warrants, we can see the strength of the arguments made by these consultees. As such, it is an area which we consider could benefit from rationalisation.

7.84 We are, however, anxious not to extend the availability of all premises warrants unnecessarily. As with multiple entry warrants, we do not consider that all premises warrants should be made available in respect of all search warrants relating to a criminal investigation.

7.85 For these reasons, we consider, first, whether extension can be regarded as necessary in respect of the regimes discussed.[41] We then turn to the accompanying safeguards which ensure the power is proportionate and complies with human rights protections for the occupiers and the suspect.

7.86 We accept the argument advanced by the SFO and the FCA that the lack of availability of all premises warrants causes operational difficulties in practice where the existence of additional premises is discovered during a search. There will always be instances in which evidence indicates additional associated premises exist but the exact location is unknown. As a result, we are of the view that the availability of all premises warrants would provide direct operational benefits to investigating cases of fraud and financial crime.

---

40 Serious Fraud Office; Financial Conduct Authority.

41 Criminal Justice Act 1987, s 2; Financial Services and Markets Act 2000, s 176; Proceeds of Crime Act 2002, s 352.

7.87 We consider further, however, whether these operational difficulties stem from a gap in the statutory powers currently available. It appears that there are two potential approaches for responding to the scenario where the existence of additional premises is discovered during a search. The first is to apply for a fresh search warrant in relation to the newly identified premises. The second is to effect a search by other means.

7.88 Considering, first, applying for a new search warrant, we were informed that standard practice where new premises are identified is to apply urgently for a fresh search warrant in the Magistrates' or Crown Court. There are instances, however, where action would be required immediately to preserve evidence. Therefore, in some instances, the opportunity to investigate criminal activity fully is curtailed.

7.89 Where there is a justified reason for obtaining a fresh warrant, logistical and operational difficulties are created. Prosecutors and investigators may have to divert from a live search operation to obtain further warrants. Such urgent applications also create difficulties for busy court schedules.

7.90 The second approach is to effect an arrest by a constable with a view to conducting an urgent search under section 18 of PACE. There is a question as to whether this route would be permissible or rather whether it constitutes a misuse of arrest.[42]

7.91 On a more practical level, this route assumes that there is in fact a suspect in the jurisdiction to arrest. If there is, arresting an individual in order to effect a search would still require both the availability of police support and the occupier to be present on the target premises[43] or present on the premises immediately before arrest.[44] It would also not permit officers other than constables to enter the premises or take part in the search. Such officers may know very little about the investigation or what material is relevant. Any search which did take place may therefore be carried out less effectively than it would otherwise be under a warrant.

7.92 Another concern we have is that greater use of "seize and sift"[45] powers may be made where a constable is unsure of entitlement to seize, to the detriment of both the investigator and the owner of the material. We also acknowledge the concerns expressed by the Law Society in Chapter 4 above, that arrest may have far-reaching effects on an individual, including the potential knock-on effect that the record of that arrest might have for their personal and professional life. We discuss the implications of arrest in more detail at paragraph 3.31 above.

7.93 Neither of these routes offers a perfect solution to the problem that consultees have identified. For this reason, we consider that the power to apply for all premises warrants would be justified in respect of search warrants under section 2 of the CJA, section 352 of POCA, and section 176 of FSMA.

---

42 See paragraphs 5.150 to 5.170 above.

43 Police and Criminal Evidence Act 1984, s 18: a constable may enter and search any premises occupied or controlled by a person who is under arrest.

44 Police and Criminal Evidence Act 1984, s 32; a constable may enter and search any premises in which an arrested person was when arrested or immediately before he was arrested for evidence relating to the offence.

45 Powers of seizure under Part 2 of the Criminal Justice and Police Act 2001 provides the power to seize and sift indeterminable or inseparable material off the premises

7.94 We consider that the power would provide clear operational benefits in respect of the above regimes for the same reasons identified above regarding multiple entry warrants. Those agencies who carry out investigations under the above regimes deal with complex crime. Further, a number of organisations which have had the powers under PACE extended to them can already apply for all premises warrants in respect of their investigations, including HMRC and the Insolvency Service. This is the same list of investigators detailed at paragraph 7.70 above.

7.95 We recognise the human rights concerns associated with all premises warrants. The Joint Committee on Human Rights expressed the view during the passage of the Serious Organised Crime and Police Bill that the power to issue a warrant covering all premises occupied or controlled by a person raises significant human rights concerns.[46]

7.96 In summary, the Joint Committee considered that all premises warrants confer a very wide discretion on public officials with a distinct lack of effective prior judicial control over the decision to enter (if need be, by force) private premises including dwellings.[47] For these reasons, amongst others, the Joint Committee could not be satisfied that the power would be compatible with the right to respect for private and family life, home and correspondence under article 8 of the ECHR.[48] A similar view was reached by Liberty given that entry onto undisclosed premises would lack independent judicial authorisation.[49]

7.97 As we observed above, the ECtHR has observed on a number of occasions that judicial authorisation is not necessary to ensure compliance with article 8 of the ECHR but counterbalancing safeguards must apply which place strict limits on the use of such powers.[50] In the light of these concerns, we consider that the same stringent statutory test and safeguards should apply to all premises warrants as contained under sections 8(1B), 15(2)(b), 15(2A), 15(6)(a)(iv), 16(3A) and 16(9) of PACE. These safeguards will aid in ensuring that all premises warrants are limited to those investigations in which they are strictly necessary and their use is proportionate.

7.98 After discussions with the Office of the Parliamentary Counsel, we have considered how the process for granting an all premises warrant (including the statutory conditions and associated safeguards) might be transposed into the CJA, FSMA and POCA.

7.99 We consider that an all premises warrant under these provisions should confer a power to enter and search any premises occupied or controlled by a person specified in the application, including such sets of premises as are so specified. This wording reflects the current drafting of all premises warrants in other statutory provisions.

7.100 The statutory conditions for issuing an all premises warrant should also be modelled on those currently contained in PACE. Broadly speaking, the conditions ought to be that the issuing authority is satisfied that:

---

46 Joint Committee on Human Rights, *Fourth Report* (Session 2004-05) HL 26/HC 224, para 1.90.

47 Joint Committee on Human Rights, *Fourth Report* (Session 2004-05) HL 26/HC 224, para 1.91.

48 Joint Committee on Human Rights, *Fourth Report* (Session 2004-05) HL 26/HC 224, para 1.96.

49 Liberty, *Serious Organised Crime and Police Bill briefing for the Second Reading in the House of Lords* (March 2005) para 23.

50 *Camenzind v Switzerland* (1997) 28 EHRR 458 (App No 21353/93) at [42] and [45]; *Klass v Germany* (1978) 2 EHRR 214 (App No 5029/71) at [55]; *Amarandei v Romania* (2016) App No 1443/10 at [224].

(1) there are reasonable grounds for believing (or suspecting, if that is the test adopted in the regime) that it is necessary to search premises occupied or controlled by the person in question which are not specified in the application in order to find the documents, information or material specified; and

(2) it is not reasonably practicable to specify in the application all the premises which the person occupies or controls and which might need to be searched.

7.101 These statutory conditions would set a high bar. The FCA considered that the question for the issuing authority should be whether the Crown has presented cogent information that material can be expected to be on other premises. They feared that the above formulation may make all premises warrants unobtainable or more vulnerable to judicial review. However, we consider the test to be appropriate. It reflects the current law and the test which other agencies currently have to pass to obtain all premises warrants.

7.102 Additional safeguards in relation to the application for and execution of a search warrant should be that:

(1) Where an investigator applies for an all premises warrant, they have a duty to state, if the application relates to one or more sets of premises specified in the application, each set of premises which it is desired to enter and search; and

(2) If the warrant is an all premises warrant, no premises which are not specified in it may be entered or searched unless a senior officer[51] has in writing authorised them to be entered.

7.103 We also note the CrimPR search warrant application forms would have to be amended accordingly.

7.104 As explained at paragraph 7.73 above, the geographical scope of this project applies to the law of England and Wales so the changes we are recommending would extend only to England and Wales.

[51] See Proceeds of Crime Act 2002, s 378 for definitions of senior officers. See also the Proceeds of Crime Act 2002 (References to Financial Investigators) (England & Wales) Order 2015 (SI 2015 No 1853) (as modified by SI 2018 No 318, Sch 1), Sch 1.

Recommendation 27

7.105 We recommend that the following search warrant provisions be amended to enable a warrant to provide authority to enter and search any premises occupied or controlled by a person specified in the application, including such sets of premises as are so specified (an "all premises warrant"):

(1) section 2 of the Criminal Justice Act 1987;

(2) section 176 of the Financial Services and Markets Act 2000; and

(3) section 352 of the Proceeds of Crime Act 2002.

7.106 The statutory condition for granting such a warrant should be that the issuing authority is satisfied that:

(1) there are reasonable grounds for believing (or suspecting, if that is the test adopted in the regime) that it is necessary to search premises occupied or controlled by the person in question which are not specified in the application in order to find the documents, information or material specified; and

(2) it is not reasonably practicable to specify in the application all the premises which the person occupies or controls and which might need to be searched.

7.107 We also recommend that comparable safeguards to those under the Police and Criminal Evidence Act 1984 apply.

THE SEARCH OF PERSONS ON PREMISES PURSUANT TO A WARRANT

The current law

7.108 There is nothing in section 8 of, or schedule 1 to, PACE to allow warrants issued under those provisions to permit the police to search persons who are on the premises subject to the search. However, searches of persons in the course of searches of premises are not uncommon: there are several statutory provisions which do permit an investigator to search persons on premises.

7.109 There are powers to search persons on premises which are not connected to search warrant provisions but instead emanate from distinct statutory powers and are exercisable when an investigator is on premises.[52] In the case of section 32 of PACE and section 43(2) of the Terrorism Act 2000, a person must be arrested before they are searched. A person can then be searched for anything which might be evidence relating to an offence,[53] or may constitute evidence that the person is a terrorist.[54]

---

52 For example, Firearms Act 1968, s 47(3); Misuse of Drugs Act 1971, s 23(2); Police and Criminal Evidence Act 1984, s 32; Criminal Justice Act 1988, s 139B(1); Terrorism Act 2000, 43(2); Proceeds of Crime Act 2002, s 289(2); Psychoactive Substances Act 2016, s 36(2); Ivory Act 2018, s 14(2) (not yet in force).

53 Police and Criminal Evidence Act 1984, s 32(2)(a)(ii).

54 Terrorism Act 2000, s 43(2).

7.110 Some powers of search emanate under the authority of the warrant.[55] Typically, these warrants relate to searches for dangerous substances or matters relating to national security. While a constable cannot search persons under a section 8 or schedule 1 warrant, there are examples on the statute book of other officers being empowered to search persons when searching premises pursuant to warrants under these provisions.

(1) Section 114 of PACE provides the power for the Treasury to make an order applying certain provisions of PACE to HMRC officers, and subsection (2)(d) expressly allows such an order to give HMRC officers the power to search persons when they are executing a section 8 or a schedule 1 warrant. The statutory instrument made under this section includes such a power.[56] A search can only occur where the investigator has reasonable cause to believe that person to be in possession of material which is likely to be of substantial value (whether by itself or together with other material) to the investigation of the offence.[57] The order also states that no person should be searched except by a person of the same sex.[58]

(2) A similar power has been provided to immigration officers and designated customs officials by section 23 of the Borders, Citizenship and Immigration Act 2009.[59] In addition to the two requirements of the substantial value of the evidence and the search being by a person of the same sex, two further conditions are set out. First, the power to search a person is only a power to search to the extent that is reasonably required for the purpose of discovering material of substantial value.[60] Secondly, the power to search is not to be construed as authorising an immigration officer or designated customs official to require a person to remove any of his clothing, other than an outer coat, jacket or gloves, but they do authorise a search of a person's mouth.[61]

7.111 Consent is not a valid ground to search a person. This is spelled out in paragraph 1.5 of Code A of PACE,[62] which states:

> An officer must not search a person, even with his or her consent, where no power to search is applicable. Even where a person is prepared to submit to a search voluntarily, the person must not be searched unless the necessary legal power exists, and the search must be in accordance with the relevant power and the provisions of this code.

---

55 Explosives Act 1875; Official Secrets Act 1911, s 9(1); Theft Act 1968, s 26; Misuse of Drugs Act 1971, s 23(3); Landmines Act 1998, s 18(4); Terrorism Act 2000, Sch 5, paras 1, 2, 11 and 15; Anti-terrorism, Crime and Security Act 2001, s 52; Cluster Munitions (Prohibitions) Act 2010, s 22(7).

56 Police and Criminal Evidence Act 1984 (Application to Revenue and Customs) Order 2015 (SI 2015 No 1783), art 18.

57 Police and Criminal Evidence Act 1984 (Application to Revenue and Customs) Order 2015 (SI 2015 No 1783), art 18(a).

58 Police and Criminal Evidence Act 1984 (Application to Revenue and Customs) Order 2015 (SI 2015 No 1783), art 18(b).

59 Police and Criminal Evidence Act 1984 (Application to immigration officers and designated customs officials in England and Wales) Order 2013 (SI 2013 No 1542), arts 8(2) and 17(2).

60 Police and Criminal Evidence Act 1984 (Application to immigration officers and designated customs officials in England and Wales) Order 2013 (SI 2013 No 1542), arts 8(3) and 17(3).

61 Police and Criminal Evidence Act 1984 (Application to immigration officers and designated customs officials in England and Wales) Order 2013 (SI 2013 No 1542), arts 8(4) and 17(4).

62 *R v Keenan* [1990] 2 QB 54.

The consultation paper

7.112 We did not discuss the topic of searching persons pursuant to a search warrant in our consultation paper. However, potential problems with the law were raised in consultation responses from consultees.

Consultation responses

7.113 Three consultees[63] responded with comments regarding the search of persons pursuant to a search warrant. The NCA observed that they are unable to search persons on premises when they are executing a search warrant issued under section 8 of PACE. They suggested that it would be useful to include a power to search people when executing a warrant under section 8 of PACE, noting that HMRC are able to do so under a section 8 warrant.

7.114 Dijen Basu QC, while discussing the problems posed by mobile phones, observed that mobiles will usually be where their owner is and about their person. Additionally, a phone will usually be found, and therefore need to be searched for, on the owner's person, rather than by way of a search of premises under a PACE warrant.

7.115 DS Parminder Kang, a detective sergeant with Leicestershire Police, informed us that it would be of great operational benefit for the police to be able to search persons on premises for evidence of the crime being investigated. It was observed that the police are current permitted to search persons on premises for drugs. It was said that, when police arrive at premises, gaining entry and securing the premises takes time. This may be caused, for example, by being met with serious violence or having to use negotiators. Even in straightforward cases, occupants may see the police arrive. In that time frame, material can easily be transferred to a third-party to hold. Therefore, without a power to search persons on premises in certain circumstances, the police's ability to investigate crime effectively is impeded.

Analysis

7.116 In our view, there are several reasons why a power to search persons pursuant to a warrant under section 8 of PACE would be desirable. This reasoning applies equally to a search under warrant pursuant to paragraph 12 of schedule 1 to PACE, which provides for search warrants in respect of excluded and special procedure material. We use the term "PACE warrant" to cover search warrants issued under both of these provisions.

7.117 First, there are clearly instances where a person may have material on their person which will be of substantial value evidentially. The reasoning behind the HMRC power seems to be that it preserves pre-existing powers to search persons on premises.[64] The justification for preserving the power to search persons centres around the concern that evidence may be concealed by an individual on their person and that it might not be appropriate to arrest everybody found on the premises to locate the evidence.[65] The point has also been made

---

63 National Crime Agency; Dijen Basu QC; DS Parminder Kang, Leicestershire Police.

64 HM Revenue and Customs, *HM Revenue and Customs and the Taxpayer: Modernising Powers, Deterrents and Safeguards: Criminal Investigation Powers: Publication of draft clauses and explanatory notes Responses to the August 2006 consultation document* (17 January 2007) para 4.

65 HM Revenue and Customs, *HM Revenue and Customs and the Taxpayer: Modernising Powers, Deterrents and Safeguards: Criminal Investigation Powers: Publication of draft clauses and explanatory notes Responses to the August 2006 consultation document* (17 January 2007) paras 57 and 58.

that a person, such as a bookkeeper, who is not in their own right considered a suspect, may have evidence on their person.[66]

7.118 We agree with Dijen Basu QC, however, that there is a particularly high likelihood that portable electronic devices such as mobile phones will be on someone's person. These are items commonly searched for under a PACE warrant which further indicates a need for a power to search persons pursuant to a warrant in some instances. We also attach great weight to the response of DS Parminder Kang, which indicates a real risk that relevant evidence may be concealed on a person and highlights that a power to search persons would enable the police to respond flexibly to a range of scenarios that they may be met with on premises.

7.119 Secondly, current statutory powers are insufficient to obtain evidence on an individual's person when executing a PACE warrant. While there are search warrants which permit the search of persons, these relate to specific offences, such as drug, firearm and terrorism investigations. These offences may be different from the offence being investigated under a PACE warrant. For example, a PACE warrant would have to be obtained for a murder investigation.

7.120 Other search powers would still be exercisable while executing a PACE warrant, however, these only permit a search of a person for dangerous articles (such as drugs or firearms) and cash. As we have discussed, it is not just drugs and cash that may be kept in a pocket: where the evidence sought is a mobile phone the powers to search a person for a dangerous article or cash will not be engaged.

7.121 In order to search a person on premises for evidence of an offence where the powers above do not apply, a constable would have to arrest the person and then carry out a search under section 32 of PACE. As we discuss at paragraph 4.102 of the consultation paper, arrest under section 24 of PACE requires particular criteria to be met. Under section 24(1) to (3) of PACE, the criteria are that the person arrested is about to commit, is committing or has committed an offence or the police officer has reasonable grounds for suspecting this to be so. Arrest must also be necessary for one of the reasons identified in section 24(5) of PACE. If the individual on the premises being searched under warrant and on whose person there is evidence is not a suspect, a lawful arrest could not be made.

7.122 Thirdly, to the extent that powers to search persons can currently be used, a power to search persons when exercising powers pursuant to a warrant is more likely to be a proportionate exercise of law enforcement powers. As discussed above, an arrest may have far-reaching effects on an individual, the implications of which we discuss in more detail at paragraph 3.31 above. There is also no restriction on searching for excluded or special procedure material where a person is searched under section 32 of PACE.

7.123 Fourthly, a number of safeguards could be introduced to prevent the power to search persons being used oppressively or unreasonably. These safeguards could also provide standards against which a challenge could be made. The four safeguards which are found in current provisions, which we have set out at paragraph 7.110 above, are:

(1) the investigator must have reasonable grounds to believe that the person to be searched is in possession of material which is likely to be of substantial value

---

66 GOV.UK, *HMRC's criminal investigation powers and safeguards guidance* (May 2019) https://www.gov.uk/government/publications/criminal-investigation/criminal-investigation

(whether by itself or together with other material) to the investigation of the offence for which the warrant was issued;

(2) the power is only a power to search to the extent that is reasonably required for the purpose of discovering any such material;

(3) the power does not authorise an investigator to require a person to remove any of their clothing, other than an outer coat, jacket or gloves but does authorise a search of a person's mouth; and

(4) no person may be searched except by a person of the same sex.

7.124 Fifthly, it seems to us anomalous and without principled basis for HMRC and immigration officers to be able to search persons under a PACE warrant while constables cannot. The rationales behind these powers, namely concealment and impracticability of arrest, apply to constables. We also consider that the underlying rationale of those statutory powers which do empower a constable to search a person on premises apply equally, if not more, in the PACE context where the material sought may be on a person.

7.125 For these reasons, we recommend that there should be a power to search persons pursuant to a search warrant under section 8 of, or paragraph 12 of schedule 1 to, PACE. We consider that the most desirable method of drafting would be for the power to arise where a constable is searching premises pursuant to a PACE warrant rather than stem from the warrant itself. In that respect, we are of the view that the power provided to immigration officers and designated customs officials is the most desirable drafting model.[67]

Recommendation 28

7.126 We recommend that the Police and Criminal Evidence Act 1984 be amended to include a power to search any person found on premises searched pursuant to a warrant under section 8 of, or paragraph 12 of schedule 1 to, the Act. The power should be subject to stringent safeguards regarding when the power can be exercised and the manner in which it can be exercised.

THE TIME AT WHICH THE SEARCH IS CONDUCTED

The current law

7.127 Section 16(4) of PACE and Code B of PACE require any search to be conducted at a "reasonable hour" unless the constable considers that this would frustrate the purpose of the investigation. Lord Woolf CJ has observed that whether a search is conducted at a reasonable hour depends on all the circumstances of the case.[68]

7.128 Where a search warrant is issued other than to a constable, section 16(4) of PACE does not apply. However, where the warrant concerns a criminal investigation, due regard must be had to Code B of PACE.

---

67 Police and Criminal Evidence Act 1984 (Application to immigration officers and designated customs officials in England and Wales) Order 2013 (SI 2013 No 1542), arts 8(2) and 17(2).

68 *Kent Pharmaceuticals v Director of the Serious Fraud Office* [2002] EWHC 3023 (QB) at [18] by Lord Woolf CJ.

7.129 Individual enactments other than PACE may also require a warrant to be executed at a reasonable hour. Where an Act is silent on this issue, it seems that there is no limit to the range of times at which the warrant may be executed.[69]

The consultation paper

7.130 A number of commentators have previously raised concerns regarding the rules surrounding the time at which the search should be conducted. It has been said that the current law suffers from a lack of legal certainty and gives too much discretion to officers, risking inconsistent practices.[70]

7.131 In our consultation paper, we observed that some jurisdictions require search warrants to be executed between certain times during the day.[71] We identified several reasons in favour of restricting the hours during which a search warrant can be executed and requiring express judicial authorisation to search outside of those hours:

(1) night searches can have a particularly severe impact on the privacy of families living at the premises, many of whom may not have been involved in criminal activity;

(2) the ECtHR has indicated that the time of a search is an important factor in determining whether a violation of article 8 of the ECHR has occurred;

(3) where a search warrant is executed late at night or early in the morning, it may be difficult for the occupier to access legal advice; and

(4) requiring the issuing authority to authorise night time searches means that evidence to justify that more serious intrusion into the occupier's privacy would have to be adduced and challenged.

7.132 We then identified a number of counter arguments:

(1) what is "reasonable" will vary from case to case: commercial premises operate at different times and individuals will be present in their dwelling at different times;

(2) introducing such a scheme would create an additional hurdle for investigators to obtain a search warrant by having to satisfy the court that it is necessary to permit the warrant to be valid during certain hours;

(3) circumstances may change once a search warrant is issued, which results in an unforeseen need to conduct a search at a particular time to prevent evidence being lost or destroyed; and

---

69 *R v Adams* [1980] Q.B. 575.

70 *H Fenwick on Civil Liberties and Human Rights* (5th ed 2017) pp 870 to 871; H Snook, *Crossing the Threshold: 266 ways the State can enter your home* (2007) p 59.

71 These include the Federal Rules of Criminal Procedure (United States), r 41(e)(2)(A)(ii): the hours during which a search warrant must be executed, unless the judge for good cause expressly authorises execution at another time, are 6am to 10pm) and Canada (Criminal Code RSC, 1985, c C-46, s 488: the hours during which a search warrant must be executed, unless the justice is satisfied that there are reasonable grounds for it to be executed by night, are 6am to 9pm).

(4) the execution of a search warrant is an operational issue, which arguably should be left to the discretion of the investigator subject to the current limitations.

7.133 On balance, we considered that, where it may be necessary to execute a search warrant late at night or early in the morning, prior judicial authorisation should be required. We provisionally proposed:[72]

(1) where an investigator seeks to execute a search warrant between the hours of 10pm and 6am, prior judicial authorisation to do so should be required;

(2) the existing rule, that searches under warrant must take place at a reasonable hour unless it appears to the constable that the purpose of a search may otherwise be frustrated, should continue to apply; and

(3) a search warrant should be required to state whether it authorises a search only between 6am and 10pm or at any time.

7.134 We also invited consultees' views on whether further guidance should be provided on what is likely to constitute a reasonable hour in the case of residential and commercial premises.

Consultation responses

7.135 Eighteen consultees addressed this issue. On the question of whether prior judicial authorisation ought to be required for searches between the hours of 10pm and 6am: 10 agreed;[73] and eight disagreed.[74] On the question of whether further guidance should be provided on what is likely to constitute a reasonable hour in the case of residential and commercial premises: eight agreed;[75] and three disagreed.[76]

Prescribed times

7.136 A small majority of consultees agreed that there should be prescribed times for executing a search warrant. The main reason given in support of this change was to increase the likelihood that a search will be proportionate. Some consultees considered that it would be very unusual to need to execute a warrant between 10pm and 6am.[77] Two consultees suggested requiring judicial authorisation for searches between 10pm and 7am.[78]

---

72 Consultation Question 32.

73 Council of Her Majesty's Circuit Judges; Guardian News and Media; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Independent Office for Police Conduct; The Law Society; Justices' Clerks' Society; Magistrates Association; Bar Council and the Criminal Bar Association; Professor Richard Stone.

74 Senior District Judge (Chief Magistrate); Dijen Basu QC; Southern Derbyshire Magistrates' Bench; National Crime Agency; Metropolitan Police Service; Serious Fraud Office; Competition and Markets Authority; Financial Conduct Authority.

75 Council of Her Majesty's Circuit Judges; Birmingham Law Society; Southern Derbyshire Magistrates' Bench; The Law Society; Justices' Clerks' Society; Magistrates Association; Bar Council and the Criminal Bar Association; Serious Fraud Office.

76 Independent Office for Police Conduct; National Crime Agency; Metropolitan Police Service.

77 Independent Office for Police Conduct; Law Society.

78 Justices' Clerks' Society; Professor Richard Stone.

7.137 A significant number of consultees disagreed that the law should prescribe the time at which a warrant can be executed. They raised a number of arguments against the proposal.

7.138 It was stressed that officers require flexibility when dealing with dynamic situations and this cannot always be foreseen by the court issuing the warrant.[79] The decision around time of entry should always remain with the agency executing the warrant, based on the risk and operational need.[80]

7.139 It was also observed that circumstances often change in investigations.[81] Therefore, what might otherwise have been a reasonable hour may become an unreasonable hour. Prescribed times create a false assumption that reasonableness is wholly dependent on the time of the search. Given that circumstances may change in an investigation, it was suggested the current requirement that search warrants must be executed at a reasonable hour is flexible enough to meet the justice of every situation.

7.140 It was said that the time at which warrants are executed rarely causes a problem in practice, suggesting that the reasonable hours requirement operates well.[82] It was also argued that the "reasonable hour" requirement strikes a fair balance between the rights of occupiers and operational considerations which will vary depending on the nature of the investigation.[83]

7.141 Some consultees thought that it was unclear under our proposal what the position would be where a search is likely to continue past 10pm.[84] It was pointed out that it is not uncommon for large scale criminal investigations searches to last in excess of a day and occupiers may prefer the search team to continue working late into the night rather than leaving for an overnight rest and returning in the morning. The Bar Council and the CBA accepted that a cut-off point once lawful entry had been effected would be a hindrance in practice.

7.142 A number of consultees, while disagreeing with the proposal to introduce prescribed hours, made other suggestions for reform. Dijen Basu QC considered that there would be no harm in including within the prescribed application form a requirement to provide details of the intended execution time and date and a detailed rationale for it. The Senior District Judge (Chief Magistrate) considered that the issuing authority should always record in its reasons where warrants may be executed outside usual hours.

Guidance on the reasonable hour requirement

7.143 The majority of consultees agreed that there should be greater guidance on what constitutes a "reasonable hour" for the purpose of executing a search warrant.

7.144 The SFO noted that the present iteration of Code B no longer contains guidance on timing for officers, and suggested that it would be a useful addition to the next edition of the code.

7.145 The Magistrates Association stated that an important and relevant factor as to the possible impacts of carrying out a search at night is the presence or likely presence of children or

---

79 Senior District Judge (Chief Magistrate).

80 National Crime Agency.

81 Dijen Basu QC.

82 Dijen Basu QC.

83 Serious Fraud Office.

84 Serious Fraud Office.

other vulnerable people. It is therefore important that in making an application, police have taken reasonable steps to identify the presence of children or vulnerable people and indicate, on the face of the search warrant, if it is believed they may be present. The Bar Council and the CBA observed that the rights of children are guaranteed by article 8 of ECHR as incorporated by the Human Rights Act 1998 and the UN Convention on the Rights of the Child, article 3 of which requires action to take full account of the best interests of the child.

7.146 The Bar Council and the CBA also noted that different approaches need to be adopted in relation to residential property and commercial premises.

Analysis

7.147 Our overarching aim is to ensure that any entry and search under warrant is always proportionate. Our provisional proposal was designed to ensure that the issuing authority gave proper thought to whether executing a search warrant during the hours of 10pm to 6am was necessary. In the light of the consultation responses, we consider that a degree of uncertainty is preferable to stricter requirements which risk fettering operational decision making. In reaching this conclusion, we have also formed the view that judicial scrutiny of the proposed timing to execute a warrant can be achieved by other means.

7.148 As Lord Woolf CJ observed, whether a search is conducted at a reasonable hour depends on all the circumstances of the case.[85] This is a fact-sensitive matter which necessarily implies a degree of legal uncertainty under the reasonable hour requirement. After further consideration we are persuaded that this flexibility is necessary, desirable and allows adaptation to the circumstances of each case.

7.149 We have sought further clarification from law enforcement agencies regarding the potential impact of the provisional proposal that we made in the consultation paper. We are persuaded that imposing set times within the law risks creating unnecessary rigidity and could affect operational decision-making. For example, drug operations usually involve transient material. Intelligence may indicate that material is to be suddenly removed from the premises. Were this to occur during at a time which has not been judicially authorised, the window of opportunity would be lost. This would be the case even though execution of the warrant at that time would otherwise be deemed a reasonable hour.

7.150 A number of consultees agreed with the proposal on the basis that it would be very unusual to need to execute a warrant between 10pm and 6am. Consultation responses from law enforcement agencies have indicated that it is not in fact that uncommon for search warrants to be executed between 10pm and 6am. The decision will be likely to be dictated by intelligence, which may indicate that a person is on the premises during a particular window of time.

7.151 Further, the proportionality of the search would still be dependent on the final decision of the investigator as to when exactly to execute the warrant within the prescribed times. We agree with those consultees who argued that the current test offers flexibility while requiring consideration of the reasonableness of the search. It is for these reasons that we do not recommend the introduction of prescribed times for executing a search warrant.

---

[85] *Kent Pharmaceuticals v Director of the Serious Fraud Office* [2002] EWHC 3023 (QB) at [18] by Lord Woolf CJ.

7.152 We recommend at paragraph 4.80 above that application forms should invite applicants to include the anticipated timing of the search. We would add to this the suggestion from the Senior District Judge (Chief Magistrate) that the court should always record in the reasons where warrants may be executed outside usual hours. This requirement would encourage the issuing authority to consider whether it would be proportionate to conduct the search outside reasonable hours.

Recommendation 29

7.153 We recommend that the Criminal Procedure Rule Committee consider amending application forms to invite the issuing authority to record their reasons for granting a warrant which may be executed outside usual hours.

7.154 Finally, we consider that Code B of PACE should provide guidance as to what constitutes a reasonable hour. We noted at paragraph 6.57 of our consultation paper that guidance note 5A of the 1995 edition of Code B of PACE provided considerations to which the officer in charge should have regard. It is not clear why these were removed in subsequent editions. We are of the view that it would be worthwhile reinstating relevant considerations. We consider that the guidance note should include reference to:

(1) the impact of carrying out a search at night in the presence or likely presence of children or other vulnerable people; and

(2) the different considerations to which regard should be had when searching commercial and residential premises.

Recommendation 30

7.155 We recommend that the PACE Strategy Board consider amending Code B of the Police and Criminal Evidence Act 1984 to provide guidance as to what constitutes a reasonable hour, including consideration of:

(1) the impact of carrying out a search at night in the presence or likely presence of children or other vulnerable people; and

(2) the different considerations to which regard should be had when searching commercial and dwelling premises.

THE INFORMATION PROVIDED TO THE OCCUPIER DURING THE SEARCH

The current law

7.156 Section 16(5) of PACE provides that, if the occupier is on the premises at the time of the search, they must be provided with documentary evidence of the status of the person conducting the search; have the search warrant itself produced; and be supplied with a copy of it. Section 16(6) of PACE applies in the same way where the occupier is not on the premises but there is some other person who appears to be in charge.

The consultation paper

7.157 In the consultation paper, we observed that section 16(5) of PACE has become heavily qualified by the case law. In particular, case law states:

(1) what information is to be produced when executing a warrant (a copy of the full warrant including any schedules);

(2) the meaning of a warrant being "produced", namely that the occupier is given a chance to inspect the warrant;

(3) the circumstances under which a warrant need not be produced, namely where it appears to the officer, once lawful entry is effected, that the search may be frustrated;[86] and

(4) when it is permissible to redact the mention of other premises on the warrant in the case of all premises warrants.

7.158 To ensure these observations are followed consistently, we provisionally proposed[87] that section 16(5) of PACE ought to be amended to take account of the developments in case law specified above.

Consultation responses

7.159 Seventeen consultees answered this question: 16 agreed in full;[88] and one expressed another view.[89] Every consultee but one agreed with our provisional proposal to amend section 16(5) of PACE. The SFO took a slightly different view, arguing that guidance in Code B of PACE would be preferable to statutory amendment for two reasons. First, Code B of PACE is more likely to be read by officers. Secondly, the SFO queried whether augmenting section 16(5) of PACE may overload the provision, thereby rendering it less comprehensible.

Analysis

7.160 While every consultee agreed with our provisional proposal, the SFO provided the most comprehensive response to the consultation question. We agree with the SFO that Code B of PACE, and in particular a guidance note, is a more suitable place in which to state developments from case law. In this regard, we are differing with the majority only on the point of where the change should be.

---

86 For example, in *R v Longman* [1988] 1 WLR 619, the occupier, who was storing drugs at the premises, lunged at a police officer with a knife when it was discovered that the officers were in fact police officers and not delivering flowers. It was held that subterfuge could be used to gain entry to the premises before complying with the requirements of the Police and Criminal Evidence Act 1984, s 16(5).

87 Consultation Question 33.

88 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; The Law Society; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; National Crime Agency; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Financial Conduct Authority.

89 Serious Fraud Office.

7.161 Code B of PACE is more likely to be read by officers. Further, the developments identified expand on the statutory wording, they do not drastically alter the meaning of it. Such expansion is well suited for Code B of PACE. We also agree that statutory expansion risks making section 16(5) of PACE less comprehensible.

Recommendation 31

7.162 We recommend that the PACE Strategy Board consider amending Code B of the Police and Criminal Evidence Act 1984 to take account of developments in case law, namely to clarify that:

(1) a copy of the full warrant must be supplied, including any schedule appended to it;

(2) a warrant is "produced" where the occupier is given a chance to inspect it;

(3) non-compliance with section 16(5)(a) and (b) of PACE may be justified where it appears to the officer, once lawful entry is effected, that the search may be frustrated; and

(4) it is permissible for all premises warrants to be redacted to omit the identity of other premises to be searched.

AN AUTHORITATIVE GUIDE TO SEARCH POWERS

The current law

7.163 As indicated at paragraph 7.156 above, section 16(5) and 16(6) of PACE require various items of information to be disclosed to an occupier. If an officer conducts a search to which Code B of PACE applies, Code B of PACE states that the officer shall, unless it is impracticable to do so, provide the occupier with a copy of a "notice of powers and rights".[90] Code B of PACE prescribes the matters that should be included in a notice of powers and rights and the manner in which it should be given to the occupier.[91]

The consultation paper

7.164 Concern has been raised that occupiers are not provided with sufficient information to understand what can and cannot occur during a search. Professor Helen Fenwick has argued that section 16(5) of PACE is presentational in nature and in fact serves little purpose as it does not provide much detail about how a search should be conducted.[92] One stakeholder with whom we met who worked for a law enforcement agency suggested that the occupier should be given a copy of the statutory provision authorising the entry and search of their home.

7.165 In our consultation paper, we emphasised strongly that an occupier should be provided with information about the law governing search warrants. We were not convinced though that

---

90 Code B of PACE (2013) para 6.7.

91 Code B of PACE (2013) paras 6.7 and 6.8.

92 *H Fenwick on Civil Liberties and Human Rights* (5th ed 2017) p 870.

this would be best achieved by providing copies of legislation, which might be difficult for someone without legal training to understand. Instead, we provisionally proposed[93] that a person executing the warrant should provide the occupier with an authoritative guide to search powers, written in plain English for non-lawyers and available in other languages.

Consultation responses

7.166 Twenty-one consultees answered this question: 16 agreed;[94] and five expressed other views.[95] No consultee disagreed with the argument in principle of giving occupiers more information concerning search warrants. However, a number of practical points were raised, and additional comments made.

7.167 It was argued that arrangements should be made where the premises are known to contain non-English speakers.[96] It was pointed out that the provision of an authoritative guide, especially in languages other than English, may not always be practicable immediately or foreseeable in certain circumstances.[97]

7.168 Several concerns stemmed from the time and cost implications which might be imposed on law enforcement agencies. One consultee suggested that the authoritative guide should be centrally produced, rather than an expectation being placed on individual enforcement bodies to produce their own.[98] Another consultee pointed out that creating guides for each warrant they can execute would be a significant undertaking.[99]

7.169 It was argued that it is unnecessary to provide the guide in hard copy, with the warrant, at the premises and that online information should suffice.[100] Another consultee saw merit in also providing a website link to an online guide for individuals.[101]

7.170 Some consultees queried whether the guide would be necessary given the potential overlap with the notice of powers and rights.[102] Paragraph 6.7 of Code B of PACE (and paragraph 7.1 of the Home Office Powers of Entry Code of Practice) requires an occupier to be provided with a notice of powers and rights. The standard format notice includes an explanation of the extent of the powers of search and seizure conferred by PACE and the rights of the occupier or owner of the property seized. Crucially, a notice of powers and rights need not be provided if it is impracticable to do so.

---

93 Consultation Question 34.

94 One member of the public; Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; The Law Society; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Privacy International.

95 Kent County Council Trading Standards; National Crime Agency; Competition and Markets Authority; Serious Fraud Office; Financial Conduct Authority.

96 Birmingham Law Society.

97 Senior District Judge (Chief Magistrate); Metropolitan Police Service.

98 Independent Office for Police Conduct.

99 Kent County Council Trading Standards.

100 Metropolitan Police Service.

101 Bar Council and the Criminal Bar Association.

102 National Crime Agency; Serious Fraud Office; Financial Conduct Authority.

7.171 In terms of content, it was suggested that the guidance should specify the right to obtain the information provided in support of the warrant and how to do so, rights of challenge, appeals, rights to compensation, and how to access legal advice.[103] It was also suggested that the guide should set out the powers of the police.[104]

Analysis

The notice of powers and rights

7.172 Having considered carefully the consultation responses, we remain of the view that occupiers should be given a guide to search powers, written in plain English for non-lawyers and available in other languages. Such information would enable individuals to understand the law and their rights. It would enable checks to be carried out on those who have executed the warrant and aid in considering the merits of challenging the warrant itself or the conduct of the search.

7.173 At the time of writing our consultation paper, we did not fully appreciate the potential overlap that our provisionally proposed guide would have with the notice of powers and rights under Code B of PACE. On reflection, we consider that a document to be presented to an occupier during the search is an appropriate mechanism through which to convey information about search powers. In particular, we consider that a physical document ought to be given to the occupier given that their electronic devices may be seized resulting in difficulty accessing the internet.

7.174 Our attention therefore turns to the adequacy of the notice of powers and rights in fulfilling this role. Measured against our desired policy, there are two shortcomings with the notice of powers and rights in its current form. First, we have no way of accurately determining how frequently the notice is provided. We note that the notice has no statutory basis but is instead contained in Code B of PACE. There also appears to be little consequence to failing to provide a notice: in *R (Haly)*, the Administrative Court observed that a notice was not provided to the occupier but then made no further mention of it in its judgment.[105]

7.175 We see merit in inserting a requirement in section 16 of PACE to provide an occupier with a notice of powers and rights. This would promote a more consistent practice of providing a notice. This is particularly so given our recommendation to ensure that the safeguards in sections 15 and 16 of PACE apply more widely. In addition, we regard the provision of a notice as important a safeguard as documentary evidence of the identity of the searcher, which is required under section 16(5)(a) of PACE. Amendment should also be made to other statutory regimes to ensure that the duty applies to all law enforcement agencies who obtain a search warrant for the purpose of a criminal investigation.

7.176 The second shortcoming of the notice of powers and rights is the seeming lack of consistency as to its content. Further research has revealed variations in content and levels of detail. For example, few notices seem to state how to apply for a copy of the information sworn in support of a search warrant. For this reason, we recommend that further consideration be given, in consultation with law enforcement agencies, as to whether amendment to Code B of PACE regarding the contents of the notice of powers and rights is

---

103 Law Society; Dijen Basu QC.

104 Dijen Basu QC.

105 *R (Haly) v Chief Constable of West Midlands Police* [2016] EWHC 2932 (Admin) at [3].

necessary. We recognise that matters of practicability and resources must be taken into account, which require further thought. In addition to the comments made by consultees set out above in this report, consultation should include:

(1) the content of the notice of powers and rights;

(2) the desirability of formulating generic templates which can be modified by law enforcement agencies;

(3) the translation of the notice of powers and rights; and

(4) how notice of powers and rights is to be produced.

7.177 In relation to the contents of a notice of powers and rights, we make several recommendations in this report which, if introduced, we consider could usefully be explained in the notice of powers and rights. Accordingly, a notice of powers and rights should state that an individual has right to:

(1) request details of what material was seized from premises (Recommendation 55 at paragraph 17.85 below);

(2) request details of what action was taken in respect of electronic devices on premises (Recommendation 56 at paragraph 17.95 below); and

(3) request protocols from a law enforcement agency setting out how seized or copied electronic material is to be examined off-site (Recommendation 57 at paragraph 17.101 below).

7.178 A notice of powers and rights should also explain how a person affected by a warrant can apply for the information sworn in support of the warrant, which we discuss at paragraphs 7.190 to 7.192 below.

Recommendation 32

7.179 We recommend that:

(1) section 16(5) of the Police and Criminal Evidence Act 1984 be amended, and provisions under other statutes as is necessary, to require that the constable or other investigator produce a notice of powers and rights; and

(2) section 16(7) of the Police and Criminal Evidence Act 1984 be amended, and provisions under other statutes as is necessary, to provide that the constable or other investigator must also leave a copy of the notice of powers and rights in a prominent place on the premises.

Information page on the Government website

7.180 In addition to recommending amending the current notice of powers and rights, we have considered whether a more permanent and detailed document could be created. We agree with the Bar Council and the CBA that it would be desirable to have a website page with a guide for individuals on search warrants.

7.181 We note that the Government website has a dedicated section on "crime, justice and the law". This contains an A to Z list of various topics, include arrest and stop and search. There is not, however, a section on search warrants.

7.182 We consider that there would be real value in a dedicated webpage hosted on that site on search warrants, which incorporates the areas raised by consultees. Those areas were the right to obtain the information provided in support of the warrant and how to do so, rights of challenge, appeals, rights to compensation, and how to access legal advice. A link could be included on the notice of powers and rights. Thought should also be given to translations.

Recommendation 33

7.183 We recommend the introduction of a specific search warrants "your rights and the law" webpage on the Government website. This should involve consultation with those with experience of the needs of individuals affected by a warrant.

HOW TO APPLY FOR THE UNDERLYING INFORMATION

The current law

7.184 An occupier must be provided with a copy of the search warrant. However, after the search of their premises, an occupier may want to obtain other relevant information. This includes the information which the investigator provided to the issuing authority in support of their application for a search warrant, the time taken to consider the application, additional notes taken during the hearing and the statement of reasons by the court for the issue of the search warrant. A person affected by a search warrant has a right to apply for this information, following the procedure set out in rule 5.7(6) to (9) of the CrimPR.[106]

The consultation paper

7.185 In the interests of transparency, in our consultation paper we provisionally proposed[107] that a search warrant should be required to state clearly that the occupier is entitled to the information sworn in support of the warrant and provide instructions on how to apply for a copy of that information.

Consultees responses

7.186 Nineteen consultees answered this question: 14 agreed;[108] three disagreed;[109] and four expressed other views.[110] The majority of consultees agreed with our provisional proposal

---

106 We discuss this procedure in more detail at paragraphs 9.11 to 9.14 below.

107 Consultation Question 35.

108 One member of the public; Professor Richard Stone; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Birmingham Law Society; Southern Derbyshire Magistrates' Bench; The Law Society; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Financial Conduct Authority.

109 National Crime Agency; Competition and Markets Authority.

110 HM Council of District Judges (Magistrates' Court); Kent County Council Trading Standards; Independent Office for Police Conduct; Serious Fraud Office.

based on the need for fairness and transparency. One consultee suggested that we could go further, and consider recommending that the information sworn in support of the warrant should be disclosed as a matter of course.

7.187 A large proportion of consultees who responded raised the concern that some of the information applied for may be sensitive and therefore redacted or unable to be disclosed to the occupier. Those consultees who disagreed with the provisional proposal did so on the ground that the right to information was in fact qualified and therefore it would be misleading to suggest that the occupier is entitled to the information.

7.188 Other consultees considered it possible to clarify that occupiers are not automatically entitled to the information sworn in support of a warrant, but rather that they have a right to apply for such information.

7.189 The SFO suggested that it may be preferable for the right to apply for the information sworn in support of the warrant to be stated in the guidance proposed above, or the notice of powers and rights, rather than on the face of the warrant.

Analysis

How to obtain a copy of the application form

7.190 We remain of the view that that an occupier should be provided with instructions on how to apply for a copy of the information. We agree with consultees that the instructions should not state that the person is entitled to the information but rather they are entitled *to apply for* the information. This should be qualified to explain that that the court may restrict what they are able to obtain or redact parts of it.

7.191 Given that we make a recommendation to require the production of a notice of powers and rights at Recommendation 32 above,[111] we consider that it would be appropriate to include in the notice of powers and rights how to obtain a copy of the information sworn in support of the warrant.

7.192 We agree with the SFO that it would be preferable for the right to be included in the notice of powers and rights rather than on the face of the warrant. This is because, provided Recommendation 32 above was implemented, provision of the notice to an occupier would be compulsory. The rights of an occupier would be contained in a single, self-contained document that would lend itself better to narrative text than a search warrant. We also consider that it would keep the content, presentation and purpose of a search warrant simple and straightforward: to indicate the extent of a law enforcement agencies authority to enter and search premises.

Disclosure of the application form as a matter of course

7.193 We do not consider that the application form should be provided as a matter of course for the reasons set out at paragraph 8.33 of our consultation paper. Disclosure of the application form may be legitimately withheld for a number of reasons, such as on public interest grounds.[112] Requiring disclosure as a matter of course would require the courts to determine matters such as public interest immunity during the application stage before the

---

111 See paragraph 7.179 above.

112 We discuss public interest immunity in Chapter 9 of this report.

application is automatically disclosed. This would impose a disproportionate burden on law enforcement agencies and the courts. It would be undesirable as not every occupier will request a copy of the information and would therefore be an onerous and unnecessary task for the court to determine, in advance of such a request, what can and cannot be disclosed.

7.194 We understand that law enforcement agencies adopt different practices and may list for disclosure both the warrant and the information sworn in support unless they contain sensitive information which needs to be protected. We regard the matter of pre-request disclosure as a matter properly left to individual law enforcement agencies.

THE PRESENCE OF LEGAL REPRESENTATIVES DURING THE SEARCH

The current law

7.195 The execution of a search warrant does not, in itself, divest an occupier of their power to invite third parties onto the premises. However, as discussed at paragraph 3.99 above, persons on premises must not, through their number or by their behaviour, obstruct the search. It is a matter of discretion for the officer in charge of the search whether to delay the search to await the arrival of an invitee.

7.196 In large-scale financial investigations, it is common for occupiers to ask a legal representative to be present at the search. However, there is no specific statutory right for a legal representative to be present during the execution of a search warrant. Nor is there guidance which sets out the functions or limits of a legal representative who is present during a search. Code B of PACE states:

> A friend, neighbour or other person must be allowed to witness the search if the occupier wishes unless the officer in charge of the search has reasonable grounds for believing the presence of the person asked for would seriously hinder the investigation or endanger officers or other people. A search need not be unreasonably delayed for this purpose. A record of the action taken should be made on the premises search record including the grounds for refusing the occupier's request.[113]

7.197 Code B of PACE treats a legal representative as "another person": there is no separate right to a legal representative that goes beyond the general right to have a friend, neighbour or other person present. This general right is also often set out in the notice of powers and rights, which we discussed at paragraphs 7.173 to 7.177 above.

The consultation paper

7.198 Stakeholders have informed us that the lack of statutory guidance results in inconsistent practices across different investigative agencies. It was suggested that Code B of PACE should acknowledge the distinct position of a legal representative and provide clearer guidance on the issue.

7.199 We considered that it would be helpful if Code B of PACE acknowledged the role of the legal representative and provided greater guidance on this issue. This would lead to more consistent practice, while retaining flexibility for the investigator and legal representative

[113] Code B of PACE (2013) para 6.11.

present to agree a protocol to enable the search to continue unhindered. In the consultation paper we therefore provisionally proposed[114] that Code B of PACE be amended to state that:

(1) if the occupier asks for a legal adviser or supporter to be present during the search, this should be allowed if it can be done without unduly delaying the search; and

(2) if present, a legal adviser or assistant has the right to observe the search and seizure of material in order to make their own notes.

7.200 In addition, we provisionally proposed that Code B of PACE should provide guidance on how far it is reasonable to delay a search to wait for a legal representative to attend.

Consultation responses

7.201 Nineteen consultees answered this question. On the question of whether Code B of PACE should be amended to state that, if the occupier asks for a legal adviser or supporter to be present during the search, this should be allowed if it can be done without unduly delaying the search: 12 agreed;[115] three disagreed;[116] and six expressed other views.[117]

7.202 On the question of whether Code B of PACE should be amended to state that, if present, a legal adviser or assistant has the right to observe the search and seizure of material in order to make their own notes: 11 agreed;[118] one disagreed;[119] and two expressed other views.[120]

7.203 On the question of whether Code B of PACE should also provide guidance on how far it is reasonable to delay a search to wait for a legal representative to attend: 11 agreed;[121] and two disagreed.[122]

7.204 The majority of consultees agreed with these proposals principally because they would protect the rights of occupiers and ensure that a search is carried out lawfully. However, several observations were made regarding the effects of delaying a search in order to allow a legal representative to observe it.

---

114 Consultation Question 36.

115 One member of the public; Professor Richard Stone; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; The Law Society; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; Bar Council and the Criminal Bar Association.

116 Kent County Council Trading Standards; Metropolitan Police Service; Financial Conduct Authority.

117 One member of the public; HM Council of District Judges (Magistrates' Court); National Crime Agency; Competition and Markets Authority; Serious Fraud Office.

118 Professor Richard Stone; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; Bar Council and the Criminal Bar Association; Serious Fraud Office.

119 Kent County Council Trading Standards.

120 Independent Office for Police Conduct; National Crime Agency.

121 Professor Richard Stone; Council of Her Majesty's Circuit Judges; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; Bar Council and the Criminal Bar Association; Serious Fraud Office.

122 National Crime Agency; Metropolitan Police Service.

7.205 First, a number of risks were identified where searches are delayed. It was said that waiting for a legal representative to attend the premises would increase the time that the execution of a warrant takes, adding to the cost of searches and, in some cases, the distress of occupiers.[123] Therefore, the longer it takes for a lawyer to travel to a search site, the more police time and recourses are taken up.[124] Investigators may also not be in a position to prevent tipping-off if there are other search warrants yet to be executed.[125]

7.206 Any delay also creates risks that evidence may be interfered with.[126] For example, electronic material may be deleted.[127] Clear guidance on what would amount to "undue delay" as we have put it would be necessary.[128] The point was also made that creating the right to delay may in certain circumstances result in it becoming necessary to arrest the occupant(s) until the delay is at an end to prevent them interfering with evidence.[129]

7.207 The point was made during a public lecture[130] that there are risks where a legal representative attends a search. It was said that it is unlikely that errors will be spotted there and then and if there is an error it may be more strategic to let it crystallise. Silence when legally privileged material is removed may also make it more difficult to object later. Further, there is a general risk of the legal representative becoming a witness if there is a dispute regarding what is said, which will impact on the occupier.

7.208 Secondly, it was pointed out that legal representatives can be contacted and attend as things stand.[131] Any right to attend might create the perception of an operational role for the legal adviser during the search. Seeking telephone advice from a legal representative may also be a possible alternative to physical attendance.[132]

7.209 Thirdly, there would be a tension between the right to delay a search until the legal representative arrives and the offence of intentionally obstructing the exercise of any rights conferred by a warrant.[133]

7.210 Fourthly, it was emphasised that a warrant is an order granted by the court: the protections are built into the application and issue processes. Investigators should be left to execute the warrant.[134]

---

123 Kent County Council Trading Standards.

124 Serious Fraud Office.

125 Metropolitan Police Services.

126 Independent Office for Police Conduct.

127 Financial Conduct Authority.

128 Independent Office for Police Conduct.

129 Financial Conduct Authority.

130 Matthew Hardcastle, Solicitor at Kingsley Napley, during the Red Lion Lecture Series, Challenging Search Warrants, 25 June 2019.

131 Financial Conduct Authority.

132 Serious Fraud Office.

133 Financial Conduct Authority.

134 Financial Conduct Authority.

7.211 Fifthly, with the increasing use of body-worn cameras by police officers and other means of documenting searches, the benefits of a legal representative documenting the search may be said to diminish.[135]

Analysis

7.212 We provisionally proposed a qualified right to have a legal representative present during the search. We agree with consultees that there should not be an unqualified right for a legal representative to attend the search given the clear risks of frustrating the search. The execution of a search warrant is a highly fact specific exercise in relation to the property, occupants and material sought. As such, we remain of the view that the execution of a search warrant is an operational matter and that the ultimate decision whether to delay a search should remain with the investigator carrying out the search.

7.213 Nonetheless, given the lack of inclusion of guidance on legal representatives in Code B of PACE, we still see value in there being a greater level of detail regarding the presence of legal representatives in order to encourage a more consistent practice. Such guidance and consistency will reduce the risk of arbitrary decision-making and ensure that the current law is properly understood.

7.214 For these reasons, we consider that Code B of PACE should make clear that a legal representative must be allowed to be present and observe a search under warrant in order to make their own notes. In our view, this should be subject to the same qualifier as currently applies when a friend or neighbour is requested: unless the officer in charge of the search has reasonable grounds for believing the presence of the person asked for would unreasonably delay the search, seriously hinder the investigation or endanger officers or other people. A record of the action taken should also be made on the premises search record, including the grounds for refusing the occupier's request for a legal representative.

7.215 An amendment along these lines would reflect the current law as found in Code B of PACE while recognising the importance of obtaining legal advice. We recognise the concerns raised by consultees militating against delaying a search, namely: the risks of inordinate delay, tipping-off simultaneous searches being conducted, electronic data being deleted or altered and the interference with evidence. These are all matters which could legitimately be taken into account when assessing whether a search can be delayed under the current test and therefore would not impinge on operational decision-making. Moreover, we do not consider that such an amendment would conflict with the offence of wilfully obstructing an officer in the execution of their duty.

7.216 It is clear that any amendment to Code B of PACE would require further consultation to ensure that the test is unambiguous.[136] We also observe that guidance note 6D in Code C of PACE discusses the solicitor's role in the police station and the limits of that role. Accordingly, a similar approach might be regarded as sensible in this context. Additionally, paragraph 6.11 of PACE applies to the search of premises generally, be it pursuant to a search warrant or another power to enter premises. To avoid inconsistency, thought should

---

135 Bar Council and the Criminal Bar Association.

136 Note that such consultation is required by statute in most circumstances: before revising a Code of Practice, the Secretary of State must consult a set group of organisations and such other persons as they think fit (see Police and Criminal Evidence Act 1984, s 67(4)).

also be given to whether our recommendation ought to be limited to searches pursuant to a warrant.

Recommendation 34

7.217 We recommend that the PACE Strategy Board consider amending Code B of the Police and Criminal Evidence Act 1984 to state that a legal representative must be allowed to be present and observe a search under warrant in order to make their own notes. This should be subject to the following exception and requirement currently contained in Code B of the Police and Criminal Evidence Act 1984:

(1) a legal representative need not be allowed to be present and observe the search if the officer in charge of the search has reasonable grounds for believing the presence of the person asked for would unreasonably delay the search, seriously hinder the investigation or endanger officers or other people; and

(2) a record of the action taken should also be made on the premises search record, including the grounds for refusing the occupier's request for a legal representative.

Chapter 8: Challenging a search warrant

INTRODUCTION

8.1 In this chapter we discuss how challenges can be made to both the lawfulness of a search warrant and the way in which a search under warrant has been conducted. We consider the following avenues for reform:

(1) the introduction of a new Crown Court procedure for challenging a search warrant or the conduct of a search; and

(2) amending section 59 of the Criminal Justice and Police Act 2001 ("CJPA"), which allows the Crown Court to order the return of seized material, most commonly because its seizure was not authorised under the relevant search warrant.

8.2 In the consultation paper we described legal challenges to search warrants as time-consuming, expensive and risky. We therefore provisionally proposed a new Crown Court procedure by which to challenge procedural breaches of search warrants, which would supplement applications for judicial review and applications under section 59 of the CJPA.

8.3 After carefully considering consultation responses, we are no longer of the view that there would be merit in the introduction of an entirely new procedure to challenge search warrants in the Crown Court. We provide detailed reasons why we have reached this conclusion at paragraphs 8.47 to 8.74 below.

8.4 However, we do identify worthwhile amendments to section 59 of the CJPA. We recommend that a judge hearing an application under this provision have the power to order costs between parties.[1] This will permit the recovery of public money spent opposing unsuccessful applications, and thereby deter people from making applications where there are no reasonable prospects of success. At the same time, it will encourage law enforcement agencies not to resist meritorious challenges.

8.5 We also recommend that a judge hearing a judicial review challenge to a search warrant have the powers and duties of the Crown Court in relation to the return or retention of material under section 59 of the CJPA. This will avoid the need for hearings to be duplicated, thereby saving both time and money.

A NEW CROWN COURT PROCEDURE FOR CHALLENGING SEARCH WARRANTS

The current law

Judicial review

8.6 We begin this section by setting out the current law governing challenges to search warrants. At present, the only way to challenge the validity of a search warrant is by judicial

[1] Arnold LJ has recently called for the Law Commission to review the practice on awards of costs against regulatory bodies who are unsuccessful in litigation: see *Competition and Markets Authority v Flynn Pharma Ltd* [2020] EWCA Civ 617, [2020] Costs LR 695 at [110].

review. The occupier or owner of the seized property or the premises searched must apply to the High Court for an order quashing the warrant.

8.7 Judicial review in search warrant cases usually involves challenges to either the validity or the execution of the search warrant. The applicant may argue that the warrant is invalid because it has been issued unlawfully, or that the warrant was improperly executed, rendering the entry, search and seizure unlawful. We discuss how non-compliance with the statutory safeguards effects the lawfulness of a search warrant in Chapter 2 of this report.

8.8 Common grounds of judicial review concerning the validity of the warrant include that:

(1) the statutory conditions for issuing the warrant were not met;

(2) the issuing authority was provided with inadequate, incomplete or misleading information; or

(3) the statutory safeguards were not complied with, such as the warrant was drawn impermissibly wide.

8.9 A search warrant can only be quashed where it is found to be invalid. If a warrant is quashed on judicial review, or the conduct of the search is held to have been unlawful, the High Court may exercise its discretion to order the return of any material taken during the search.

8.10 There are two principal problems with judicial review in this context. First, the cost involved puts judicial review proceedings beyond the financial reach of many litigants.[2] Secondly, judicial review is a time-consuming procedure. In non-urgent cases, the final hearing may be a year or more after the original application.

8.11 The situation is therefore unsatisfactory in two respects. On the one hand, where those searched have deep pockets, which may be the case in large-scale financial investigations, a criminal investigation can be tactically delayed through unmeritorious applications for judicial review, which take time to resolve. On the other hand, more routine criminal investigations in which the vast majority of search warrants are obtained are rarely judicially reviewed, because the cost of bringing judicial review proceedings is prohibitively high for many potential applicants. We explained in the consultation paper that this leads to inadequate oversight of police powers and perpetuates a justice gap based on financial means.

Section 59 of the Criminal Justice and Police Act 2001

8.12 A new procedure was introduced in 2001 to allow for the return or retention of material taken during a search, under section 59 of the CJPA. Section 59(2) of the CJPA gives anyone with a relevant interest in property, which has been seized under a relevant power of seizure, the right to apply to the Crown Court for its return. It is noteworthy that the relevant powers of seizure include powers that are exercisable in civil or regulatory investigations.[3] The main ground for making an application under section 59 is that there was no power to make the seizure, for example because it was not authorised under the warrant.

---

2 Judicial review guides suggest that the overall legal costs for a judicial review case could amount to £30,000 or more. See Public Law Project, *An Introduction to Judicial Review* (2019) p 13.

3 Criminal Justice and Police Act 2001, sch 1, part 1, paras 35, 56A and 73P.

8.13 The Crown Court hearing an application under section 59 of CJPA has no jurisdiction to decide whether the warrant was properly issued.[4] This means that the procedure has a relatively narrow scope. It also means that a challenge to the validity of a warrant must be brought separately in a judicial review application, adding cost and delay to the criminal process.

8.14 If material has been taken in exercise or purported exercise of a power of seizure, and ought in principle to be returned, the investigator or person holding the material may apply to the Crown Court to retain it under section 59(6) of the CJPA. The investigator or person holding the material must demonstrate, on the balance of probabilities, that a warrant to re-seize the property would be justified.

8.15 Section 59 of the CJPA has also faced criticism. The former Lord Chief Justice, Lord Thomas, has commented that section 59 of CJPA "could have been more felicitously drafted".[5] During our consultation, some of the main criticisms made by stakeholders were that:

(1) it was an unfamiliar and unpopular procedure with Crown Court judges;

(2) its narrow scope means that occupiers or property owners may have to bring additional claims to obtain the relief sought; and

(3) there is no cost regime to enable a party to recover legal fees incurred in the course of litigation against the other party.

The consultation paper

8.16 The two current avenues of challenge often result in long delays and disproportionate costs, encouraging unmeritorious and tactical challenges while creating barriers to access for potential claimants. We sought to devise a new procedure to address these issues. In our consultation paper, we provisionally proposed[6] that the Crown Court should have a comprehensive power of judicial oversight of search warrants relating to a criminal investigation, covering both the warrant itself and the way in which a search was conducted.

8.17 The contents of the provisionally proposed procedure[7] were broadly based on section 59 of the CJPA. Anyone with an interest in property seized or produced under a warrant would be entitled to apply to a Crown Court judge for the warrant to be set aside, resulting in the return of material or an order for the material to be retained.

8.18 This procedure would therefore permit an examination of whether the procedure for applying for or issuing the warrant was defective (due to insufficiency of information or non-compliance with section 15 of PACE) and/or whether the search was improperly conducted (due to unlawful seizure or non-compliance with section 16 of PACE).

8.19 If a Crown Court judge found that the procedure for applying for or issuing a warrant was defective or a search was improperly conducted, they could choose not to set the warrant

---

4 *R (Chaudhary) v Bristol Crown Court* [2014] EWHC 4096 (Admin), [2015] 1 Cr App R 18 at [61]; and *R (Goode) v Nottingham Crown Court* [2013] EWHC 1726 (Admin), [2014] ACD 6 at [50] and [51].

5 *R (Panesar) v Central Criminal Court* [2014] EWHC 2821 (Admin), [2015] 1 WLR 2577 at [44].

6 Consultation Question 37.

7 Consultation Question 38.

aside and allow the investigator to retain the materials. For this to happen, the investigator would have to satisfy the judge on the balance of probabilities that the conditions for issuing a warrant were fulfilled and it was in the interests of justice for the material to be retained (having regard to a non-exhaustive list of factors).

8.20 The Crown Court judge would have the power to: set aside the warrant; order the return of seized or produced material; authorise the retention of seized or produced material; give directions as to the examination, retention, separation or return of the whole or any part of the seized or produced material; order the return or destruction of copies; and make an order for costs between the parties.

8.21 The proposed procedure would be narrower than section 59 of the CJPA as it would be limited to search warrants relating to a criminal investigation. The section 59 procedure would therefore need to be retained.

8.22 The proposed procedure would also be narrower than judicial review proceedings. The procedure would not replicate the broad grounds of review which are ill-suited to a busy Crown Court. Instead, our intention was for the Crown Court to apply clear tests and not consider questions such as whether the access conditions or other statutory criteria were met.

8.23 It was our firm intention that judicial review should not be ousted. If the proposed procedure were to be implemented, judicial review would remain the avenue of choice for those who wished to have their rights vindicated by declaratory relief, as is often the case for high-profile individuals. Judicial review would therefore remain an avenue to challenge search warrants.

8.24 Considering all of the above, in our consultation paper we outlined arguments for and against the introduction of a new Crown Court procedure to challenge search warrants. The advantages of introducing such a procedure were identified as:

(1) it would be substantially quicker than judicial review, and would therefore cause fewer delays in criminal investigations;

(2) by replacing judicial review in many cases, it would reduce the workload of the High Court;

(3) dealing with challenges to the warrant and applications for the return or retention of materials in the same hearing would reduce the need for multiple proceedings;

(4) the available grounds of application would be clearly stated in statute and would not depend on judicial review concepts such as the warrant being invalid or unlawful;

(5) the Crown Court would be able to reconsider questions of fact and evidence, such as whether public interest immunity should be allowed;

(6) a wider range of remedies could be provided, other than the quashing of the warrant; and

(7) the hearing would be substantially cheaper, so that the ability to challenge a warrant would not be confined to wealthy claimants.

8.25 The disadvantages of introducing a new Crown Court challenge procedure were identified as:

(1) a cheaper and more accessible procedure might encourage more applications and overburden the Crown Court;

(2) jurisdiction under the new procedure would be narrow, meaning that it may be of limited utility in practice because claims involving search warrants usually require several issues to be considered together. For example, an occupier may contend that the warrant should not have been issued because the statutory criteria were not met, the procedural provisions in sections 15 and 16 of PACE were not adhered to and the investigator's powers of seizure were exceeded or used improperly; and

(3) judicial review might only be pushed back a step given that a decision by the Crown Court under the proposed procedure would also be amenable to judicial review.

Consultation responses

8.26 Twenty-one consultees responded to the question of whether the Crown Court should be able to review the issue and execution of search warrants relating to a criminal investigation: 11 agreed;[8] six disagreed;[9] and four expressed other views.[10]

8.27 A number of consultees agreed with the introduction of a new Crown Court procedure to challenge search warrants. Several reasons were given in support of the proposal. One consultee said that the Crown Court is the most appropriate forum for reviewing the issue and execution of search warrants and described judicial review as a lengthy process which can be misused in order to derail the investigation and any prosecution.[11]

8.28 Of those consultees who agreed, some did so subject to conditions, or expressed concern regarding a component of the procedure. In some cases, consultees' concerns contradicted one another.

8.29 One consultee agreed with the introduction of a new Crown Court challenge procedure on the basis that it would not prejudice the right to apply for the granting of a warrant to be judicially reviewed.[12] Another consultee agreed while expressing concern that the introduction of an additional procedure to sit alongside, rather than replace, existing routes of challenge is likely to exacerbate the problem of tactical challenges.[13] Another consultee

---

8 Professor Richard Stone; Crown Prosecution Service; Kent County Council Trading Standards; Insolvency Service; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; The Law Society; Justices' Clerks' Society; Magistrates Association; Bar Council and the Criminal Bar Association.

9 HM Council of District Judges (Magistrates' Court); Council of Her Majesty's Circuit Judges; Dijen Basu QC; Metropolitan Police Service; Competition and Markets Authority; Financial Conduct Authority.

10 Senior District Judge (Chief Magistrate); Independent Office for Police Conduct; National Crime Agency; Members of the Senior Judiciary.

11 Insolvency Service.

12 Birmingham Law Society.

13 Bar Council and the Criminal Bar Association.

raised similar concerns in respect of multiple remedies being granted in different proceedings.[14]

8.30 Other consultees urged us to go further by recommending that the Crown Court procedure be the only way in which a person can challenge a warrant or request that seized material be returned to them.[15] Another consultee considered that limiting the grounds of challenge under the proposed procedure, and thereby retaining the possibility of concurrent judicial review proceedings, may cancel out much, if not all, of the potential benefit of the new procedure.[16]

8.31 In response to our suggestion that the Crown Court should not be authorised to determine whether the statutory criteria were met, one consultee observed that the Crown Court already makes this determination implicitly under section 59 of the CJPA.[17] In particular, in deciding whether material should be retained by the investigator, subsection 59(7) of the CJPA requires the court to consider whether it would immediately become appropriate to issue a new warrant.

8.32 One consultee agreed, but queried the appropriateness of the Crown Court reviewing a search warrant issued by a Crown Court judge.[18] Other consultees agreed while raising concerns about how this would be accommodated given the Crown Court's reduced sitting capacity.[19] Another concern raised was the likely judicial aversion to the procedure in the Crown Court.[20]

8.33 The above concerns, and others, were also expressed by those who disagreed with introducing a new Crown Court procedure to challenge search warrants.

8.34 Two consultees who disagreed with the procedure argued that, as a matter of principle, it would be problematic for a Crown Court judge to review the decision of another Crown Court judge.[21] This concern was also raised at a roundtable organised by the Law Commission with the senior judiciary.

8.35 Secondly, one consultee said that the Crown Court is not a suitable forum for reviewing the issuing and execution of search warrants.[22] Another consultee observed that the procedure would be "rather unique".[23] In order to determine whether the search was properly conducted the court would have to hear evidence to resolve factual disputes, which would take considerable time. Further, challenges to whether something seized was within the terms of the warrant may already be subject of private proceedings in the civil courts. It was further argued that the Crown Court may not have the expertise adequately to consider

---

14 Independent Office for Police Conduct.

15 Financial Conduct Authority; Crown Prosecution Service.

16 Serious Fraud Office.

17 Serious Fraud Office.

18 Kent County Council Trading Standards

19 Law Society; Bar Council and the Criminal Bar Association.

20 Bar Council and the Criminal Bar Association.

21 Dijen Basu QC; Serious Fraud Office.

22 Metropolitan Police Service.

23 Senior District Judge (Chief Magistrate).

claims under the new procedure.[24] Even those consultees who agreed with the procedure accepted that Crown Court judges would need to be appropriately trained.[25]

8.36 Thirdly, it was argued that the new procedure would place additional burdens on the already overstretched Crown Court.[26] It was pointed out that we cited burdens on the High Court as a justification for devising the new procedure, but the Crown Court is equally over-burdened and even less able to deal with these challenges than the High Court.[27] Members of the senior judiciary at our roundtable observed that, as a matter of resourcing, the new procedure may divert Crown Court judges from other work and, importantly, increase the length of time individuals must await trial.

8.37 Fourthly, one consultee had reservations over whether the new Crown Court procedure would in fact be less expensive than current proceedings.[28]

8.38 Fifthly, far from clarifying the mechanisms for challenging search warrants, it was suggested that an additional procedure would increase uncertainty, creating a less effective search warrants system.[29] For example, in cases where much of the challenge could have been brought under the new Crown Court procedure, there may be uncertainty over whether judicial review is still available.[30]

8.39 Sixthly, there was concern that an additional procedure would be likely to exacerbate the problem of tactical challenges rather than streamline the procedure.[31] It was argued that wealthy claimants may simply use this procedure as an additional line of attack in their tactical attempts to disrupt investigations.

8.40 It was pointed out that a single search warrant may lead to as many as five different sets of proceedings.[32] There could be a judicial review of the warrant itself on the grounds that the statutory conditions were not met, an application under section 59 of the CJPA for the return of seized material, an application under the new procedure to set aside the warrant and two further judicial review proceedings of the decisions of the Crown Court. A sixth avenue of challenge would arise if the Crown Court procedure had a permission filter, whereby refusal of permission could be reviewed.

8.41 Seventhly, consultees expressed reservations as to whether the proposed procedure amounts to a comprehensive scheme.[33] It was argued that, in order for the new procedure to be as effective as a claim for judicial review, it would need to include certain powers exercisable by the High Court, namely the power to grant interim relief and to award

---

24 Financial Conduct Authority.

25 Crown Prosecution Service.

26 Council of Her Majesty's Circuit Judges; Senior District Judge (Chief Magistrate); Financial Conduct Authority; Serious Fraud Office.

27 Metropolitan Police Service.

28 Serious Fraud Office.

29 Metropolitan Police Service.

30 Dijen Basu QC.

31 Financial Conduct Authority; Serious Fraud Office.

32 Financial Conduct Authority.

33 Serious Fraud Office.

damages where serious loss had been caused.[34] The question arises whether it is appropriate for the Crown Court to have these powers given that they are more suited to the civil courts.

8.42 Similarly, participants at the senior judiciary roundtable observed that the narrower scope of review may render this new challenge route ineffective, as challenges often concern several issues. Another consultee was critical that the proposed procedure did not include one of the main grounds of challenge, namely that the statutory criteria for issuing a warrant were not met.[35] It was pointed out by the Serious Fraud Office that it is difficult to disentangle a procedural challenge concerning a deficiency in the information provided to the issuing court (which would be a ground of challenge under our proposed procedure) from a substantive challenge that the statutory criteria were not met (which would not be a ground of challenge).[36] At the same time, allowing the Crown Court to determine whether the statutory criteria were met would give rise to difficulties by a court reviewing the judicial act of another court of equal jurisdiction.[37]

8.43 Eighthly, concern was expressed that, far from speeding matters up and simplifying the challenge process, an unqualified right to apply to the Crown Court to review the issuing and execution of a warrant risks slowing down the investigative process.[38] Two reasons were given for this. The first was that, without significant investment, the new procedure would be unlikely to be faster than judicial review given burdens on the Crown Court.[39] Additionally, it would add a further layer of challenge as judicial review would still be available at a later stage. This point was also raised at the senior judiciary roundtable. It was argued, therefore, that a new procedure may lead to more judicial review cases in the long term.[40]

8.44 Ninthly, it was argued that the amendments that we proposed in our consultation paper to the way in which information is provided to a person affected by a warrant[41] would provide a sufficient basis on which to assess whether the application is defective or not,[42] which may reduce speculative judicial review challenges.

8.45 Tenthly, one consultee argued that the current challenge mechanisms strike the right balance between the different interests at play.[43] It was also argued that a new challenge procedure in the Crown Court is not necessary given that very few search warrants are

---

34 Dijen Basu QC.

35 Serious Fraud Office.

36 Serious Fraud Office. See *R (Chatwani) v National Crime Agency* [2015] EWHC 1283 (Admin), [2015] ACD 110 at [101] to [104] in which the Administrative Court found that there was considerable overlap between two broad grounds of this nature.

37 Serious Fraud Office.

38 Metropolitan Police Service; Serious Fraud Office.

39 Financial Conduct Authority.

40 Financial Conduct Authority.

41 Consultation Question 34: we provisionally proposed that a person executing a search warrant should provide the occupier with an authoritative guide to search powers, written in plain English for non-lawyers and available in other languages. Consultation Question 35: we provisionally proposed that a search warrant should be required to clearly state that the occupier is entitled to the information sworn in support of the warrant and provide instructions on how to apply for a copy of that information.

42 Metropolitan Police Service.

43 Competition and Markets Authority.

challenged.[44] Further, concern was raised that, without safeguards against spurious challenges, the balance would tip too far in favour of the occupier, leading to a proliferation of search warrant challenges.[45]

Analysis

8.46 Given that we have resiled from the provisional view adopted in our consultation paper, we set out our reasons in detail here.

Appropriateness of the Crown Court reviewing a Crown Court decision

8.47 The first group of challenges were matters of principle. We see force in the argument that it would be problematic for a Crown Court judge to review the decision of another Crown Court judge. This issue, in the context of search warrants, was described in the following terms by Pitchford LJ:

> The issue of a warrant is a judicial act. It would be a novel and surprising development of the law if a court of equal jurisdiction enjoyed the power to declare invalid the judicial act of another.[46]

8.48 We have examined whether the current law contains any examples of a court of equal jurisdiction (ie at the same level) having the power to declare invalid the judicial act of another. We have found no firm examples within criminal proceedings. It is conceivable that a Crown Court judge could make an order regarding admissibility at a pre-trial hearing, with a renewed application regarding admissibility leading to a different Crown Court judge at trial reversing the decision at the pre-trial hearing. However, this is not in any true sense a declaration of invalidity.

8.49 We have considered a number of other examples and have reached a similar conclusion in respect of each. When a Criminal Behaviour Order is discharged by the court which made the original order, to account for a change of circumstances, it is not declaring the original order invalid. Where a magistrates' court varies or rescinds a sentence or other order made by it under section 142 of the Magistrates' Courts Act 1980 there will be a rehearing at which the court will look at the matter afresh.[47]

8.50 In defence of the proposed procedure, a distinction may be drawn between a court of equal jurisdiction reviewing the correctness of a court's decision to grant a warrant and reviewing the correctness of a law enforcement agency's conduct in applying for and executing a warrant. Arguably, the proposed procedure is concerned with the conduct of the law enforcement agency, such as whether it failed to discharge the duty of candour or follow the statutory safeguards under section 15 and 16 of PACE. Another distinction may be drawn between declaring an act retrospectively invalid, which is the preserve of the High Court upon judicial review, and setting the warrant aside, which is the power we provisionally proposed for the Crown Court which would not have retrospective effect.

---

44 HM Council of District Judges (Magistrates' Court).

45 National Crime Agency.

46 *R (Goode) v Nottingham Crown Court* [2013] EWHC 1726 (Admin), [2014] ACD 6 at [51]. The point was reiterated in *R (Chaudhary) v Bristol Crown Court* [2014] EWHC 4096 (Admin), [2015] 1 Cr App R 18 at [61].

47 See also *Jones v CPS* [2019] EWHC 2826 (Admin) at [17].

8.51 Alternatively, the distinction between declaring the warrant invalid and setting it aside may become blurred when determining the accuracy of the application or the specificity of the warrant. This argument would also become less tenable if the jurisdiction of the Crown Court under the proposed procedure was expanded to include consideration of whether the statutory criteria were met, as called for by a number of consultees.

8.52 One solution could be to exclude warrants issued by the Crown Court from the procedure, so that only warrants issued by a magistrates' court could be challenged in the Crown Court. However, this would create a potentially arbitrary situation where the availability of challenge depends on which court issued the warrant. It might also encourage law enforcement agencies to apply for warrants before the Crown Court to close off the proposed procedure as an avenue of challenge. Another solution might be for challenges to warrants issued in the Crown Court to be heard by a High Court judge sitting in the Crown Court, which may arguably defeat the advantage of relieving pressure on the High Court.

Whether the Crown Court is suitable forum

8.53 We also agree that questions arise regarding whether the Crown Court is the most suitable forum for a procedure of this type. It may be argued that the Crown Court would be the most suitable forum given that the procedure would be limited to search warrants relating to criminal investigations.[48]

8.54 Whether the Crown Court is a suitable forum for this procedure may also depend on the jurisdiction and powers conferred upon it. For example, if the Crown Court were given the power to award damages this would arguably bring it closer to the civil courts, where considerations of liability and quantum are determined. This would likely make hearings lengthier and more complex. It is worth pointing out that Crown Court judges exercise a variety of powers which are civil-related, such as powers under the Proceeds of Crime Act 2002. One answer may also be to delegate such matters to the county court. However, this would lead to additional proceedings and raises questions regarding the interplay between criminal and civil proceedings.

8.55 The fact that the Crown Court lacks expertise to deal with applications of this type could be remedied with training. A more fundamental issue revealed by consultation responses is that the Council of Her Majesty's Circuit Judges, who represent the judges who would be hearing such applications, did not agree that they should be given the jurisdiction to review the issue or execution of search warrants. It was argued that the burdens on the Crown Court are great as it without a new one being introduced. Similar concerns were also raised by attendees at our senior judiciary roundtable. As we have seen with section 59 of the CJPA, judicial aversion can lead to lengthy delays: one case indicated a section 59 application passed around due to the difficulty identifying a judge who was "suitable and willing" to hear the application.[49] Better listing of hearings in the Crown Court may allay some resistance but it is unlikely to garner much greater support for the procedure. At the same time, judicial aversion is not in itself a sufficient reason to dispense with a new procedure.

8.56 Relatedly, we understand the concern that the proposed procedure would not be a comprehensive scheme as it would lack certain remedies available from the High Court. Some claimants seek declaratory relief in order to be publicly vindicated, while others seek

---

48 See *R (AL) v Serious Fraud Office* [2018] EWHC 856 (Admin), [2018] 1 WLR 4557 at [65].

49 *R (Panesar) v Central Criminal Court* [2014] EWHC 2821 (Admin), [2015] 1 WLR 2577 at [21].

damages to compensate for serious loss. Neither remedy would be available under the proposed procedure. In our view, a declaratory relief equivalent in the Crown Court would have limited effect because Crown Court cases are not reported, meaning that case law would only emerge if decisions under the new procedure were judicially reviewed.

8.57 As we discussed above, certain grounds of challenge would be unavailable under the new procedure, such as whether the statutory conditions were met. We accept the point made by the Serious Fraud Office ("SFO") that parallels may be drawn with the Crown Court's decision-making process when deciding whether it would immediately become appropriate to issue a fresh warrant if seized property were returned.[50] For this reason, the Crown Court would arguably be equipped to consider whether the statutory criteria were met. That said, expanding the grounds of challenge may be of little benefit if the Crown Court is not able to award the full range of remedies.

Delay and expense

8.58 The next set of challenges raised were to the practicalities of the Crown Court having oversight at all. Several consultees raised concern that the Crown Court is over-burdened. Sitting days in the Crown Court have been reduced, causing a rising backlog of cases across England and Wales.[51]

8.59 Coupled with this, according to Her Majesty's Courts and Tribunals Service ("HMCTS"), there are around 30,000 search warrant applications a year.[52] Giving the Crown Court jurisdiction over a new challenge procedure is likely to divert resources and increase the length of time individuals must await trial. It is possible that the Crown Court would receive extra funding because of savings in the High Court, but this cannot be guaranteed.

8.60 We also accept the argument that diverting challenges to the Crown Court may not reduce delay. Lessons can be learnt from section 59 of the CJPA. Although the explanatory note to section 59 raises the hope that it "will provide a quick and easy mechanism for challenging search warrant powers",[53] some cases still experience significant delay. In *Panesar*, the then Lord Chief Justice, Lord Thomas, noted that the case had been delayed for over two years, caused by issues with identifying a suitable judge and the general pressure of work at the Central Criminal Court.[54] On one view, training may help to reduce delays. However, unless additional funding is forthcoming our proposed procedure is likely to face similar issues.

8.61 Although one consultee had reservations over whether the new Crown Court procedure would in fact reduce expense, we have no firm evidence either way. From a HMCTS perspective, publicly available information suggests that the cost per Crown Court courtroom day is £2,041,[55] however, we have no evidence of the comparable cost per High Court

---

50 Criminal Justice and Police Act 2001, s 59(7).

51 *Court Sitting Days Under Review as Backlog of Cases Rises* (18 October 2019), https://www.thetimes.co.uk/article/court-sitting-days-under-review-as-backlog-of-cases-rises-bthg3cdx3.

52 https://www.policeconduct.gov.uk/recommendations/national-recommendations-and-recommendations-made-metropolitan-police-service.

53 Explanatory Notes to the Criminal Justice and Police Act 2001, para 176, http://www.legislation.gov.uk/ukpga/2001/16/notes/division/3/2/1/10.

54 *R (Panesar) v Central Criminal Court* [2014] EWHC 2821 (Admin), [2015] 4 All ER 754 at [21].

55 Crime (Overseas Production Orders) Bill: Impact Assessment, https://publications.parliament.uk/pa/bills/lbill/2017-2019/0113/18113-impact-assessment.pdf.

courtroom day. On the one hand, it may be argued that, in principle, the Crown Court is ideally placed to resolve factual disputes involving the calling and challenging of evidence. On the other hand, resolving such disputes would likely require lengthy hearings, which would be costly for HMCTS and prospective claimants. Increasing the jurisdiction of the proposed procedure to include matters such as whether the statutory criteria were met will only exacerbate these concerns.

Issues arising from having two avenues of challenge

8.62 Further concerns stem from the fact that this was envisioned as an *additional* procedure. Adding a challenge mechanism may cause greater uncertainty when determining the most appropriate route. For example, where a prospective applicant wishes to challenge whether the statutory conditions were met and whether the safeguards were followed, only the latter issue would be amenable to challenge under our proposed procedure.

8.63 A prospective applicant may wish to address all heads of challenge in judicial review proceedings, instead of using the proposed procedure. Alternatively, they may wish to bring proceedings under both routes concurrently. Judicial review is a remedy of last resort.[56] The High Court may decline to exercise its jurisdiction where there exists an alternative way in which the dispute in question could be resolved.[57] A prospective applicant might therefore be refused permission to apply for judicial review where the proposed procedure has not been exhausted.

8.64 A further layer of complexity stems from our terms of reference, which means that our proposed procedure only concerns search warrants relating to a criminal investigation. Therefore, the avenues of challenge would further vary depending on the statutory provision under which the warrant was sought or the type of investigation. Section 59 of the CJPA would exist for civil and regulatory investigations and our new procedure for criminal investigations.

8.65 We also agree that the fact that the proposed procedure would be an additional avenue of challenge is likely to exacerbate the problem of tactical challenges. Additionally, judicial review will only be pushed back a stage. Although it may be questioned whether this is a real risk, case law suggests that persons affected by a warrant will seek to bring a range of challenges.[58]

8.66 One answer to the risk of multiple proceedings could be to make our proposed procedure and judicial review mutually exclusive, such that bringing proceedings under one procedure would prevent proceedings being brought under the other. However, wealthy prospective claimants would probably still choose judicial review with its wider suite of potential remedies. Another problem would arise if potential grounds of challenge outside of the scope of the new procedure were to emerge once proceedings under that procedure were brought. The claimant would be barred from bringing a judicial review challenge, limiting their ability to access a just and effective remedy.

---

56 *Glencore Energy UK Limited v Commissioners of HMRC* [2017] EWHC 1476 (Admin), [2017] STC 1824.

57 *R (AL) v Serious Fraud Office* [2018] EWHC 856 (Admin), [2018] 1 WLR 4557 at [55].

58 *R (Panesar) v Central Criminal Court* [2014] EWHC 2821 (Admin), [2014] EWCA Civ 1613, [2015] 1 WLR 2577; R (*Business Energy Solutions Ltd) v Preston Crown Court* [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [121].

8.67 It is important not to oust the availability of judicial review. Removing the option to judicially review search warrants could only be considered if all of the current grounds of challenge and remedies were made available under the proposed procedure in order not to deprive individuals of particular forms of redress. This was a position supported by consultees.

Summary of objections to a new Crown Court procedure

8.68 Consultees' responses have persuaded us that the proposed procedure, in its current form, is an unsatisfactory mechanism for challenging search warrants. Building in additional grounds of challenge and remedies would overcome some of the concerns raised by consultees, but it would heighten others. Concerns that would remain include: whether the Crown Court is suited to replicating judicial review hearings; the likelihood of lengthy hearings and delays placing further burdens on an already over-stretched Crown Court; and the fact that judicial review will still be pursued, meritoriously or otherwise.

8.69 We are therefore in a difficult position: the more we try to address the gaps identified in our procedure, the more likely we are to render it unworkable in practice. We also note that there was a remarkably wide divergence in consultees' views on how any new procedure should operate, which makes devising a workable scheme even more complex.

8.70 The final challenges related to whether it is in fact necessary to reform the current challenge mechanisms. We still have reservations over whether the current mechanisms strike the right balance between the compelling interests at play. We do not accept that because only a small proportion of the warrants issued are challenged there is clearly no need for a new procedure. Recent reviews carried out by the National Crime Agency ("NCA") and Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services ("HMICFRS") suggest that defective warrants are regularly issued. Nonetheless, if only a small number of warrants are challenged this suggests that a new procedure would not overburden the Crown Court with new cases.

8.71 We agree that amending the information which is provided to an individual affected by a warrant could help them to assess whether the warrant was issued or executed defectively.[59] Under the current law, individuals affected by search warrants who do not have vast amounts of wealth or legal expertise face significant barriers to accessing justice. If those individuals were given more information about their rights and how to apply for the information sworn in support of a warrant, they would be in a better position to assess whether it is worth bringing an application. But other obstacles remain, perhaps chief among these is how to fund a claim.

8.72 Recommendations made elsewhere in this report, which promote access to justice and greater efficiency, would go some way towards removing those obstacles.

(1) *Recommendation 35* – we recommend at paragraph 8.94 below that a judge hearing an application under section 59 of the CJPA have the power to order costs between parties. This would allow parties to recoup legal fees incurred by bringing or defending a claim. Further, it would encourage law enforcement agencies not to resist meritorious challenges.

(2) *Recommendation 36* – we recommend at paragraph 8.101 below that a judge hearing a judicial review of a search warrant have the powers and duties of the Crown Court in

[59] Metropolitan Police Service.

relation to the return or retention of material under section 59 of the CJPA. This would streamline judicial review and section 59 proceedings.

(3) *Recommendation 61* – we recommend at paragraph 17.133 below that a person with an interest in electronic material should be able to apply to the Crown Court for a judge to decide how an investigator should treat that material. For instance, a judge could determine how any protected material on an electronic device will be sifted. This would allow greater scrutiny of the way in which investigators handle electronic material, notwithstanding that an application cannot be made for the return of all or part of the property under section 59(2) of the CJPA.

(4) *Recommendation 62* – we recommend at paragraph 17.139 below that a person with an interest in electronic material which has been seized should be able to apply to the Crown Court for the return or deletion of specified electronic data or the return of an electronic storage device on the grounds that:

(a) the material is reasonably required by the person with an interest in the data; or

(b) continued retention by an investigator of the material is not necessary.

This would permit a person with an interest in an electronic device or data on that device to apply for its return or deletion notwithstanding that the material is lawfully held and therefore an application for its return could not be made under section 59(3) of the CJPA.

8.73 Ultimately, the question is whether the significant reforms originally proposed in our Consultation Paper are the best course of action. In answering this question, it is useful to take a step back and ask what remedy might be sought by a person affected by a warrant and how that might be achieved.

(1) *Person wants their property back* – the most common remedy that a person affected by a warrant will seek is the return of their property. To that end, so long as they have a relevant interest in the seized property, they can make an application to the Crown Court for its return under section 59(2) of the CJPA. We recommend below that a judge hearing a section 59 application have the power to order costs between parties. We also propose a route to applying for the return of electronic data or devices in circumstances not provided for under the current law. Finally, the return of property is also a discretionary remedy in judicial review applications.

(2) *Person does not want the investigator to retain copies of material seized* – a person may have received their property back but remain concerned that the investigator has held on to copies of the material. Such a person can apply under section 59 of the CJPA for the investigator to delete data it holds.[60] We also recommend below a right to apply to the Crown Court for an investigator to delete data where continued retention is not necessary.

(3) *Person is concerned about how their property is to be handled* – a person may be concerned about an investigator looking at certain material or treating their property in a particular way. Under the current law, a person can apply for injunctive relief from

[60] The Divisional Court has held that to "return" material includes deleting copies of it: *R* (*Business Energy Solutions Ltd) v Preston Crown Court* [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [17].

the High Court, prohibiting investigators from examining the material.[61] In addition, we recommend a right to request protocols governing how electronic material will be handled as well as a right to apply to the Crown Court to adjudicate on disputes regarding the handling of electronic material.

(4) *Person seeks damages due to the conduct of the investigator* – quite apart from the return of property, a person may seek damages due to the conduct of those who executed the warrant or the harm caused by their conduct. As we discussed at paragraph 7.19 of our consultation paper, damages may also arise in civil claims in tort and under the Human Rights Act 1998.

(5) *Person wants to complain about an investigator's conduct* – a person may wish to complain about the conduct of someone involved in the search. Each law enforcement agency will have their own procedures. A person can complain about the conduct of a police officer;[62] NCA officer;[63] HM Revenue and Customs Officer;[64] a member of the SFO;[65] a member of the Financial Conduct Authority;[66] or a Trading Standards officer.[67]

(6) *Person wants to challenge the lawfulness of the warrant*– where a person wishes to challenge the lawfulness of the warrant itself, judicial review is required. A quashing order cannot be pursued without judicial review, except if representations made to the investigator lead them to concede that the warrant was unlawful.[68]

(7) *Person wants to be publicly vindicated* – where an individual seeks public vindication through declaratory relief, they must bring a judicial review application.

8.74 Taking all of the above into consideration, we conclude that a new procedure to challenge search warrants should not be introduced.

AMENDMENTS TO SECTION 59 OF THE CRIMINAL JUSTICE AND POLICE ACT 2001

The power to order costs between parties

The current law

8.75 Neither the CJPA nor the CrimPR contains any express provision enabling the Crown Court to make orders for costs in section 59 proceedings.

---

61 *R* (*Business Energy Solutions Ltd) v Preston Crown Court* [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [125].

62 By complaint to the individual police force or the Independent Office for Police Conduct.

63 By complaint to the National Crime Agency or the Independent Office for Police Conduct.

64 By complaint to HM Revenue and Customs or the Independent Office for Police Conduct.

65 By complaint to the Serious Fraud Office.

66 By using the complaints scheme set up under the Financial Services Act 2012, Pt 6.

67 By complaint to the chief executive of the person's local authority.

68 *R (Chatwani) v National Crime Agency* [2015] EWHC 1283 (Admin), [2015] ACD 110 at [2].

8.76 While the Crown Court is a superior court of record and has the like powers of the High Court in relation to all matters incidental to its jurisdiction,[69] it does not have an inherent jurisdiction to order costs on a section 59 application. This is because an order for costs would not be directly linked to the exercise of the jurisdiction of a judge of the Crown Court in the exercise of their statutory functions under section 59 of the CJPA.[70]

8.77 Since an application under section 59 of the CJPA will typically be a criminal cause or matter, it is no longer possible to make a costs order in respect of it under rule 12 of the Crown Court Rules 1982. This is because those rules were revoked in relation to criminal causes or matters as a result of the exercise of powers conferred by the Courts Act 2003, whereby the Senior Courts Act 1981 was amended and the CrimPR introduced.[71]

8.78 We are also aware of an unsuccessful claim in 2017 for the costs of a section 59 hearing being made under section 19 of the Prosecution of Offences Act 1985 (POA) and regulation 3 of the Costs in Criminal Cases (General) Regulations 1986. These provisions permit a party to criminal proceedings to make a claim for costs against another party to those proceedings. A similar argument was made by Channel 4 Television Corporation ("Channel 4"), who sought an order that the Metropolitan Police Service ("MPS") pay the costs that Channel 4 incurred in opposing a production order application, replying on section 19 of the POA. Edis J as he then was, sitting in the Crown Court, held that an order for costs could not be made pursuant to section 19 POA as the production order application itself did not constitute "criminal proceedings".[72]

8.79 Therefore, the Crown Court does not have jurisdiction to order costs in respect of applications under section 59 of the CJPA.

The consultation paper

8.80 Given that our proposed procedure would sit alongside, rather than replace, section 59 of the CJPA, we invited consultees' views[73] on whether there were any aspects of the proposed new procedure that ought to be replicated under section 59. In particular, we asked whether a judge hearing an application under section 59 should have the power to order costs between parties, which would allow a party to recover costs incurred in the course of litigation against the other party.

8.81 We provisionally proposed a costs regime under the new procedure as it would deter unmeritorious applications and encourage the authorities not to resist meritorious challenges.

8.82 We also observed that a rule about costs in relation to section 59 proceedings could be introduced by amending the CrimPR: subsection (13) of section 59 (which was inserted by section 82(5) of the Deregulation Act 2015) provides that Criminal Procedure Rules may make provision about proceedings under section 59.

---

69 Senior Courts Act 1981, s 45(1) and (4).

70 *R (Chaudhary) v Crown Court at Bristol* (No 2) [2015] EWHC 723 (Admin), [2016] 1 WLR 631 at [35].

71 *R (Chaudhary) v Crown Court at Bristol* (No 2) [2015] EWHC 723 (Admin), [2016] 1 WLR 631 at [28].

72 *Channel 4 v MPS* [2019] 1 Costs LR 67 at [85].

73 Consultation Question 40.

Consultation responses

8.83 Fourteen consultees answered our question about introducing a costs regime: nine agreed;[74] two disagreed;[75] and three expressed other views.[76] Consultees generally supported the introduction of a between parties costs regime. The MPS argued that such a power would be in the public interest. Of the two consultees who disagreed, neither detailed why the power should not be introduced.

Analysis

8.84 Our preliminary view at the time of writing the consultation paper was that a judge hearing an application under section 59 of the CJPA should have the power to order costs between parties. We are fortified in this view following consultees' responses.

8.85 We accept that there are arguments against the introduction of a costs regime. The owner of property which has been seized might be put off bringing an application for the return of property under section 59(2), or defending an investigator's application for retention under section 59(6), by the prospect of being required to pay the other party's costs.

8.86 From an investigator's point of view, if an entirely reasonable section 59(6) application against a well-funded respondent could result in a costs order against the investigator far in excess of the costs which the investigator had actually incurred, then the investigator might also be deterred from making applications. Accordingly, it would be unsatisfactory if law enforcement agencies were reluctant to exercise their legitimate public responsibilities to make reasonable applications to the court for fear of a disproportionate costs order.

8.87 On balance, we do not consider these to be strong reasons against introducing a costs regime. Costs would be at the court's discretion, when it is just and reasonable to award them. The wording of the costs provision will therefore be relevant. For example, section 19 of the POA 1985, only allows parties in criminal proceedings to recover their costs if they have been incurred "as a result of an unnecessary or improper act or omission by, or on behalf of, another party to the proceedings". It is for this reason that costs applications against a public prosecutor are very rare and restricted to exceptional cases.[77]

8.88 Edis J, as he then was, has described section 19 of the POA 1985 as primarily designed to enable the court to encourage efficiency, rather than to compensate parties who have incurred legal expenses.[78] We regard this as an important distinction, as compensation alone may be viewed by some as an insufficient justification for the introduction of a costs regime. As we made clear in the consultation paper, it is the encouragement of efficiency which underpins our policy. Ultimately, the basis on which a jurisdiction to order costs ought to exist is a delicate issue that will require further consideration.

---

74 HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Justices' Clerks' Society; Magistrates Association; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Financial Conduct Authority; Serious Fraud Office.

75 Council of Her Majesty's Circuit Judges; The Law Society.

76 Crown Prosecution Service; National Crime Agency.

77 *Evans v Serious Fraud Office* [2015] EWHC 263 (QB), [2015] 1 WLR 3595.

78 *Channel 4 v Metropolitan Police Service* [2019] 1 Costs LR 67 at [75].

8.89 The final question is how a costs regime for section 59 proceedings could be introduced. As discussed above, our preliminary view was that a costs regime could be implemented in relation to section 59 proceedings by amending the Criminal Procedure Rules. Section 59(13) of the CJPA, which was inserted by section 82(5) of the Deregulation Act 2015, states:

> Criminal Procedure Rules may make provision about proceedings under this section on an application to a judge of the Crown Court in England and Wales.

8.90 Having given the matter further thought, and having discussed the matter with the Criminal Procedure Rule Committee ("CPRC"), we consider it unclear whether section 59(13) empowers the CrimPR to provide for costs in respect of hearings under section 59 of the CJPA. This is because jurisdiction to award costs would rest with a judge rather than the court, and section 59(13) does not extend to empowering the CrimPR to make provision about the powers vested in particular judges: the subsection empowers the CrimPR to make provisions about *proceedings* under section 59.

8.91 There are two reasons why this might involve too narrow a reading of section 59(13) of the CJPA. First, the construction rests on a fine distinction between the powers of the Crown Court and the powers of a judge of the Crown Court. Fulford LJ discussed this distinction in *R (Chaudhary)*, writing:

> I would add that there is, potentially, an important difference between the separate legal concepts of "a judge of the Crown Court" and "the Crown Court", on the basis that legislation has, on occasion, treated certain types of judges as being legally distinct from the court in which they sit. Put in a nutshell, there is a possible argument that a judge dealing with an application under section 59 of the 2001 Act is not exercising the general jurisdiction of the Crown Court as a superior court of record. Instead, he is simply acting pursuant to the discrete powers given to a judge of the Crown Court in this particular situation: see sections 59(2) and 64(1)(a) of the [CJPA]. However, this argument is dependent on drawing something of a fine distinction between these two concepts and we have not received submissions on the issue. In any event, it is unnecessary to resolve the point given the conclusions that I have reached above and I therefore say no more about it.[79]

8.92 Secondly, we note that section 59 of the CJPA itself is all phrased as powers of "an appropriate judicial authority",[80] defined as "a judge of the Crown Court". If section 59(13) does not apply to powers vested in judges, then on this argument the subsection is totally empty of all content.

8.93 We remain of the view that any costs regime should be contained in the CrimPR, however, thought would need to be given as to whether the CPRC are currently empowered to do so by virtue of section 59(13) of the CJPA.

---

79 *R (Chaudhary) v Crown Court at Bristol* (No 2) [2015] EWHC 723 (Admin), [2016] 1 WLR 631 at [36].

80 Criminal Justice and Police Act 2001, s 59(4), (6) and (9).

Recommendation 35

8.94 We recommend that a judge hearing an application under section 59 of the Criminal Justice and Police Act 2001 have the power to order costs between parties.

High Court ancillary powers

The current law

8.95 At present, a High Court judge cannot exercise the powers under section 59 of the CJPA when hearing a claim for judicial review. For example, where a warrant has been quashed and no order, or a conditional order, is made for the material seized to be returned, an investigator must make a separate application under section 59(6) of the CJPA to retain the material. As a consequence, sometimes immediately following a judicial review hearing and in the same courtroom, a High Court judge will sit as a judge of the Crown Court to dispose of the section 59 application.[81]

The consultation paper

8.96 We suggested at paragraph 7.95 of our consultation paper that, to avoid the duplication of proceedings, whenever judicial review of a search warrant is granted, the High Court should have all the powers of the Crown Court under section 59 or the new procedure, and should make any necessary order for the return or retention of the materials as part of its judgment in the judicial review proceedings.

Consultation responses

8.97 Three consultees[82] suggested that on an application for judicial review, the High Court should have the powers and duties of the Crown Court in relation to the return or retention of material under section 59 of the CJPA. It was argued that this would allow it to determine ancillary section 59 applications and remove the need for multiple cases to be brought in relation to one warrant.[83]

8.98 Dijen Basu QC explained that, at present, High Court judges are not infrequently asked to sit in their capacity as judges of the Crown Court to hear a section 59 application immediately following the end of a judicial review hearing involving a challenge to a search warrant. The section 59 application must be then married up with the judicial review hearing, as "the Crown Court sitting at the Royal Courts of Justice", for example, to the great bemusement of Crown Court listing officers. Therefore, it was suggested that it would be better for High Court judges to be able to determine a section 59 application made in response to a claim for judicial review, rather than having to sit in their capacity as judges of the Crown Court in order to exercise the power. This would enable costs orders to be made and obviate the need for breach to be dealt with as a contempt by the Crown Court.

---

81 *R (Goode) v Nottingham Crown Court* [2013] EWHC 1726 (Admin), [2014] ACD 6 at [49] to [50]; and *R (Dulai) v Chelmsford Magistrates' Court* [2012] EWHC 1055 (Admin), [2013] 1 WLR 220 at [38].

82 Dijen Basu QC; Bar Council and the Criminal Bar Association; Serious Fraud Office.

83 Dijen Basu QC; Bar Council and the Criminal Bar Association; Serious Fraud Office.

Analysis

8.99 We accept that, in practice, the High Court may prefer to leave the matter of a section 59 CJPA hearing to the Crown Court. We accept that where a High Court judge wishes to exercise the powers under section 59 of the CJPA it is possible, in theory, for a separate section 59 CJPA application to the Crown Court to be listed before the High Court judge who is hearing the judicial review so that the High Court judge can concurrently dispose of the judicial review and section 59 application. However, we agree with those consultees who responded that the High Court on judicial review should have the powers and duties of the Crown Court in relation to the return or retention of material under section 59 of the CJPA for the reasons given by consultees: cost and efficiency.

8.100 The question is how this could be best achieved. We consider that an amendment to section 59 of the CJPA may be the most desirable way of conferring the powers in section 59 of the CJPA on a High Court judge hearing a judicial review claim.

Recommendation 36

8.101 We recommend that a judge hearing a judicial review of a search warrant have the powers and duties of the Crown Court in relation to the return or retention of material under section 59 of the Criminal Justice and Police Act 2001.

Chapter 9: Sensitive material and public interest immunity

INTRODUCTION

9.1 Chapter 8 of the consultation paper discussed the procedure for dealing with sensitive information contained in an application for a search warrant, and claims for public interest immunity. Search warrant schemes envisage a purely ex parte procedure (in the absence of the defence) in which an investigator may rely on information when seeking a warrant whose disclosure to the subject of the warrant would be damaging to the public interest. An investigator may therefore later claim that information relied on in an application for a search warrant should not be disclosed to a person affected by a warrant because disclosure would create a real risk of serious prejudice to an important public interest. This is known as asserting public interest immunity. One common example of information in respect of which public interest immunity is asserted is information which identifies an informant.

9.2 We begin this chapter by setting out the procedure under the current law when search warrant applications involve sensitive material and public interest immunity claims in order to contextualise the consultation responses that we received and our analysis of them. We then summarise this section of our Consultation Paper and outline the issues raised by consultees in their consultation responses. We then discuss each of the topics raised by consultees in turn.

9.3 We look first at how sensitive material is stored following a search warrant application. We conclude that more prescriptive rules governing the handling of sensitive material in the Criminal Procedure Rules ("CrimPR") would be beneficial given the lack of a consistent approach. We consider that sensitive material is likely to be better protected if stored by the investigator, however, discretion must ultimately reside with the court. We provide a suggestion of what more prescriptive rules might look like and then recommend that the Criminal Procedure Rule Committee ("CPRC") consider amending the CrimPR to include rules governing the storage of sensitive material provided to the court during a search warrant application. We end the section by discussing two related issues concerning the use of a separate sensitive document when applying for a search warrant.

9.4 We turn to discuss the investigator's right to register an objection to an application by a person affected by a warrant for supply of the underlying information, the procedure for which is currently set out in the CrimPR. We recognise the concerns expressed to us that the current procedure carries the risk that an investigator might not have notice of a request for disclosure of an application in time, or at all, resulting in the disclosure of highly sensitive information. We discuss a number of options for reform, none of which we are entirely persuaded by. We therefore recommend that the CPRC consider the desirability of amending the rules governing an investigator's right to issue an objection, with the aim of ensuring that the investigator receives the relevant request.

9.5 We then discuss the desirability of formalising the matters relevant to the court's decision to disclose sensitive material. We recognise the value in elaborating on such matters. Accordingly, we recommend that consideration be given to amending the Criminal Practice Directions to set out matters that should be considered by the court when determining whether sensitive material ought to be withheld on the grounds of public interest immunity.

9.6 Finally, we discuss the consequences of a decision to order disclosure of sensitive material and whether the investigator should have the option to avoid disclosure by returning the material seized. We explain that, for several reasons, we consider that it would be inappropriate for law enforcement agencies to be able to avoid the disclosure of material where it is ordered by the court.

THE CURRENT LAW

Preparing a search warrant application

9.7 Prior to preparing an application, an investigator may identify material as sensitive. Law enforcement agencies will have their own procedures by which they grade sensitive material. The Code of Practice made under the Criminal Procedure and Investigations Act 1996 sets out how police officers are to record, retain and reveal to the prosecutor material obtained in a criminal investigation. This Code provides a non-exhaustive list of examples of material which may be deemed sensitive for the purposes of disclosure. For example, the list includes material relating to national security and the identity of informants. Whether information is sensitive, however, depends on the facts of the particular case.

9.8 When preparing a search warrant application, an investigator has two choices regarding the presentation of sensitive material. The first option is to include it in the body of the search warrant application. The second option, as provided for in rule 47.26(4) of the CrimPR, is to append the sensitive material to the application in a separate document, marked accordingly, and in that document include the reason(s) why that information ought not to be supplied to anyone other than the court. Such a "sensitive material document" may be sent to the court electronically with the application or provided in hard copy where the applicant has concerns about security. Commenting on the second option, the Supreme Court in *Haralambous* stated:

> It is no doubt sensible practice for applicant officers to adopt, where practicable and where time permits, the permissive rule 47.26(4) procedure and to identify information which they contend ought not to be supplied to anyone but the court. That may reduce the risk of accidental disclosure, and no doubt a magistrate considering an application would, where this is done, bear in mind that there is information which a person affected might never be able to test. But there is no suggestion, or I think likelihood, that [rule 47.26(4)] intended the constable or magistrate at this early stage, when speed is often of the essence, to try to form a definitive view as to what the public interest might ultimately prove to require. That is an exercise which in accordance with the rules falls to be undertaken at a later stage by a magistrate under the procedure in *Bangs* and/or a Crown Court under section 59 of CJPA.[1]

The search warrant application hearing

9.9 During the search warrant application hearing, the issuing authority will consider all the material to determine whether there are reasonable grounds to believe or suspect (as the case may be) that the statutory grounds for issuing the warrant are met. Importantly, the issuing authority does not determine whether the material is in fact sensitive or whether it is immune from disclosure because of public interest immunity.

---

1 *R (Haralambous) v Crown Court at St Albans* [2018] UKSC 1, [2018] AC 236 at [27].

9.10 After a search warrant is granted, the information or application form will be stored by the court. If a sensitive material document was appended to the application, it will be either stored by the court or returned to the investigator. Rule 47.3(1)(b) CrimPR provides that, unless the court otherwise directs, the court officer may arrange for the whole or any part of a written application to be kept by some other appropriate person, subject to any conditions that the court may impose. Again, no issue of public interest immunity arises at this stage.

Making an application for information following the execution of a search warrant

9.11 Search warrants are granted without notice, which means that a person affected by a warrant will only learn that it was granted if it is executed. Rule 5.7(6) to (9) of the CrimPR, which is in effect a codification of the procedure in *Bangs*,[2] set out the procedure which must be followed when a person affected by a warrant wishes to see the information or application kept by the court. At paragraph 7.178 above, we write that it would be appropriate to state how to apply for a copy of the information sworn in support of the warrant in the notice of powers and rights. At Recommendation 32 above, we recommend that there be a statutory duty to provide a notice of powers and rights to an occupier.

9.12 Rules 5.7(2) and 5.7(6)(a) CrimPR provide that the person affected by the warrant must apply to the court officer for the underlying information and serve the request on the investigator who applied for the warrant. The request is therefore for disclosure of the grounds on which the warrant was issued. This may be contained in the application form, separate application schedules, additional notes recorded during the hearing, the issuing authority's reasons for issuing the warrant, and any transcript of the hearing.[3]

9.13 This application procedure does not involve a challenge to, or result in a determination of, the lawfulness of the warrant, entry, search or seizure. Rather, the information is often sought in order to determine whether to make such a challenge, or to assist with live proceedings.

9.14 The judge who considers an application for information might not be the same judge who issued the warrant (the issuing authority). For this reason, we will now refer to the court rather than the issuing authority.

Objecting to an application for information

9.15 Under rule 5.7(6)(b) CrimPR, the investigator has 14 days to object to an application by a person affected by a warrant for supply of the underlying information. An objection may be on public interest immunity grounds or for other reasons. The notice of objection must be served on both the court and person requesting the information. If the investigator wants a hearing, they must explain why one is needed.

9.16 Rule 5.7(7) CrimPR provides that the notice of objection must explain which information the investigator objects to disclosing and the grounds for the objection. However, rule 5.7(8) CrimPR provides that, where the investigator considers that the notice of objection includes information that the person applying for the information should not see, the investigator must:

---

2 *Commissioner of the Metropolis v Bangs* [2014] EWHC 546 (Admin), (2014) 178 JP 158.

3 *R (Austen) v Chief Constable of Wiltshire Police and South East Wiltshire Magistrates' Court* [2011] EWHC 3386 (Admin) at [49]; *Fitzgerald v Preston Crown Court* [2018] EWHC 804 (Admin) at [8].

(1) omit that material from the notice served on that person;

(2) mark the material to which the objection relates to show that this material is only for the court; and

(3) with that material include an explanation of why it has been withheld, for example, on public interest immunity grounds.

The closed material procedure and determination of public interest immunity

9.17 Rule 5.7(9) CrimPR sets out the closed material procedure. Rule 5.7(9)(a) CrimPR provides that a hearing of the application may take place, wholly or in part, in the absence of the party or person applying for information. Rule 5.7(9)(b) CrimPR then sets out the suggested sequence in which representations are heard.[4] The general rule is that the court must consider, in the following sequence:

(1) representations first by the party or person applying for information and then by the objector, in the presence of both; and then

(2) further representations by the objector, in the absence of that party or person.

However, the court may direct other arrangements for the hearing.

9.18 Several principles concerning the determination whether material attracts public interest immunity can be extracted from case law.

(1) The starting principle is that the person affected by the warrant is entitled to a copy of the information that persuaded the issuing authority to issue the warrant.[5]

(2) Documents which ought otherwise to be disclosed may only be withheld if the court concludes that the public interest that the evidence be withheld outweighs the public interest in the administration of justice.[6]

(3) Therefore, in all cases where the issue of public interest immunity is raised, the public interest in the material being withheld must be balanced against the public interest in the administration of justice. The goal is to ensure that the individual and the court have the fullest possible access to all relevant material.[7]

(4) When carrying out the balancing exercise, the court must ask whether there is a *real risk* that disclosure would result in harm to the relevant public interest.[8] It does not follow that a higher standard of cogency is required of a party asserting public interest

---

4 See also *Competition and Markets Authority v Concordia International RX (UK) Ltd* [2018] EWHC 3448 (Ch), [2019] Lloyd's Rep FC 183; and *R (Jordan) v Chief Constable of Merseyside Police* [2020] EWHC 2274 (Admin) at [12].

5 *EastEnders Cash & Carry v South Western Magistrates Court* [2011] EWHC 937 (Admin), [2011] 2 Cr App R 11 at [7].

6 *Al Rawi v Security Services* [2011] UKSC 34, [2012] 1 AC 531 at [145]; *R v Chief Constable of West Midlands Police ex parte Wiley* [1995] 1 AC 274, 280 to 281; and *R (Jordan) v Chief Constable of Merseyside Police* [2020] EWHC 2274 (Admin) at [17].

7 *Commissioner of Police for the Metropolis v Bangs* [2014] EWHC 546 (Admin), (2014) 178 JP 158 at [40].

8 *Commissioner of the Metropolis v Bangs* [2014] EWHC 546 (Admin), (2014) 178 JP 158 at [50].

immunity in a case where material attracting public interest immunity may be considered by the court in a closed material procedure.[9]

(5) While the decision ultimately lies with the court, proper weight must be given to the views of the public official (for instance the Government Minister or police officer) who has claimed public interest immunity.[10]

(6) Depending on which public interest or interests the investigator believes is at risk, some further principles may also be relevant.

(a) *The protection of informants* – Material concerning the identity of informants is generally immune from disclosure. It is in the public interest for informants to help the police to detect and prevent crime, and therefore protecting informants is given considerable weight during the balancing exercise.[11]

(b) *Risk to national security, relationship with other Governments or identifying covert surveillance* – The widest margin is likely to be accorded to the investigator when they are concerned about risks to national security or our relationships with other Governments, or the risks of identifying methods of covert surveillance or informers.[12]

(c) *Risk of a miscarriage of justice* – The margin will generally be different when the investigator is concerned about the risk of a miscarriage of justice because that is a matter on which a judge is better able to form a view, depending on the facts of the case.[13]

9.19 When a claim to public interest immunity is established which would require all of the information held by the court to be withheld, the court must consider whether the substance of the redacted information could be paraphrased in a way that would convey its essential elements without damaging the public interest.[14] The provision of extracts or a summary is known as a "gist".

9.20 There are circumstances where it may be in the public interest to withhold even the gist of the information on which the investigator relied when applying for the warrant.[15] Therefore, there is no irreducible minimum level of disclosure. If a gist document is prepared, it should accurately represent the information which can be disclosed.[16]

---

9 *R (Jordan) v Chief Constable of Merseyside Police* [2020] EWHC 2274 (Admin) at [17(e)].

10 *Conway v Rimmer* [1968] AC 910, 952 per Lord Reid; and *Commissioner of the Metropolis v Bangs* [2014] EWHC 546 (Admin), (2014) 178 JP 158 at [48].

11 *Chief Constable of the Greater Manchester Police v McNally* [2002] EWCA Civ 14, [2002] 2 Cr App R 37; and *Commissioner of the Metropolis v Bangs* [2014] EWHC 546 (Admin), (2014) 178 JP 158 at [45].

12 *Commissioner of the Metropolis v Bangs* [2014] EWHC 546 (Admin), (2014) 178 JP 158 at [49].

13 *Commissioner of the Metropolis v Bangs* [2014] EWHC 546 (Admin), (2014) 178 JP 158 at [49].

14 *R v Chief Constable of West Midlands Police ex parte Wiley* [1995] 1 AC 274, 306 to 307; and *Commissioner of the Metropolis v Bangs* [2014] EWHC 546 (Admin), (2014) 178 JP 158 at [42].

15 *R (Haralambous) v Crown Court at St Albans* [2018] UKSC 1, [2018] AC 236 at [65].

16 *Commissioner of the Metropolis v Bangs* [2014] EWHC 546 (Admin), (2014) 178 JP 158 at [43].

9.21 Where a claim to public interest immunity is rejected, the court must order disclosure of the grounds for issuing the warrant.

9.22 In some cases, the determination of a public interest immunity claim is dealt with as a prelude to a live judicial review application for an order quashing a search warrant.[17] Chamberlain J has set out the appropriate procedure to follow where a public interest immunity claim has been upheld and the material attracting public interest immunity is to be considered in a closed material procedure in the context of a substantive judicial review hearing.[18]

THE CONSULTATION PAPER

9.23 The procedure in the CrimPR outlined above was endorsed in passing by the Supreme Court in *Haralambous*.[19] The case was concerned with the narrow issue of the extent to which a court can rely on information which cannot be disclosed to a person affected by a search warrant because of public interest immunity.

9.24 In light of the endorsement in *Haralambous*, our provisional view in the consultation paper was that the procedure governing sensitive material and public interest immunity was not in need of reform. During our pre-consultation engagement though, stakeholders raised three potential issues on which we sought further views:

(1) a lack of knowledge of the CrimPR governing the procedure in respect of sensitive material and public interest immunity in search warrant cases;

(2) a divergence of views on certain aspects of the procedure; and

(3) a need for clarification on areas not currently dealt with by the CrimPR.

9.25 In the consultation paper we set out our understanding of the current law and invited consultees' views[20] on whether reform was required to these three areas or any other aspects of the procedure for dealing with sensitive information and claims for public interest immunity.

OUTLINE OF CONSULTATION RESPONSES

9.26 Sixteen consultees[21] answered the question about whether reform was needed. Five considered that the current procedure for dealing with sensitive information and public interest immunity in relation to search warrants requires reform;[22] and 11 considered that the

---

17 See for example *R (Jordan) v Chief Constable of Merseyside Police* [2020] EWHC 2274 (Admin).

18 *R (Jordan) v Chief Constable of Merseyside Police* [2020] EWHC 2274 (Admin) at [35].

19 *R (Haralambous) v Crown Court at St Albans* [2018] UKSC 1, [2018] AC 236 at [27].

20 Consultation Question 41.

21 Crown Prosecution Service; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; The Law Society; Magistrates Association; Dijen Basu QC; Bar Council and the Criminal Bar Association; Metropolitan Police Service; National Crime Agency; Competition and Markets Authority; Serious Fraud Office; Financial Conduct Authority.

22 Crown Prosecution Service; Independent Office for Police Conduct; Metropolitan Police Service; National Crime Agency; Serious Fraud Office.

current procedure for dealing with sensitive information and public interest immunity in relation to search warrants does not require reform.[23]

9.27 The majority of consultees did not consider that the current procedure for dealing with sensitive information and public interest immunity required reform. Of those who did, four issues were raised:

(1) it is unclear whether highly sensitive material should be stored by the issuing authority or the investigator making the application;

(2) whether, when an application is made for sensitive documents held by a court, the investigator should be required to confirm receipt of the application before the court makes its decision on whether the documents should be released;

(3) whether the decision-making procedure adopted by the courts when determining a public interest immunity application should be formalised; and

(4) whether an investigator should be able to respond to an order for the disclosure of sensitive material by returning the seized material instead.

9.28 We deal with each of these issues in turn. In each case we consider the underlying issue, whether reform is required and, if so, the most appropriate method of reform.

THE STORAGE OF SENSITIVE MATERIAL

Comments made by consultees

9.29 Several consultees emphasised the importance of ensuring that sensitive material is adequately protected.[24] Consultees stated that there is no consistent practice as to whether sensitive material documents appended to applications for search warrants are stored by the issuing authority or returned to the investigator.

9.30 As was set out at paragraph 9.8 above, when investigative agencies apply for a search warrant, any sensitive material is either contained in the application or is appended in a separate document "marked accordingly" pursuant to rule 47.26(4) CrimPR. The Serious Fraud Office ("SFO") observed that it is a choice, rather than a requirement, to append sensitive material in a separate document under rule 47.26(4) CrimPR. It argued that including sensitive material in the main application form may lead to it being unintentionally disclosed.

9.31 The Crown Prosecution Service ("CPS") suggested two options for reform, both of which envisage including sensitive material in a separate document.

(1) The first option is to permit an investigator to take the sensitive material document away after the hearing if two conditions are met:

---

[23] HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; The Law Society; Magistrates Association; Dijen Basu QC; Bar Council and the Criminal Bar Association; Competition and Markets Authority; Financial Conduct Authority.

[24] Crown Prosecution Service; National Crime Agency; Metropolitan Police Service; Serious Fraud Office; Financial Conduct Authority.

(a) the non-sensitive application indicates that there is a separate sensitive material document; and

(b) the sensitive material document is endorsed by the issuing authority, and its existence is recorded so that it can be identified at a later stage.

(2) The second option is to clarify the phrase "marked accordingly" in rule 47.26(4) so that sensitive material documents are appropriately stored by the court and there is no risk of unintentionally disclosing their contents.

9.32 The SFO suggested that there should be a provision for taking sensitive information away from a hearing, which would be triggered by certain circumstances. For example, it could be triggered if the material relates to national security and/or the court cannot accommodate a sufficiently secure method of storage. Such material would be held by the investigator in accordance with an order of the court.

9.33 The Metropolitan Police Service ("MPS") observed that if it states on the application form that sensitive material is contained in a separate document, this may itself pose a risk were the application form to be disclosed.

Analysis

The storage of sensitive material

9.34 As we noted at paragraph 9.10 above, part 47 of the CrimPR governs the possession and control of documents. Rule 47.3(1)(b) provides that, unless the court otherwise directs, the court officer may arrange for the whole or any part of a written application to be kept by some other appropriate person, subject to any conditions that the court may impose.

9.35 We accept that this rule is not directed specifically at sensitive material and that it confers a wide discretion. On one view, this flexible rule suffices to regulate who ought to hold on to sensitive material and on what terms. However, given the importance of protecting sensitive material and the unique considerations which may be involved, in our view more prescriptive rules would be beneficial.

9.36 We found no evidence of a consistent practice in relation to the storage of sensitive material. Enquiries made with Her Majesty's Courts and Tribunals Service ("HMCTS") indicated that there is no official guidance on court storage of sensitive material, or the clearance levels required to handle it. Local practices appear to have developed in individual court centres. We consider that this diversity of practice further justifies more detailed guidance on the storage of sensitive material being set out in the CrimPR.

9.37 Turning then to what those rules ought to be, our starting principle is that sensitive material must be securely stored. If not, there could be serious consequences: in extreme cases, the lives of informants and their families could be at risk. The Supreme Court observed in *Haralambous* that articles 2 and 3 of the European Convention on Human Rights may place a duty on the police to protect the safety of an informant.[25]

9.38 For these reasons, we consider that there are strong arguments for permitting law enforcement agencies to retain responsibility for storing sensitive material. The fewer places

[25] *R (Haralambous) v Crown Court at St Albans* [2018] UKSC 1, [2018] AC 236 at [27].

in which sensitive material is retained, the lower the chance of inadvertent disclosure. In courts, even where secure facilities are provided for storing information, it is not clear that in all instances these are only accessible to the issuing authority, or even exclusively to judges. Further, in cases where applications are made out of court hours to the magistrate at their own home, it is not possible to store sensitive material on the magistrate's premises.

9.39 Law enforcement agencies may also have better security facilities and more stringent protocols for the handling of sensitive material than court centres given their routine handling of such material. Within any agency, sensitive material is likely to be accessible only to those with the requisite level of clearance.

9.40 Against this, we can see that storage by the investigator may raise concerns. If material needs to be considered later by a court to determine whether disclosure should be denied on public interest immunity grounds, there may be concerns over tampering or delay in supply. However, we do not regard this as a sufficient objection nor a persuasive argument: investigators must act in accordance with the law. Further, such a risk exists with any evidence acquired by an investigator.

9.41 The matter is more complicated when sensitive material is included in the body of the application rather than in a separate document. In such cases, we do not consider that the whole application should be retained by the investigator: the court would be left with no trace of the search warrant application. If there were a rule that applications containing sensitive material had to be kept by the court, we consider that this would also incentivise investigators to prepare a separate document for sensitive material, in accordance with the permissive rule at 47.26(4) CrimPR, and as endorsed by the Supreme Court.[26]

9.42 For these reasons, we consider that sensitive material is likely to be better protected if stored by the investigator. However, we accept that this might not always be true, and discretion must ultimately reside with the court. We therefore suggest rules along the following lines:

(1) the default position ought to be that the investigator should store any separate sensitive material document;

(2) there should be an exception where the court considers that it ought to store the separate sensitive material document. In coming to this decision, the court should consider:

(a) the sensitivity of the material, including the explanation given by the investigator under rule 47.26(4) CrimPR as to why the material is sensitive;

(b) whether the court can accommodate a sufficiently secure method of storage; and

(c) any other factors the court considers relevant;

(3) if the court is of the view that the sensitive material ought to be stored by the investigator, it must ensure that:

---

[26] *R (Haralambous) v Crown Court at St Albans* [2018] UKSC 1, [2018] AC 236 at [27].

(a) the application form, which is retained by the court, indicates that there is a separate sensitive material document; and

(b) the sensitive material document is endorsed by the issuing authority, and its existence recorded,[27] so that it can be identified at a later stage;

(4) if the sensitive material is included within the application form rather than in a separate document, then the investigator should not be allowed to store the application form.

9.43 We recommend that the CPRC consider including rules to this effect in the CrimPR.

Recommendation 37

9.44 We recommend that the Criminal Procedure Rule Committee consider amending the Criminal Procedure Rules to include rules governing the storage of sensitive material provided to the court during a search warrant application.

References to sensitive material in the application

9.45 We turn now to address two ancillary matters relating to the storage of sensitive material that were raised in consultation responses. First, we consider the concern expressed by the MPS at paragraph 9.33 above that referring to a separate sensitive document in an application form disclosed to a person affected by a warrant may pose a security risk.

9.46 We consider that it is beneficial to the court for an application form to state whether a separate sensitive material document exists. However, as indicated by the Supreme Court in *Haralambous*, it would be open to the court hearing an application for information following the execution of a warrant to hold that the existence of the sensitive material should not be disclosed to the person affected by the warrant.[28]

9.47 Therefore, the answer lies in redacting the fact that a separate sensitive material document exists from the application form before it is supplied to the person affected by the warrant. This would remove any security risk associated with disclosing the existence of a separate sensitive material document.

Requiring sensitive material to be appended in a separate document

9.48 As mentioned at paragraph 9.30 above, the SFO observed that it is a choice, rather than a requirement, to append sensitive material in a separate document and that including sensitive material in the main application form may lead to it being unintentionally disclosed. We have considered whether rule 47.26(4) CrimPR should in fact impose a mandatory requirement.

9.49 We are not persuaded that investigators should be required to append sensitive material to the application in a separate document. We consider that to retain operational flexibility, the preparation of a separate document should be discretionary.

---

[27] For example, “five-page sensitive material document provided”.

[28] *R (Haralambous) v Crown Court at St Albans* [2018] UKSC 1, [2018] AC 236 at [65].

9.50 Such flexibility will be important on occasions when a warrant is required urgently, leaving no time to prepare a separate document. A good example would be where a previously unknown set of premises is discovered during the course of a search and access is needed quickly to guard against material being destroyed. Nonetheless, a sensitive material document should be prepared where practicable, as noted by the Supreme Court in *Haralambous*, quoted at paragraph 9.8 above.

9.51 We reiterate that we see value in including a prompt on search warrant application forms for applicants to include any sensitive material in a separate document, as we suggest at paragraph 4.108 above. This would promote the use of separate sensitive material documents.

THE INVESTIGATOR'S RIGHT TO REGISTER AN OBJECTION

Comments made by consultees

9.52 As set out at paragraphs 9.11 to 9.16 above, where a person affected by a warrant requests a copy of the application form or other information, they must also serve the request on the investigator who applied for the warrant. The investigator then has 14 days from when the request was served to issue a notice of objection.

9.53 Three consultees[29] suggested that, because the duty is on the person affected by a warrant to serve the investigator and court independently with a copy of their application, the 14-day limit may mean that an investigator does not have notice of a request in time, or at all. The underlying concern was that sensitive material may be disclosed without the investigator having considered or made representations on the potential dangers of doing so, creating a real risk of serious prejudice to an important public interest.

9.54 Some consultees suggested that the investigator should be required to confirm that they have received the request before potentially highly sensitive material is provided to the person affected by the warrant. The SFO argued that it would be prudent for the court to contact the investigator to obtain written confirmation of receipt and check that they have no objections before disclosing the underlying information.

9.55 The CPS suggested that it should be assumed that an investigator objects to the disclosure of any separate sensitive material document, unless they provide written consent to its disclosure.

Analysis

9.56 We recognise that the current procedure carries the risk that an investigator might not have notice of a request for disclosure of an application in time, or at all. We also accept that disclosure in such circumstances might risk serious prejudice to an important public interest, such as by risking the life of an informant.

9.57 At the same time, we lack sufficient evidence as to whether this is a real, rather than merely perceived, risk. In practice, the procedural safeguard must be the lay justice or district judge (magistrates' courts) who is considering an application from an occupier for the information. The judge ought to reach their own assessment of whether disclosing particular details might

[29] Crown Prosecution Service; Metropolitan Police Service; Serious Fraud Office.

risk prejudice to an important public interest. If they are concerned that it would, the judge may decide to hold a hearing before reaching a decision on the application.

9.58 Good sense also suggests that assurances could be sought that the notice was given to, or received by, the investigator. The court should therefore satisfy itself that the investigator has seen the request.

9.59 On balance, it is our view that the issue merits consideration. We have considered several ways in which this risk could be minimised, some of which could be combined, including:

(1) requiring the investigator to confirm that they received the request before the information is disclosed to the person affected by the warrant;

(2) extending the 14-day period given to investigators to object to a request;

(3) requiring the court, rather than the occupier, to contact the investigator; and

(4) maintaining the current position but requiring the copy of the warrant served on the occupier to specify the investigator's email or postal address.

We discuss each of these possible amendments below in turn.

Requiring confirmation that the investigator received the request

9.60 This was the most popular suggestion amongst consultees. However, in our view, neither starting the 14-day clock from the date on which an investigator confirms that they received the request, nor requiring that disclosure can only be ordered where an investigator has confirmed that they received the request, are proportionate solutions to this problem.

9.61 First, a requirement that the investigator confirm receipt might incentivise an investigator to delay confirming receipt, or not do so at all. In extreme cases, an investigator could effectively block disclosure (although we accept that this is unlikely). For this reason, the court must have the power to disclose information in the absence of confirmation. One possible solution is that, once the 14-day notice period is over, the court issues a summons for the officer to attend, and if the officer does not respond within a further 14 days the court may disclose the information.

9.62 Secondly, we note that a requirement to confirm receipt within a set number of days is not a formula typically found in the CrimPR. This is for good reason: it would be undesirable to have a system where proof of receipt is always required for service to be deemed effective. This is because it would lead to disputes as to whether documents were really received, hence the adoption of deemed dates of service in the Civil Procedure Rules.

9.63 On balance, therefore, while confirmation of receipt of an application might be advantageous because of the potential risk of serious prejudice to an important public interest, we are not persuaded that it would be a necessary or proportionate amendment.

Extending the period of 14 days to object

9.64 This suggestion can be dealt with quickly. We are not convinced that extending the period of 14 days on its own would be of much benefit. If a request for information is not successfully served on the investigator, and therefore never reaches them, then extending the period within which they can register an objection would be of no advantage.

9.65 Extending the period may also cause prejudice to a person who wishes to challenge the decision to issue a search warrant. The time limit to bring a judicial review application typically runs from the date on which the decision (in this case to issue a search warrant) was taken.[30] The longer an investigator is given to register an objection, the less time a person affected by a warrant may have to assess whether to bring judicial review proceedings.

Requiring the court to contact the investigator

9.66 At first glance, there are good reasons to require the court officer, rather than the occupier, to contact the investigator. If this were the case, the 14-day period could run from the date of the request by the court officer to the investigator.

9.67 With the increase in search warrant applications being submitted electronically, it should usually be relatively straightforward for a court officer to forward a request to the relevant investigator. In addition, court officers already serve summonses and so this would not introduce a new strand of work.

9.68 However, requiring the court to contact the investigator would place administrative costs and burdens on the court, albeit minor ones. There is also still a chance that an investigator would not receive the application. We are therefore equally unpersuaded by an amendment along these lines.

Requiring the warrant to specify a contact address

9.69 Maintaining the current position, but requiring the copy of the warrant served on the occupier to include the investigator's contact details, has several attractions. Providing the occupier with contact details, such as a dedicated email address, would clearly reduce the risk of a request made by a person affected by the warrant not reaching the investigator.

9.70 If warrants were amended to include the investigator's contact details, this could encourage a person affected by a warrant to send one email to both the investigator and the court officer. If the person affected by a warrant did send an email to both, the court considering the request would know if it had been served on the investigator. However, there are several reasons why this may not happen. The person affected by a warrant may not have access to email, or they may choose to send two separate emails or to apply in another way, for instance by post. A transcription error with the investigator's email address may also occur, which is not noticed by the court officer. Additionally, requiring the warrant to specify a contact address would only address the problem of a person affected by a warrant who is genuinely mistaken as to where to serve the application, not one who has no intention of serving it.

Conclusion

9.71 We are not entirely persuaded by any of the possible amendments discussed above. However, we recognise the concerns raised by consultees regarding the disclosure of sensitive material which might otherwise attract public interest immunity. We therefore recommend that the CPRC consider the desirability of amending the requirement under rule 5.7(6) CrimPR that an investigator has 14 days to issue an objection after being served with

---

30 *R (Sustainable Development Capital LLP) V Secretary of State for Business, Energy and Industrial Strategy* [2017] EWHC 771 (Admin) at [32].

a request for the supply of information, with the aim of ensuring that the investigator receives the relevant request for disclosure of the information.

Recommendation 38

9.72 We recommend that the Criminal Procedure Rule Committee consider the desirability of amending the requirement under rule 5.7(6) that an investigator has 14 days to issue a notice of objection after being served with a request for the supply of information.

FORMALISING THE MATTERS RELEVANT TO THE DECISION TO DISCLOSE SENSITIVE MATERIAL

Comments made by consultees

9.73 The CPS and MPS argued that the decision-making process when an investigator claims that certain material is sensitive should be set out in the CrimPR. The CPS suggested that the following matters should be considered by the court:

(1) whether a form of disclosure can be made which does not compromise the material in respect of which sensitivity is claimed;

(2) whether material claimed by the investigator to be sensitive is in fact sensitive, applying the test in *R v H*,[31] and whether a non-exhaustive list of examples of sensitive material could be provided; and

(3) whether the material claimed to be sensitive could reasonably be expected to assist a challenge to the warrant.

Analysis

9.74 We can see the value in elaborating on matters that are relevant to the decision on whether the court should disclose sensitive information. In particular, setting out the matters which the court must consider would likely make decision-making more consistent. However, we make two observations.

9.75 First, we do not consider that the matters should be set out in the CrimPR. What consultees envisage are factors which relate to the court's jurisdiction to make a ruling on public interest immunity. The factors are not, strictly speaking, a matter of procedure. For this reason, we consider that the Criminal Practice Directions[32] ("CrimPD") would be a more suitable place to set out the decision-making process.

9.76 Secondly, the content of the matters must be considered carefully and in the round. It is not a linear test: depending on the circumstances, the court may be required to consider a range

---

31 [2004] UKHL 3, [2004] 2 AC 134 at [36]. The House of Lords held that the court must address a series of questions, including whether there is a real risk of serious prejudice to an important public interest (and, if so, what) if full disclosure of the material is ordered.

32 The Criminal Practice Directions, which are issued under the authority of the Lord Chief Justice, operate in conjunction with the CrimPD in a supplementary manner, thereby forming an integrated procedural framework for criminal cases.

of factors. We have distilled a number of relevant observations from case law at paragraphs 9.18 to 9.20 above, which make clear that the decision-making process must be formulated carefully. We consider that it would be both possible and desirable to do this in the CrimPD.

Recommendation 39

9.77 We recommend that the Criminal Procedure Rule Committee consider amending the Criminal Practice Directions to set out matters that should be considered by the court when determining whether sensitive material ought to be withheld on the grounds of public interest immunity.

THE CONSEQUENCES OF A DECISION TO ORDER DISCLOSURE

Comments made by consultees

9.78 On consultation the CPS and the MPS invited us to consider the consequences where the court rules against a claim of public interest immunity and orders that the material deemed sensitive by the investigator must be disclosed.

9.79 In a criminal trial, a prosecution may be discontinued without the consent of the court up until the close of the prosecution case.[33] This decision may also be taken during the pre-trial stage, for instance when the court orders disclosure and the prosecutor considers that there is a real risk that disclosure would endanger an informant. Therefore, during the pre-trial and trial stage, the prosecutor has, in effect, the choice to decline to disclose. If the court orders disclosure the prosecution can discontinue the case and offer no evidence, rather than disclosing the material.

9.80 The CPS and MPS were concerned with the position at the investigative stage. Where a claim to public interest immunity is unsuccessful and disclosure is ordered, they questioned whether the investigator should have the option to avoid disclosure by returning the material seized. They suggested that there could be circumstances in which an investigator would prefer to return material seized rather than disclose material they regard as sensitive.

Analysis

9.81 Under the current law, where a public interest immunity claim fails the court must order disclosure of the grounds for issuing the warrant. In practical terms, either the court officer or the investigator must then supply the information to the person affected by the warrant. There is no option for the investigator to return the items seized instead. Further, the court has no statutory power to order the return of material as there is no determination made during a public interest immunity hearing on the lawfulness of the warrant, entry, search or seizure.

9.82 We understand that in certain circumstances law enforcement agencies would prefer to return the items seized rather than disclose material they regard as sensitive. It is also possible that, in certain circumstances, occupiers would prefer return of their items rather than the sensitive information. For example, an occupier may only request a copy of the

[33] *R v Grafton* [1993] QB 101.

information relied upon by the investigator to assess whether to make an application for the return of material under section 59 of the Criminal Justice and Police Act 2001 ("CJPA").

9.83 However, we do not consider that a power for the investigator to return the material seized, instead of disclosing information they deem to be sensitive, would be either desirable or workable in practice.

9.84 An investigator will always have a route of appeal should they disagree with the court's decision to order disclosure of sensitive material. We consider that this is an adequate safeguard where disclosure of potentially prejudicial material is ordered, as can be seen in the case of *Bangs*.[34]

9.85 We are also hesitant to recommend such a power in the light of the following observation made by Lord Woolf CJ:

> Information may contain details of an informer which it would be contrary to the public interest to reveal. The information may also contain other statements to which public interest immunity might apply. But, subject to that, if a person who is in the position of this claimant asks perfectly sensibly for a copy of the information, then speaking for myself I can see no objection to a copy of that information being provided. The citizen, in my judgment, should be entitled to be able to assess whether an information contains the material which justifies the issue of a warrant. This information contained the necessary evidence to justify issuing the warrant.[35]

9.86 Here we are considering a scenario in which a court has held that there is no public interest immunity. We agree that in such circumstances, an individual should be entitled to view the grounds on which a warrant to enter, search and seize material from their premises has been sought.

9.87 There are also a number of practical issues that have compelled us to conclude that a power to return material in lieu of disclosure would be unworkable in practice.

9.88 First, would an investigator have to return or delete any copies made of seized material? If not, an investigator would potentially be able to "have their cake and eat it" by bringing a prosecution based on copies of material seized, even though material seized had been returned in lieu of disclosure of sensitive material. The court would have to interpret "return" as requiring no trace of the material to be left with the investigator who is returning it.[36] Any return would also have to preclude the use of section 59 of the CJPA to retain the material, otherwise an investigator could avoid disclosure yet retain the property.[37]

9.89 Secondly, what should happen to the information sworn in support of a warrant? It would seem unjust for an investigator to be able to seek to obtain a fresh warrant, otherwise the

---

34 *Commissioner of the Metropolis v Bangs* [2014] EWHC 546 (Admin), (2014) 178 JP 158.

35 *R (Cronin) v Sheffield Justices* [2002] EWHC 2568 (Admin), [2003] 1 WLR 752 at [29].

36 The definition of "return" was construed in such a fashion by the Divisional Court in *Business Energy Solutions Ltd v Crown Court at Preston* [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [83].

37 See *R (Van der Pijl) v Kingston Crown Court* [2012] EWHC 3745 (Admin), [2013] 1 WLR 2706 at [88] where Wilkie J quashed a warrant and ordered the return of property seized under warrant. In doing so, he considered that it would not be just to quash the warrant on terms which would stop the investigator from being able to make an application to the Crown Court under the Criminal Justice and Police Act 2001, s 59. See also *R (Panesar) v Central Criminal Court* [2014] EWHC 2821 (Admin), [2015] 4 All ER 754.

return of items would provide no real remedy. However, it might be that fresh evidence comes to light which meets the statutory grounds for issuing a warrant in relation to the same or another offence, without having to rely on the previous evidence. It seems to us that it must be possible for a search warrant to be obtained, and a prosecution to flow, from fresh evidence. If this was not possible, anyone suspected of a crime would be put in a far better position by the investigative authority obtaining a warrant than they would have been in had the warrant never been issued.

9.90 If the above is correct, then the risk of prosecution remains. It follows that the occupier is unlikely to gain much in the long-term from the return of their property. Therefore, the comparison made with the position pre-trial and at trial, where the withdrawal of a prosecution removes the possibility of a criminal conviction, is not a strictly analogous one.

9.91 Thirdly, what would happen to knowledge obtained during the search? For example, a search warrant may be executed on the "buyer" of a firearm which reveals information about the "seller" of the firearm. If material were returned, for instance, to avoid disclosing the identity of the informant, could this information be used as part of the grounds for obtaining a fresh warrant on different premises? It seems to us that the answer must be yes for the same reasoning above: anyone suspected of a crime would be put in a far better position by the investigative authority obtaining a warrant than they would have been in had the warrant never been issued.

9.92 Fourthly, what would the position be where no material is seized yet the occupier requests the grounds on which the warrant was issued? Here no concession can be made by the investigator by returning the material seized in lieu of disclosing sensitive material. For this reason (coupled with other reasons which we discuss below) the rule could not operate fairly where no material was seized. The only possible benefit of this rule for an occupier whose property is not seized is it could be specified that any information obtained during the search could not be used to obtain a fresh warrant. As observed above, this may have perverse outcomes and be of no substantive benefit to the person affected by the warrant. Nor, as we see it, could other remedies be provided for.

9.93 Additionally, if the option to return material in lieu of disclosure existed only where material was seized, this might encourage investigators to seize any potentially relevant material to ensure that they have the option to return items rather than disclosing material they regard as sensitive. Further, where the material seized is unimportant to the occupier, for instance a small number of copies of old business documents, it is likely that the occupier would far rather see the grounds for issuing the warrant than have the material returned.

9.94 Fifthly, to what extent, if any, would the reasons for the person requesting the grounds for issuing the warrant be taken into account when deciding whether to return material in lieu of disclosure? For example, a person affected by a warrant may feel aggrieved by both the decision to issue a warrant and the way in which it was executed. A person may therefore wish to see the grounds for issuing the warrant to assess whether to launch judicial review proceedings. In such cases, the return of material may be an ancillary concern, or of no concern at all. To this end it should be noted that a warrant must be quashed before an occupier can bring a civil action, such as trespass or interference with goods.[38] Therefore, if the court orders the return of items in lieu of disclosure, an occupier may be unable to pursue other remedies.

---

[38] *Mouncher v Chief Constable of South Wales* [2016] EWHC 1367 (QB) at [452].

9.95 One solution would be for the court to balance the wishes of the occupier and the investigator when assessing whether to order the return of items or disclosure of the material the investigator regards as sensitive. However, this risks overcomplicating the matter and would also be far different to allowing the investigator to choose the return of seized material over disclosure.

9.96 For all of these reasons, we consider that where a court has ruled that material would not pose a real risk to an important public interest, it would not be practicable for there to be a power, or duty, to order the return of items instead.

Chapter 10: Iniquitous material

INTRODUCTION

10.1 We use the term "protected material" as an umbrella term to refer to those categories of material that cannot be the target of a search warrant, or can be only if additional criteria are met. Depending on the statutory regime, those categories may include:

(1) legally privileged material,[1] which is absolutely exempt from being searched for and seized, unless seized under sections 50 and 51 of the Criminal Justice and Police Act 2001 because it is not reasonably practicable to sift indeterminable or inseparable material on the premises;[2]

(2) excluded material, which comprises confidential personal records, human tissue, tissue fluid and confidential journalistic material;[3] and

(3) special procedure material, confidential business records and non-confidential journalistic material.[4]

10.2 Protected material may lose its protected status, or be regarded as never having been afforded confidential status, if it is tainted by "iniquity", which is the subject of this chapter. Under the iniquity or "crime-fraud" exception, the protection afforded to special categories of material is lost when, broadly speaking, it is created, acquired or held for an iniquitous purpose. For example, communications between a lawyer and their client are ordinarily subject to legal professional privilege.[5] This means that such communications cannot be searched for or seized under a search warrant.[6] However, where the communications are held with the intention of furthering a criminal purpose, they are not subject to legal privilege.[7]

10.3 In setting out the current law in the consultation paper, we stated that, as with legal privilege, the special status afforded to other categories of material is lost where it is held in furtherance of a crime.[8] We reached this view on our reading of the Court of Appeal case of *R v Norman*.[9] This would mean, for example, that confidential journalistic material held with the intention of furthering a criminal purpose would not constitute excluded material under section 11 of the Police and Criminal Evidence Act 1984 ("PACE").

---

1 Police and Criminal Evidence Act 1984, s 10. We discuss the treatment of legally privileged material in Chapter 11.

2 Criminal Justice and Police Act 2001, ss 50(4) and 51(4).

3 Police and Criminal Evidence Act 1984, s 11. We discuss the treatment of excluded material in Chapter 12.

4 Police and Criminal Evidence Act 1984, s 14. We discuss the treatment of special procedure material in Chapter 13.

5 Police and Criminal Evidence Act 1984, s 10(1).

6 Police and Criminal Evidence Act 1984, s 8(1)(d). A similar exception is found in other search warrant provisions.

7 Police and Criminal Evidence Act 1984, s 10(2).

8 See Search Warrants: Consultation Paper (2018) Law Commission CP No 235 para 9.26.

9 *R v Norman* [2016] EWCA Crim 1564, [2017] 4 WLR 16 at [39].

10.4 The only consultation question that we asked relating to iniquitous material concerned special procedure material. Stakeholders raised concern around the position of special procedure material which is held with the intention of furthering a criminal purpose. This led us in our consultation paper to invite consultees' views on whether greater clarity needs to be introduced in defining searches for special procedure material held with the intention of furthering a criminal purpose.[10]

10.5 During the course of our consultation period, it transpired that the present law regarding the application of the iniquity exception was not so clearly understood. In particular, there were conflicting views regarding the extent to which forms of protected material other than those covered by legal privilege lose their confidentiality where created, held or acquired in furtherance of a crime.

10.6 The scope of the iniquity exception has a profound practical impact on the use of search warrants during criminal investigations. For this reason, we sought where possible to obtain consultees' views on their understanding of the current law as well as what the law ought to be.

10.7 In this chapter of the report, we set out a more detailed discussion of the current law, identifying specific areas of ambiguity. We then set out comments provided by consultees on the current law and how it ought to be reformed. We end by discussing matters which would be relevant to reforming the current law on iniquitous material.

10.8 We do not make a firm recommendation for reform. This is because the rules governing when material loses its protected status apply to other investigative powers. For example, production orders for special categories of material are sought far more frequently than search warrants, owing to the fact that search warrants are often predicated on the inability to obtain a production order. Any reform would therefore primarily impact the operation of other statutory powers on which we did not directly consult. Additionally, there are several matters that would require further consideration and consultation before reform was taken forward, which we discuss in this chapter. We therefore recommend that the Government considers whether the law relating to iniquitous material in the context of criminal investigations ought to be reformed.

THE CURRENT LAW

10.9 Below, we consider the extent to which the iniquity exception affects the three main categories of protected material that are exempted from search and seizure: legally privileged material, excluded material and special procedure material. In each of these categories we consider:

(1) how the iniquity exception is formulated; and

(2) the effect on the status of material tainted by iniquity, being either:

(a) complete loss of protection; or

(b) downgrading to a lesser category of protection.

[10] Consultation Question 47.

Legal professional privilege

10.10 The iniquity exception has developed in the context of legal professional privilege.[11] In *R v Cox and Railton*, Stephen J explained that the rule affording legal privilege does not include communications either criminal in themselves or intended to further any criminal purpose.[12] The reason for the iniquity exception is that the protection of such communications would be injurious to the interests of justice,[13] and involve an abuse of the lawyer/client relationship.[14]

10.11 The iniquity exception applies to both litigation privilege and legal advice privilege.[15] The lawyer need not be party to any iniquity for confidentiality to be lost.[16] Nor must the client be a party to any iniquity, but instead may be "an innocent tool".[17]

10.12 Section 10 of PACE provides a definition of legally privileged material.[18] Section 10 of PACE also provides that:

> Items held with the intention of furthering a criminal purpose are not items subject to legal privilege.[19]

10.13 According to the House of Lords, this is a statutory enactment of the common law position.[20] This accords with Hansard records, which indicate that the qualification for information held in furtherance of a criminal purpose in respect of legally privileged material was included in the Police and Criminal Evidence Bill as it had long been part of the well-established and understood definition of legally privileged material.[21]

Excluded material

10.14 The main developments regarding the iniquity exception have been in the context of confidential journalistic material. Confidential journalistic material was afforded special protection under section 11 of PACE and falls under the definition of "excluded material". Confidential journalistic material cannot be searched for under search warrant provisions which pre-date the enactment of PACE.[22] A search warrant can only be obtained under PACE for such material if a stringent set of access conditions are met under schedule 1 to PACE.[23] Confidential journalistic material has also been given protection under some search

---

11 A summary of the legal principles was recently distilled by the High Court in *Addlesee v Dentons Europe LPP* [2020] EWHC 238 (Ch) at [28] to [35].

12 *R v Cox and Railton* (1884) 14 QBD 153, 167.

13 *R v Cox and Railton* (1884) 14 QBD 153, 167.

14 *JSC BTA Bank v Ablyazov* [2014] EWHC 2788 (Comm), [2014] 2 CLC 263 at [68].

15 *Kuwait Airlines Corp v Iraqi Airways Co (No 6)* [2005] EWCA Civ 286, [2005] 1 WLR 2734.

16 *R v Cox and Railton* (1884) 14 QBD 153, 168; *Kuwait Airlines Corp v Iraqi Airways Co (No 6)* [2005] EWCA Civ 286, [2005] 1 WLR 2734 at [14].

17 *R v Central Criminal Court ex parte Francis & Francis* [1989] 1 AC 346, 395H to 397C.

18 Police and Criminal Evidence Act 1984, s 10(1).

19 Police and Criminal Evidence Act 1984, s 10(2).

20 *R v Central Criminal Court ex parte Francis & Francis* [1989] 1 AC 346, 355.

21 *Hansard* (HC), 3 May 1983, vol 42, cols 165 to 166.

22 Police and Criminal Evidence Act 1984, s 9(2).

23 Police and Criminal Evidence Act 1984, sch 1, paras 3 and 12.

warrant regimes enacted after PACE.[24] Importantly, journalistic material which is not held in confidence is still afforded protection as it falls under the definition of "special procedure material" under section 14 of PACE.

10.15 Hansard indicates a clear and conscious policy decision not to provide a statutory iniquity exception for excluded material and special procedure material under PACE as was provided for legally privileged material. It was said, to allay certain anxieties caused by this, that anybody holding material with a criminal purpose is almost always guilty of at least conspiracy and is therefore liable to arrest and, in light of that arrest, liable to have their premises searched.[25]

10.16 It was generally understood that the iniquity exception did not extend to journalistic material. This issue arose during the Leveson Inquiry into the culture, practices and ethics of the British press ("the Leveson Inquiry"). According to the submission on behalf of the Metropolitan Police Service ("MPS") to the Leveson Inquiry:

> One problem for the MPS has been that it is not clear whether journalistic material continues to fall within the scope of the excluded material definition, and thus remain subject to the second set of access conditions, if the journalist has created or acquired it in furtherance of a crime. The question that arises is as follows: if there was iniquity such as crime or fraud did the duty of confidence ever arise? If not, then the journalistic material will not be held under an undertaking, restriction or obligation of confidence as required by s 11(3) of PACE.[26]

10.17 In response, Leveson LJ wrote in the Leveson Inquiry report:

> It is certainly remarkable that Parliament might have provided greater protection for journalistic material than in relation to legal professional privilege as a matter of general law. Even more so that it would provide less protection for the material where the public interest is served in relation to a terrorist investigation than might be the case if that material has been created or acquired in furtherance of crime. Although the circumstances in which the provision might bite will hopefully be very rare, I see force in the submission that s11(3) PACE should be amended by providing that journalistic material is only held in confidence for the PACE provisions if it is held, or has continuously been held since it was first acquired or created, subject to an enforceable or lawful undertaking, restriction or obligation.
>
> I am very conscious that I have received submissions only from the MPS on this topic and that there is potential room for argument that any amendment to PACE will have far wider ramifications of which I have not been apprised and go beyond the limited goals that DC Mackey seeks to achieve. Before any conclusion can be reached on any of these issues, appropriate consultation will be essential.
>
> In the circumstances, without pre-judging any conclusion, I recommend that the Home Office should consider and, if necessary, consult upon … whether s 11(3) of PACE should be amended by providing that journalistic material is only held in confidence for the PACE

---

24 For example, Terrorism Act 2000, sch 5, para 4.

25 *Hansard* (HC), 3 May 1983, vol 42, col 120.

26 The Leveson Inquiry, "Submission for module 4 on behalf of the Metropolitan Police Service" (10 July 2012), para 3.1.

provisions if it is held or has continuously been held since it was first acquired or created subject to an enforceable or lawful undertaking, restriction or obligation.[27]

10.18 The effect of this amendment would be for iniquitous confidential journalistic material (excluded material) to be downgraded to non-confidential journalistic material (special procedure material). This is because journalistic material would only lose its confidential status rather than no longer satisfy the definition of non-confidential journalistic material under section 13 of PACE, which makes it qualify as special procedure material.

10.19 On 20 November 2016, the judgment in *R v Norman* was handed down.[28] This case concerned an appeal by a prison officer following his conviction for an offence of misconduct in public office. Norman was paid more than £10,000 by a tabloid journalist over a period of some five years in return for information about the prison in which he worked. The information formed the subject matter of numerous articles published by the two newspapers for which the journalist worked.

10.20 Norman's prosecution was founded on evidence including confidential journalistic material. Mirror Group Newspapers had voluntarily provided to the MPS details of payments which had been made to Norman which reflected his confidential provision of information to their journalists. Norman appealed on the basis, amongst others, that the trial judge should have acceded to an application to stay proceedings as an abuse of process because his right to freedom of expression was protected by PACE, which did not permit access to excluded material, and the MPS had circumvented this by receiving protected material voluntarily provided.

10.21 The Court held that there were three reasons to reject this ground of appeal. The second reason was expressed in the judgment of the whole court, including the then Lord Chief Justice, Lord Thomas, as follows:

> The material so sought would not have amounted to "excluded material" because it would not have been impressed with the necessary quality of confidentiality to bring it within section 11. It is well established in the context of legal professional privilege that a communication made in furtherance of a crime prevents the privilege from arising by reason of what is commonly called the iniquity exception. Iniquity for these purposes includes the commission of a crime, although it is not so limited and extends to fraud or equivalent underhand conduct which is in breach of a duty of good faith or contrary to public policy or the interests of justice. The reason such iniquity prevents the existence of legal privilege in the relevant communication is that it precludes the existence of confidentiality in the communication; and confidentiality is a necessary condition for legal privilege. These principles are well established by a long line of cases from *R v Cox & Railton* (1884) 14 QBD 153, which were considered and analysed in *JSC BTA Bank v Ablyazov* [2014] EWHC 2788 (Comm), [2014] 2 CLC 263 at paragraphs [68] to [93]. The appellant's communications with Mr Moyes were in furtherance of his criminal conduct and so attracted no confidentiality. They are not therefore excluded material for the purposes of a PACE production order. The position might be otherwise for a genuine whistleblower

---

27 The Leveson Inquiry, vol 4, paras 9.10 to 9.11. Emphasis in original.

28 *R v Norman* [2016] EWCA Crim 1564, [2017] 4 WLR 16.

acting in the public interest whose conduct vis a vis the journalist would retain its express or implied undertaking of confidentiality.[29]

10.22 By way of initial observation, we note that the phrase "underhand conduct" is vague and seemingly very broad. The phrase was used by Popplewell J in *JSC BTA Bank v Ablyazov*:

> The [crime-fraud exception] is not confined to criminal purposes, but extends to fraud or other equivalent underhand conduct which is in breach of a duty of good faith or contrary to public policy or the interests of justice.[30]

10.23 Use of the word "underhand" in the present context originates from the following passage of Kekewich J in *Williams v Quebrada*:

> It is of the highest importance, in the first place, that the rule as to privilege of protection from production to an opponent of those communications which pass between a litigant, or an expectant or possible litigant, and his solicitor should not be in any way departed from. However hardly the rule may operate in some cases, long experience has shewn that it is essential to the due administration of justice that the privilege should be upheld. On the other hand, where there is anything of an underhand nature or approaching to fraud, especially in commercial matters, where there should be the veriest good faith, the whole transaction should be ripped up and disclosed in all its nakedness to the light of the Court.[31]

10.24 It seems to us that the phrase "underhand conduct" has been used in a purposefully broad manner so as to capture any form of conduct which might be (1) in breach of a duty of good faith; (2) contrary to public policy; or (3) contrary to the interests of justice.

10.25 Additionally, given that iniquity precludes confidentiality, this suggests that confidential journalistic material is only downgraded to journalistic material, as confidentiality is not a necessary condition for journalistic material. In PACE terms, the excluded material would become special procedure material.

10.26 Statutory amendment has resolved this issue in other settings. The Investigatory Powers Act 2016 ("IPA") and the Crime (Overseas Production Orders) Act 2019 ("COPOA") both contain iniquity exceptions.[32] Synthesising the very similar statutory language, the provisions provide:

(1) Material/electronic data is not to be regarded as (having been) created or acquired for the purposes of journalism if it is (or was) created or acquired with the intention of furthering a criminal purpose, and

---

29 *R v Norman* [2016] EWCA Crim 1564, [2017] 4 WLR 16 at [39].

30 *JSC BTA Bank v Ablyazov* [2014] EWHC 2788 (Comm), [2014] 2 CLC 263 at [68].

31 *Williams v Quebrada* [1895] 2 Ch 751, 754 to 755.

32 Unlike previous Acts, the Crime (Overseas Production Orders) Act dispenses with the distinction between confidential and non-confidential journalistic material. The distinction would be unnecessary as the Act exempts all journalistic material from the scope of an Overseas Production Order.

(2) Material/electronic data which a person intends to be used to further such a purpose is not to be regarded as intended to be used for the purposes of journalism.[33]

10.27 These particular statutory exceptions preclude material from being for the purposes of journalism. It follows that iniquitous confidential journalistic material would not simply lose its confidentiality, and so be downgraded to journalistic material, but rather lose its status as journalistic material altogether.

10.28 Removing all protections afforded to confidential journalistic material appears compatible with the European Convention on Human Rights. One of the challenges to the IPA bulk warrants regime in the recent case of *Liberty v Home Office*[34] was that the exclusion of certain material from "journalistic material" because it was "created … with the intention of furthering a criminal purpose" in section 264(5) of IPA goes too far in excluding material which ought to be protected. The Divisional Court observed that the Claimant:

> did not cite any Strasbourg authority which suggests that this inclusion is problematic, nor do we think that the inclusion creates any difficulty with the compatibility of the definition taken as a whole with the Convention rights.[35]

10.29 Unlike confidential journalistic material, confidential personal records have not been subject to discussion in case law nor have statutory exceptions been made. However, the passage of *Norman* discussed above suggests that the iniquity exception precludes confidentiality in any setting.

Special procedure material

10.30 Special procedure material comprises confidential business records and (non-confidential) journalistic material. We consider *Norman* as confirming that the common law iniquity exception precludes confidentiality in any setting.[36]

10.31 The iniquity exception is often described by the phrase that there is no confidence in iniquity. If this is right, this would mean that whether special procedure material loses its protection depends on whether confidentiality is a necessary condition of its definition. In the case of confidential business records, the material would no longer constitute special procedure material as confidentiality is a necessary condition. On the other hand, confidentiality is not a necessary condition of journalistic material.

10.32 While the common law iniquity exception precludes confidentiality, the statutory iniquity exceptions to journalistic material set out at paragraph 10.26 above preclude material being for the purposes of journalism and therefore remove its protection entirely.

---

33 Investigatory Powers Act 2016, s 264(5); Crime (Overseas Production Orders) Act 2019, s 12(6).

34 *Liberty v Home Office* [2019] EWHC 2057 (Admin), [2020] 1 WLR 243.

35 *Liberty v Home Office* [2019] EWHC 2057 (Admin), [2020] 1 WLR 243 at [352].

36 See also *Fitzgerald v Preston Crown Court* [2018] EWHC 804 (Admin) at [69], in which one of the challenges made to a search warrant was that there was no jurisdiction to issue a warrant under the Police and Criminal Evidence Act 1984, sch 1 for special procedure material as the investigator was not seeking confidential business records but iniquitous material over which there could be neither confidentiality nor privilege.

Conclusion

10.33 From the current law discussed above, three formulations of the iniquity exception can be identified:

(1) a broad common law test, applying to any confidential material, whereby confidentiality is precluded by iniquity;[37]

(2) a statutory test under PACE in relation to legally privileged material which provides that "items held with the intention of furthering a criminal purpose are not items subject to legal privilege";[38] and

(3) a statutory test under IPA and COPOA in relation to journalistic material which is "created or acquired with the intention of furthering a criminal purpose" and which precludes such material from being for the purposes of journalism.[39]

CONSULTATION RESPONSES

10.34 Six consultees[40] provided comments on the operation of an iniquity exception generally. A further nine consultees[41] responded to our consultation question asking whether greater clarity needs to be introduced in defining searches for special procedure material held with the intention of furthering a criminal purpose.

Legally privileged material

10.35 In relation to legally privileged material, the Bar Council and the Criminal Bar Association observed that, while the definition in section 10(2) of PACE is well-known and generally causes little problem in practice, it does give rise to the question, by whom is material held in furtherance of a criminal purpose? For example, should a client's privilege be lost if a lawyer is holding legally privileged material which he intends to use as part of a fraudulent claim under a representation order?

10.36 They invited consideration of whether we should develop the principle of limited waiver which applies in cases of investigations into a lawyer's conduct by a professional disciplinary body. Addressing that matter here, we do not consider that a project on search warrants is the appropriate forum to address broader questions of the scope of legally privileged material.

Excluded material

10.37 A number of consultees provided observations regarding whether confidential journalistic material loses its protection if held with the intention of furthering a criminal purpose.

---

37 *R v Norman* [2016] EWCA Crim 1564, [2017] 4 WLR 16 at [39].

38 Police and Criminal Evidence Act 1984, s 10(2).

39 Investigatory Powers Act 2016, s 264(5); Crime (Overseas Production Orders) Act 2019, s 12(6).

40 Crown Prosecution Service; Guardian News and Media; Financial Conduct Authority; Dijen Basu QC; Bar Council & Criminal Bar Association; Law Society.

41 HM Council of District Judges (Magistrates' Courts); Council of Her Majesty's Circuit Judges; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Northumbria Law School Centre for Evidence and Criminal Justice Studies; Dijen Basu QC; Bar Council & Criminal Bar Association; Metropolitan Police Service; Financial Conduct Authority; HM Revenue and Customs.

10.38 The Crown Prosecution Service ("CPS") observed at the outset that this question merits discussion as it will have a practical impact on investigations and prosecutions. It accepted that, prior to 2016, it was not clear whether journalistic material which is held in confidence with the intention of furthering a criminal purpose remained excluded material. The CPS considered, however, that following the Court of Appeal decision in *Norman*, the law does not protect iniquitous journalistic material held in confidence.

10.39 The CPS agreed with our interpretation in the consultation paper of paragraph 39 in *Norman*,[42] suggesting that the case should be taken to represent the current legal position. This is because it contains an unequivocal conclusion reached on this question by the former Lord Chief Justice in a recent appeal on this precise point, without any authority to the contrary. At the same time, the CPS understood *Norman* to be saying that it is the quality of confidentiality which is lost and not the categorisation of journalistic material.

10.40 In light of the above, the CPS suggested that in the same way that section 10(2) removes legal privilege from items "held with the intention of furthering a criminal purpose", section 13 of PACE which defines journalistic material should be amended to provide that "journalistic material held with the intention of furthering a criminal purpose is not journalistic material". However, this would go further than *Norman*. The CPS suggestion would have the effect not only of precluding confidentiality, which would downgrade confidential journalistic material to journalistic material, but losing its protection as journalistic material entirely.

10.41 The CPS presented five arguments in favour of statutory amendment to PACE along the lines set out above. First, it was argued that the lack of an iniquity exception would imply that journalists in this respect are entitled to operate beyond the law. Secondly, it was said that such a statutory amendment would involve codifying a complicated paragraph in a Court of Appeal judgment in one sentence.[43] Thirdly, it would confirm and simplify the existing law.

10.42 The fourth argument put forward by the CPS for amending PACE was that it would remove from PACE warrants wider and less well-defined concepts such as "quality of confidentiality" and "iniquity" (going beyond the commission of crime). Fifthly, statutory amendment would remove the need for those considering this exception to consider the wider body of common law on "no confidence in iniquity", which sometimes becomes blurred with "no confidence in the disclosure of iniquity" which would have a different implication for the protection of journalistic material.

10.43 The Guardian News and Media ("GNM") understood the definition of iniquitous material to be "communications in furtherance of a crime".[44] They accepted that this definition extends to fraud or equivalent underhand conduct, which is in breach of a duty of good faith or contrary to public policy or the interests of justice.[45]

10.44 The GNM submitted that the term "furtherance of crime" is nebulous and capable of unfairly capturing legitimate journalistic material used to fuel public debate. The GNM was concerned that, without legislative parameters, the iniquity exception is capable of

---

42 See para 10.21 above.

43 As we note at paragraph 10.40 above, however, this statutory amendment would go further than codifying the decision in *Norman*.

44 *SC BTA Bank v Ablyazov (No 13)* [2014] EWHC 2788.

45 *R v Norman* [2016] EWCA Crim 1564, [2017] 4 WLR 16 at [39].

undermining the confidentiality that is inherent in journalistic material provided by a whistleblower.

10.45 We were referred to the comments made by the Court of Appeal in *Norman* that:

> The position [that no privilege attaches to communications in furtherance of criminal conduct] might be otherwise for a genuine whistleblower acting in the public interest whose conduct vis a vis the journalist would retain its express or implied undertaking of confidentiality.[46]

10.46 In this regard it should be noted that the CPS did not consider *Norman* as imputing a public interest test into the question of whether confidentiality is precluded. Instead, they interpreted the above observation as meaning that a genuine whistleblower acting in the public interest would not be committing misconduct in public office.

10.47 The GNM also raised the case of Amelia Hill, a reporter for The Guardian who was suspected of committing an offence of aiding and abetting misconduct in public office when she received confidential information about a phone-hacking case from a police officer. In determining that prosecution would not be in the public interest, the CPS observed that the information was "although confidential, not highly sensitive". The CPS also noted that no payment was sought or received by the police officer, the disclosure did not expose anyone to a risk of injury or death, nor did it compromise the investigation. Finally, the CPS admitted the information would probably have made it into the public domain by some other means. In addition, the CPS weighed the public interest in disclosure against the criminality alleged, in this case a breach of the Data Protection Act 1998.[47]

10.48 The News Media Association ("NMA") strongly objected to any exception relating to "intention of furthering a criminal purpose" in respect of any provision relating to the protection of journalistic activities, sources or materials. It argued that such an exception would be open to abuse and exploitation, allowing easy bypass of journalistic protections and fatally undermining freedom of expression safeguards.

10.49 The NMA pointed out that there are numerous and wide-ranging criminal offences which might potentially impact upon journalistic investigations, newsgathering, reporting and publication, rendering the media organisations, journalists or their sources vulnerable to unfounded allegations of wrongdoing or conspiracy to commit, incite, aid or abet any such wrongdoing by others. These include criminal offences relating to data protection, protection of official data including misconduct in public office, official secrets and other unauthorised disclosure offences, terrorism, public order, trespass, harassment or court reporting.

10.50 The NMA observed that media organisations, journalists and their sources are particularly vulnerable to unwarranted or unscrupulous accusations of data protection or unauthorised disclosure offences. This vulnerability would be exacerbated by implementation of the Law Commission's consultative proposals on the law protecting official data,[48] which have been

---

46 *R v Norman* [2016] EWCA Crim 1564, [2017] 4 WLR 16 at [39].

47 We note that this case concerns whether prosecution is in the public interest rather than whether the confidentiality of the journalistic material itself is precluded.

48 Protection of Official Data: A Consultation Paper (2017), Law Commission CP No 320.

strongly opposed by the NMA, its members and other media, freedom of information and freedom of expression organisations.[49]

10.51 The NMA argued that any "iniquity exception" to the exemption of special procedure and excluded material from general search warrant or other access powers would be all too easily exploited and abused by those who wish to seize material, discover sources, disrupt investigation, or delay or prevent publication. In addition, the continued failure by police and courts to ensure rigorous compliance with the law's requirements could lead to "rubber stamping" of "iniquity exception" applications.

10.52 The NMA concluded that an iniquity exception would fatally undermine any attempted improvement of journalistic protections and threaten press freedom instead of safeguarding it. In the NMA's view, all "iniquity exceptions" to journalistic protections should be excised from all legislation wherever included (including recent legislation such as the IPA), and no iniquity exception to journalistic protections should be introduced or extended in any form into any other legislation, existing or new.

10.53 The Financial Conduct Authority ("FCA") considered that there ought to be an iniquity exception in respect of confidential journalistic material. Financial investigations, particularly market abuse, can give rise to instances where what might be loosely defined as journalistic material is sought. The FCA were concerned that the broad definition of journalistic material in PACE ("material acquired or created for the purposes of journalism") is open to exploitation in FCA cases. In particular, it identified two scenarios which demonstrate their concerns.

(1) Suspects may directly publish misleading or false statements designed to "abuse markets"[50] whilst describing themselves as "financial bloggers" (journalists) to provide cover for their actions.

(2) Suspects may act as sources to journalists by providing false or illegitimately acquired confidential market information for the purposes of publication. Although the intention of the source is to abuse the market, the journalist may legitimately hold and publish the information.

10.54 The FCA envisaged difficulties in applying an iniquity exception which mirrors the formulation in section 10(2) of PACE ("held with the intention of furthering a criminal purpose") to the "dishonest source" scenario described in paragraph (2) above. The FCA therefore prefers the broader iniquity exception of "underhand conduct" in *Norman*.

Special procedure material

10.55 As for iniquitous special procedure material, all consultees who responded to our specific consultation question on special procedure material agreed in principle with providing greater clarity in defining searches for special procedure material held with the intention of

---

[49] We have now published our final report in which we recommend that public interest defences be created for public servants and civilians, including journalists, that they can rely upon in court if prosecuted for an offence under the Official Secrets Act 1989. See Protection of Official Data: Report (2020), Law Com No 395 (available at https://www.lawcom.gov.uk/project/protection-of-official-data/).

[50] Certain types of behaviour, such as insider dealing and market manipulation, can amount to market abuse. See https://www.fca.org.uk/markets/market-abuse.

furthering a criminal purpose.[51] HM Revenue and Customs stated that it would assist to put beyond doubt that no confidence attracts to iniquity and thus the crime-fraud exception means that material generated in the course of the commission of a crime cannot be special procedure material. The Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate stated that further clarity would be welcome around material such as invoices which could contain evidence of criminality. The MPS considered that, although they already have established processes for managing such material, any support or guidance that makes for greater clarity for officers is to be encouraged.

10.56 In respect of journalistic material, as mentioned above, the CPS understood *Norman* to be saying that it is the quality of confidentiality which is lost and not thereby its categorisation as journalistic material. It nonetheless considered there to be an argument that non-confidential journalistic material tainted by iniquity *should* lose its status as journalistic material. The CPS contrasted non-confidential journalistic material with the position of legally privileged material as the effect of section 10(2) of PACE is that the status of legal privilege is lost in its entirety and the material is available under ordinary warrant.

10.57 The CPS could see an (untested) argument that material in pursuance of criminality is simply not journalistic material. It considered this a further reason why formalising in PACE how an application for material under the "furtherance of criminality" exception is to be made is desirable.

10.58 The National Crime Agency approached the matter on the basis that special procedure material does not stop being special procedure material because it is in furtherance of criminality. The City of London Economic Crime Academy recommended that consideration be given to removing the special status of the material if it is being used to further a criminal purpose, indicating that it did not consider that an iniquity exception exists under the current law.

10.59 Dijen Basu QC was not completely convinced by the argument that documents held for a criminal purpose could not be special procedure material because of the *Norman* iniquity rule. He stated that it is arguable that the holder still holds the material subject to an express or implied *undertaking* to hold it in confidence, albeit an iniquitous one which would not be enforceable at law. For this reason, Dijen Basu QC considered that there should be a criminal purpose exception to the definition of special procedure to make the position clear. The Financial Conduct Authority also would welcome the introduction of an iniquity exception in relation to all excluded and special procedure material.

10.60 Some consultees discussed the procedures that should be put in place to deal with iniquitous material. The Law Society considered that the burden to show reasonable cause to believe that any otherwise protected material was created to further an unlawful purpose must remain with the applicant and be heard by a senior judge, and any such material must be specifically identified. They considered that civil search order procedures may be helpful in such situations.

10.61 The Northumbria Law School Centre for Evidence and Criminal Justice Studies stated that difficulties with the operation of the iniquity exception where special procedure material is

[51] HM Council of District Judges (Magistrates' Courts); Council of Her Majesty's Circuit Judges; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Northumbria Law School Centre for Evidence and Criminal Justice Studies; Dijen Basu QC; Bar Council & Criminal Bar Association; Metropolitan Police Service; Financial Conduct Authority; HM Revenue and Customs.

involved could be dealt with through the use of a neutral independent lawyer. Such a lawyer could be appointed to review the material where the investigating body alleges that the special procedure material that is the subject of the warrant is held with the intention of furthering a criminal purpose.

ANALYSIS

10.62 We regard it as unsatisfactory that there is neither a clear nor coherent approach to the principle of iniquity under the current law. In particular, our own research and the comments made by consultees indicate a lack of clarity and coherence around the categories of material vulnerable to iniquity, the test to be applied and the effect on the material (whether loss of protection or downgrading the level of protection).[52] What is more, this lack of clarity creates confusion and other problems in practice. For this reason, we recommend at paragraph 10.71 below that the Government considers whether the law relating to iniquitous material in the context of criminal investigations ought to be reformed. In this section, we provide views on the matters which should be taken into account should such reform be considered desirable.

A statutory iniquity exception

10.63 One option for reform would be to place an iniquity exception, insofar as it relates to material other than legally privileged material, on a statutory footing. We agree with the GNM that the application of the iniquity exception to journalistic material would benefit from legislative parameters. The current ambiguity arising out of *Norman* and previous case law creates a stronger justification for statutory amendment. This also gives rise to the question of whether a statutory iniquity exception should be inserted into other statutory regimes beyond PACE.

10.64 The NMA has argued that there should be no iniquity exception in relation to journalistic material and all current statutory exceptions should be repealed insofar as they relate to journalistic material.

The wording of the test

10.65 We regard the FCA as right to point out that the way in which an iniquity test is worded will have significant implications for the conduct which causes material to be held for an iniquitous purpose.

The effect of iniquity

10.66 As discussed at paragraph 10.27 above, the statutory iniquity exceptions in IPA and COPOA preclude iniquitous journalistic material from being classified as journalistic material. The common law iniquity exception expressed in *Norman*, however, only precludes journalistic material from being confidential.

10.67 As discussed at paragraph 10.17 above, Leveson LJ, in the Leveson Inquiry report, recommended that the Home Office consider and, if necessary, consult upon whether section 11(3) of PACE should be amended to preclude the confidentiality of iniquitous

---

[52] Nick Barnard, Senior Associate at Corker Binning, has recently written that the crime-fraud exception may be underutilised or misunderstood. See Nick Barnard, "Crime, fraud and iniquity – how can an allegation of wrongdoing override Legal Professional Privilege?" Corker Binning Blog (5 July 2020) (available at https://www.corkerbinning.com/crime-fraud-iniquity-wrongdoing-legal-professional-privilege/#_ftn3)

journalistic material. The CPS has argued in response to this consultation paper that section 13 of PACE should be amended to preclude iniquitous journalistic material from being classified as journalistic material.

Procedure

10.68 Reform may also address the procedure when seeking access to iniquitous material. If iniquity destroys or precludes confidentiality, then excluded material would be downgraded to special procedure material such that an application would have to be made to a Crown Court judge under schedule 1 to PACE. Were iniquity to preclude material from being for a particular purpose then an ordinary warrant under section 8 of PACE could be sought.

10.69 The CPS considered that the protections of schedule 1 of PACE seem in principle to be appropriate for a claim by an investigator that an otherwise protected category of material is sought because it is held in furtherance of criminality. In the Leveson Inquiry report, Leveson LJ also stated that it is arguable that article 10 of the European Convention on Human Rights and section 10 of the Contempt of Court Act 1981 require a balancing exercise in any case involving the press even if the material is neither journalistic nor excluded within the PACE definitions.[53]

10.70 Should reform be pursued, detailed consultation on each of these matters and their ramifications beyond search warrants will be essential.

Recommendation 40

10.71 We recommend that the Government considers whether the law relating to iniquitous material in the context of criminal investigations ought to be reformed.

[53] The Leveson Inquiry, vol 4, para 9.10. See *R (Malik) v Manchester Crown Court* [2008] EWHC 1362 (Admin), [2008] 4 All ER 403 at [48] per Dyson LJ.

Chapter 11: The treatment of legally privileged material

INTRODUCTION

11.1 In this chapter we consider reform to the way in which legally privileged material is treated. We do not propose altering the protection which is currently afforded to legally privileged material. Instead, we consider changes to how legally privileged material is sifted and how disputes regarding its treatment are resolved.

11.2 This chapter will examine two issues. First, it will examine the case for introducing a formal procedure by which independent counsel are instructed to assist in identifying legally privileged material and separating it from other material. In summary, to retain flexibility, we recommend that the procedure for instructing independent lawyers or other experts to resolve issues associated with legal privilege be set out in a new Code of Practice. We recommend a Code of Practice governing the acquisition and treatment of electronic material later in this report – Recommendation 63 at paragraph **Error! Reference source not found.** below – which we regard to be a suitable place for the procedure to be set out.

11.3 Secondly, this chapter examines whether it would be desirable to introduce a new procedure requiring a person who claims that material sought under a warrant contains legally privileged material to assist in identifying that material, so that it can be segregated, returned and deleted more quickly. We do not recommend such a procedure in this chapter. This is because we consider that Recommendation 61 at paragraph 17.133 addresses the specific concerns that the procedure discussed in this chapter was designed to address. Those concerns are occupiers not cooperating with investigators conducting searches and the time and resources required to sift material after seizing it.

11.4 In short, we recommend at Recommendation 61 that a person with an interest in electronic material be able to apply to the Crown Court for a judge to decide how the investigator should treat electronic material, for example how legally privileged material should be sifted. This procedure would also enable a law enforcement agency to seek judicial approval of a protocol which details how they propose to sift material and resolve disputes between the parties.

FORMALISING INDEPENDENT COUNSEL PROCEDURE

The current law

11.5 A search warrant cannot be issued under the Police and Criminal Evidence Act 1984 ("PACE") or any other provision to search for material which consists of or includes items subject to legal privilege.[1] Additionally, legally privileged material cannot be seized under warrant or search powers under sections 18, 19, 20 and 32 of PACE,[2] or obtained by a production order under schedule 1 to PACE.

11.6 The only way for legally privileged material to be lawfully seized is for an investigator who is already on the premises to use the "seize and sift" powers contained in sections 50 and 51

---

1 Police and Criminal Evidence Act 1984, ss 8(1)(d), 9(2) and sch 1.

2 Police and Criminal Evidence Act 1984, s 19(6).

of the Criminal Justice and Police Act 2001 ("CJPA"). However, these powers are only designed to allow for material to be sorted through at a later stage because it is not reasonably practicable, during the search, to determine which category the material falls into or to separate the material into what may and may not be seized.

11.7 Investigators routinely instruct independent lawyers (often referred to as "independent counsel") to advise them in relation to material which may be legally privileged.[3] Independent lawyers may be instructed to assist an investigating agency at the time of the execution of a warrant, but they are more commonly instructed to assist when seized material is subsequently sifted off-site under section 50 of the CJPA.

11.8 Although instructing independent counsel has been looked upon favourably by the courts,[4] there is no authority for it in statute. Guidance as to independent counsel's role and remit has been issued by the Bar Council.[5] The Attorney General's Supplementary Guidelines on Digitally Stored Material from 2011 also provide guidance, stating that where material that has been seized is identified as potentially containing legally privileged material, it must be inspected by lawyers independent of the investigating and prosecuting authorities.[6]

The consultation paper

11.9 Several stakeholders argued that the practice of instructing independent counsel ought to be put on a legislative footing. We considered that there was a strong argument for codifying the rules governing independent counsel in the search warrants context, rather than having the boundaries of what independent counsel can and cannot do drawn out by judicial review challenges. It is noteworthy that, for civil search orders, the use of supervising solicitors is governed by the Civil Procedure Rules, Practice Direction 25A.

11.10 Another question that we raised concerned the substance of any proposed legislative framework, including whether the use of independent counsel ever ought to be mandatory and if so when. We recognised that practice varies amongst investigative agencies and a lot will depend on the facts of each case. Any legislative framework would therefore need to be adaptable to the various ways in which independent counsel may be instructed.

11.11 Accordingly, we provisionally proposed[7] that the procedure for instructing independent counsel or other experts to resolve issues of legal privilege ought to be set out in secondary legislation. We asked if consultees agreed and, if so, we welcomed consultees' views on

---

3 Bar Council, *Barristers instructed as "Independent Counsel" to advise upon legal professional privilege in relation to seized material* (November 2019), https://www.barcouncilethics.co.uk/wp-content/uploads/2017/10/LPP-Independent-Counsel-in-relation-to-seized-material.pdf.

4 *R v Middlesex Guildhall Crown Court ex parte Tamosius & Partners* [2000] 1 WLR 453, *R (Rawlinson & Hunter Trustees & Others) v Central Criminal Court, the Director of the Serious Fraud Office* [2012] EWHC 2254 (Admin), [2013] 1 WLR 1634 and *R (McKenzie) v Director of the Serious Fraud Office* [2016] EWHC 102 (Admin), [2016] 1 WLR 1308.

5 Bar Council, *Barristers instructed as "Independent Counsel" to advise upon legal professional privilege in relation to seized material* (November 2019), https://www.barcouncilethics.co.uk/wp-content/uploads/2017/10/LPP-Independent-Counsel-in-relation-to-seized-material.pdf.

6 *Attorney General's Guidelines on Disclosure: Supplementary Guidelines on Digitally Stored Material* (2011), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/16239/Attorney_General_s_guidelines_on_disclosure_2011.pdf.

7 Consultation Question 42.

what the content of those rules should be, including whether the use of independent counsel ought to be mandatory either:

(1) when a claim to legal privilege is made; or

(2) when no claim to legal privilege is made but there are other reasons for believing that legally privileged material may be present at the premises or form part of the material that has been seized.

Consultation responses

11.12 Twenty-two consultees answered this question. On the question of whether, in principle, the procedure for instructing independent lawyers ought to be formalised: 13 agreed;[8] six disagreed;[9] and three expressed other views.[10]

11.13 The majority of consultees agreed with formalising the procedure for instructing independent counsel. The main justification put forward was the need for consistency. HM Council of District Judges (Magistrates' Courts) observed that, in an increasingly digital world, it is likely that material subject to legal privilege will be seized more and more frequently. Consequently, it agreed that formalising the procedure through secondary legislation would be desirable, because it would lead to a clearer and more consistent approach.

11.14 The Law Society considered that the procedures should be set out in legislation in order to achieve consistency of approach, but that legislation ought to be supplemented by guidance. The Northumbria Law School Centre for Evidence and Criminal Justice Studies considered that it would be desirable to have a standardised process for instructing independent counsel embedded in secondary legislation.

11.15 The Bar Council and the Criminal Bar Association ("CBA") agreed with the proposal for secondary legislation and considered that consistency is necessary. It was observed that the practice of instructing independent counsel has been approved by the courts and guidance has been issued by the Bar Council and the Attorney General. Therefore, it was said to make sense for the procedure to be set out in secondary legislation or the Criminal Procedure Rules ("CrimPR"). It was argued that, however the procedure is set out, there should be a period of consultation on its contents, particularly with the legal profession. It was also suggested that if the decision is taken to set out the procedure in secondary legislation, this ought to be subject to the affirmative procedure.

11.16 Other consultees disagreed with formalising the independent counsel requirement. The Crown Prosecution Service ("CPS") was unsure that there could be a "one-size-fits-all" approach to instructing independent counsel. For example, investigators must take different approaches to claims of privilege they consider to be wholly unmeritorious and claims which

---

8 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Guardian News and Media; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; The Law Society; Justices' Clerks' Society; Magistrates Association; Bar Council and the Criminal Bar Association.

9 Crown Prosecution Service; Insolvency Service; Dijen Basu QC; National Crime Agency; Competition and Markets Authority; Financial Conduct Authority.

10 Northumbria Law School Centre for Evidence and Criminal Justice Studies; Metropolitan Police Service; Serious Fraud Office.

are simply vague. The Insolvency Service also considered that the current common law approach offered the necessary flexibility to allow investigators to decide whether to instruct independent counsel on a case by case basis.

11.17 A similar position was adopted by the National Crime Agency ("NCA"), who argued that there was no need for secondary legislation. In their view, the "well established practices amongst law enforcement agencies" are sufficient, and it is important that processes remain flexible. The Serious Fraud Office ("SFO") was not aware of any pressing issues relating to the use of independent counsel and doubted whether formalising the procedure through legislation was necessary. The SFO also highlighted the need for flexibility.

11.18 The Financial Conduct Authority ("FCA") stated that the law is already clear and, in their view, offers robust protection to the rights of suspects and third parties. It felt that mandating further rules relating to the instruction of independent counsel would unnecessarily restrict the discretion law enforcement agencies have over how best to comply with their obligations, and this would be likely to result in delays. In its view, this is an area that can only sensibly be handled on a case by case basis.

11.19 Dijen Basu QC did not agree with introducing a statutory obligation to instruct independent counsel whenever a claim to privilege is made. He felt that it may encourage experienced suspects to raise privilege as a matter of routine, even if there was little likelihood of there being any privileged material in the bulk of material seized. A similar concern was raised by the Metropolitan Police Service ("MPS"), namely that a mandatory requirement for independent counsel will be open to misuse by the defence.

11.20 The Competition and Markets Authority ("CMA") argued that requiring independent counsel to be present during the search in particular circumstances would not be cost efficient. There may be no dispute between the investigator and the occupier and, even where there is a dispute, it could likely be resolved without independent counsel being present during the search itself.

11.21 The Northumbria Law School Centre for Evidence and Criminal Justice Studies observed that requiring investigators to instruct independent counsel whenever an occupier claims that some of the material seized is legally privileged may disadvantage occupiers with less legal knowledge who are unaware that they can make such a claim.

11.22 There were also differing views on what the precise rules should be surrounding instructing independent counsel. Some consultees considered that instructing independent counsel should be mandatory whenever a claim to privilege is made or there are reasons for believing that legally privileged material may be present at the premises or form part of the material that has been seized.[11]

11.23 One consultee considered that an occupier making a claim to legal privilege should be required to specify which material may be subject to legal privilege, before a lawyer is required to be instructed.[12] The Law Society considered that instructing independent counsel

---

[11] Professor Richard Stone; The Senior District Judge (Chief Magistrate); Southern Derbyshire Magistrates' Bench; Council of Her Majesty's Circuit Judges; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Guardian News and Media.

[12] HM Council of District Judges (Magistrates' Court).

ought to be discretionary when no claim is made but there is reason for believing that legally privileged material may be present.

11.24 Another consultee suggested that any rules ought to allow for both investigators and those who allege privilege to provide written submissions to independent counsel, who should be obliged to take account of them.[13]

11.25 The Magistrates Association accepted that in the two scenarios on which we consulted (at paragraph 11.11 above), independent counsel should be instructed. At the same time, it argued that the point at which independent counsel should be instructed must be flexible. It concluded that the rules could helpfully provide clarity as to what steps an investigator should take and when.

Analysis

11.26 We agree with consultees that it is impracticable to devise a rigid one-size-fits-all approach to instructing independent counsel. It is important that flexibility is retained so that investigators can adopt the procedure that is most suited to their investigation. Each law enforcement agency will have its own procedures. In some types of investigation independent counsel will be instructed to perform an on-site review of material, while in others they will be best suited to conducting post-search reviews.

11.27 Nonetheless, we consider that some generally applicable principles can be distilled. These should assist investigators in devising a plan for instructing independent counsel which is tailored to the case before them. On one view, the guidance document issued by the Bar Council already does this. The purpose of that document, however, is to guide barristers instructed as independent counsel to advise on legal professional privilege in relation to seized material. The document is not aimed at investigators who are devising a plan for instructing independent counsel.

11.28 On balance, we consider that guidance on instructing independent counsel should be contained in the new Code of Practice governing investigations involving electronic material, which we recommend at Recommendation 63.[14] At the time of writing the consultation paper, we had secondary legislation in mind for this matter; we did not consider a Code of Practice as a possible method to formalise the independent counsel procedure. However, we now consider that a Code of Practice is more appropriate than secondary legislation because it offers greater flexibility, ease of updating and lends itself to a more detailed narrative.

11.29 A Code of Practice would improve the procedure for instructing independent counsel in a number of ways. First, it could bring a number of principles in existing guidance documents into one place. This could include relevant aspects of the Bar Council guidance. Secondly, it would provide an opportunity to incorporate internal guidance and best practice from various law enforcement agencies. Thirdly, it could create a procedure for instructing independent counsel which is both more detailed and flexible.

11.30 Fourthly, a Code of Practice would provide enforceable standards of conduct. Finally, from a human rights perspective, a Code of Practice would also provide clearer rules governing the

---

13 Birmingham Law Society.

14 See paragraph **Error! Reference source not found.** below.

treatment of legally privileged material, ensure that action taken is proportionate and that there is adequate guidance governing the process of instructing independent counsel.

11.31 We write at paragraph 17.147 below that a new Code of Practice would require further consideration and consultation. The Bar Council and the CBA considered that, however the procedure for instructing independent counsel is set out, there should be a requirement that it be subject to consultation, particularly with the legal profession. We agree and consider this to be another reason for formalising the procedure for instructing independent counsel in a Code of Practice.

11.32 One final matter remains. The Code of Practice which we recommend at Recommendation 63 concerns electronic material. Independent counsel may be instructed to deal with legally privileged material which is in hard copy form. We nonetheless are of the view that guidance would be best contained in an electronic material Code of Practice.

11.33 In modern, document-heavy criminal investigations in which independent counsel are instructed, the distinction between electronic material and hard copy material may not be so clear cut. In most cases, the evidence collected will be in electronic form. The vast majority of material which is or is claimed to be legally privileged will be electronic, as was highlighted by the HM Council of District Judges (Magistrates' Courts) in their consultation response. In those cases in which there is also hard copy material, the material will likely be scanned and uploaded into an electronic database to be reviewed through a document review platform. Material may then be reviewed by lawyers, independent counsel and others. The fact that some material was originally in hard copy form may make little difference to how it is subsequently treated.

11.34 In light of the above, we therefore consider that the Code of Practice that we recommend could usefully discuss the treatment of hard copy documents and review by independent counsel. We consider this justified by the small amount of material that may at first be encountered in hard copy form and the high likelihood that hard copy material will be scanned, uploaded and treated in the same way as digital material. As a final point, we also consider that inserting guidance on instructing independent counsel in respect of electronic material in one Code of Practice, and guidance in respect of hard copy documents in, say, Code B of PACE could create unnecessary overlap and lead to confusion as to which guidance ought to be followed.

Recommendation 41

11.35 We recommend that the procedure for instructing independent counsel or other experts to resolve issues of legal privilege be dealt with in a new Code of Practice which we recommend at Recommendation 63 of this report.

CLAIMING PRIVILEGE IN RESPECT OF MATERIAL SOUGHT UNDER A WARRANT

The current law

11.36 There are now many cases where it is not reasonably practicable to determine which category material falls into or to separate material into what may and may not be seized during the search of premises. In these cases, there are powers of "seize and sift" under sections 50 and 51 of the CJPA. These powers allow the seizure of both non-privileged and privileged material for sorting at a later stage.

11.37 Where these powers are used in respect of legally privileged material, it is increasingly common for independent counsel to be instructed to be present when the material is sorted, rather than at the search of the premises.[15] Alternatively, there may be a first sift at which investigators isolate the potentially legally privileged material using search terms provided by the owner of the material and a further sift where independent counsel is present. The courts have held this last approach to be permissible provided that there are arrangements to ensure, as far as possible, that the investigator's staff do not have sight of legally privileged material.[16]

11.38 There are important practical reasons for retaining this flexibility. In some cases, there will have been no reasonable grounds to believe that legally privileged material is on the premises when the warrant was issued. Therefore, there will have been no reason to arrange for the presence of independent counsel at the search of the premises. The issue of privilege and the need for independent counsel would only arise if material that may be privileged was found during the search or if material was seized in bulk and the owner of the material claimed that some of it was privileged.

The consultation paper

11.39 Practitioners reported considerable difficulties with conducting searches where claims for legal privilege are made, especially in cases involving large volumes of material. Investigators with whom we had spoken expressed concern that the actual or alleged presence of *any* privileged material, for example on a mobile phone or a computer drive, requires the cumbersome procedure for identifying and segregating privileged material to be put in motion. This is the case even when the material is entirely irrelevant to the offence investigated. For example, a mobile phone or computer hard drive may contain old legal documents relating to divorce proceedings or a personal injury claim, which are of no possible interest to the investigator carrying out the search.

11.40 We recognised that dealing with potentially large quantities of material which consists of or includes legally privileged material that is irrelevant to the investigation poses difficulties for investigators. At the same time, we made clear that, whatever proposals were adopted, legally privileged material should remain absolutely exempt from seizure under a search warrant.

11.41 We also acknowledged that there could be cases where the only privileged material among the material sought is clearly irrelevant to the investigation and incapable of being prejudicial. In these cases, legal privilege may be claimed only as a delaying tactic to frustrate the investigation.

11.42 To make the process of segregating, returning and deleting legally privileged material and examining non-privileged material more efficient, we provisionally proposed[17] that a person claiming legal privilege in respect of material seized should be required to make all reasonable efforts to assist the investigator in identifying what is legally privileged. We invited consultees' views on whether:

---

15 *R (Rawlinson and Hunter Trustees) v Central Criminal Court* [2012] EWHC 2254 (Admin), [2013] 1 WLR 1634.

16 *R (McKenzie) v Director of the Serious Fraud Office* [2016] EWHC 102 (Admin), [2016] 1 WLR 1308.

17 Consultation Question 43.

(1) this should take the form of a procedure in which a Crown Court judge makes an order requiring details for the identification of material for which privilege is claimed within a specified time; and

(2) the Crown Court judge should have the power to order the person claiming privilege to pay the costs of the application and of the sifting process if the claim to privilege is clearly unfounded or the information given to the investigator to locate the privileged material was too vague or not given in good faith.

Consultation responses

11.43 Twenty-one consultees[18] answered this question. On the requirement to make all reasonable efforts to assist the investigator: 14 agreed;[19] three disagreed;[20] and three expressed other views.[21]

11.44 Most consultees agreed with our provisional proposal that a person claiming legal privilege in respect of material seized following the execution of a search warrant should be required to make all reasonable efforts to assist the investigator in identifying what is legally privileged. Several consultees agreed with the procedure we set out at paragraph 9.24 of our consultation paper.[22] Under that procedure, the Crown Court would be authorised to issue an "unless order" requiring the person claiming privilege to cooperate with the investigator. If they did not, their claim would be treated as if it were never raised and they would potentially be held in contempt of court or face a costs order.

11.45 In the view of the Magistrates Association, the proposal seemed to strike the right balance between the protection of vital human rights and ensuring any search, sift or seizure is conducted flexibly enough to be effective in its legitimate aim. Further, it made the point that judicial oversight is necessary to ensure rights are protected against the powers of the State.

11.46 HM Council of District Judges (Magistrates' Courts) noted that the proposal was broadly similar to the approach taken to the disclosure of unused material in the Criminal Procedure and Investigations Act 1996 (CPIA). In the CPIA, the prosecution and defence are required to engage effectively in the process of disclosure in order to ensure resources are used efficiently.

---

18 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Guardian News and Media; Insolvency Service; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; Northumbria Law School Centre for Evidence and Criminal Justice Studies; The Law Society; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; Bar Council and the Criminal Bar Association; Metropolitan Police Service; National Crime Agency; Competition and Markets Authority; Serious Fraud Office; Financial Crime Authority.

19 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Guardian News and Media; Insolvency Service; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; Justices' Clerks' Society; Magistrates Association; Bar Council and the Criminal Bar Association; National Crime Agency; Serious Fraud Office.

20 The Law Society; Dijen Basu QC; Competition and Markets Authority.

21 Crown Prosecution Service; Northumbria Law School Centre for Evidence and Criminal Justice Studies; Metropolitan Police Service.

22 HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; Justices' Clerks' Society; Magistrates Association.

11.47 The Council of Her Majesty's Circuit Judges agreed, but emphasised that they are reluctant for Crown Court judges to assume new areas of responsibility due to resource constraints.

11.48 The NCA agreed with the proposal, and stated that it is particularly important for occupiers to help to identify potentially privileged material when it is held on electronic devices. It considered that it would be unreasonable and a disproportionate cost to require independent counsel to review everything on an electronic device because the occupier had made a claim of privilege but failed to assist in the identification of the relevant material.

11.49 The SFO also agreed with the proposal, observing that it would greatly reduce the scope for investigations to be delayed or frustrated. However, it noted that in its experience the most productive approach was a co-operative one, and therefore suggested that co-operation should be sought in the first instance before judicial intervention. They considered that the onus should be on the person claiming privilege to object to the approach proposed by the investigator, and that it should be open to the court simply to affirm that approach.

11.50 A number of consultees disagreed with our provisional proposal. The CMA considered that the proposal was overly complicated. The Law Society argued that while it is clearly helpful if someone making an assertion of privilege can tell the investigator where the material is, it is inappropriate for the state to force individuals to assist with investigations being undertaken against them. Moreover, they noted that in practice it can be very difficult for the suspect to assist the authorities in locating this material.

11.51 Dijen Basu QC also considered it inappropriate to create a statutory obligation compelling the suspect to identify privileged material. He suggested that recalibrating the section 59 CJPA procedure could allow a person with an interest in material to make an application to the Crown Court for a court-mandated examination by independent counsel of the material seized or part thereof. It could also be required that the person claiming privilege must cooperate with independent counsel.

11.52 The FCA welcomed giving the Crown Court a role in resolving issues surrounding legal privilege. However, it stated that any Crown Court procedure should enable the investigator or person with an interest in the property to apply to the court for directions as of right. The FCA considered that it was unrealistic to expect occupiers to be able to state the grounds on which privilege is raised over and above repeating the legal advice they have received, and occupiers without the benefit of legal representation can be expected to assist even less.

11.53 The FCA also stated that currently, where the occupier fails to engage (or engage sensibly) with the "LPP process", it makes its own assessment of LPP risk and causes the material to be reviewed according to a managed plan. Any potential legally privileged material identified is isolated for review by independent counsel. Therefore, it would be opposed to a development that hinders its ability to "press ahead" with an appropriately drafted plan where they receive limited assistance from or are obstructed by relevant parties.

11.54 The MPS and Northumbria Law School Centre for Evidence and Criminal Justice Studies queried what would amount to "reasonable efforts" to assist in the identification of legally privileged material. For example, would it require the party claiming privilege to pay the costs of their own lawyer?

11.55 For a number of reasons, the Bar Council and the CBA did not agree that Crown Court judges should have the power to order the person claiming privilege to pay the costs of the application and of the sifting process if the claim to privilege is clearly unfounded or the

information given to the investigator to locate the privileged material was too vague or not given in good faith.

11.56 First, there was a concern that some Circuit judges have demonstrated a propensity to make such orders too quickly. Secondly, there would be huge potential for additional litigation, which would delay the investigation to no one's benefit. Thirdly, the wasted costs procedure should be adequate to deal with unfounded or unsupported claims. Fourthly, in many instances the subject claiming privilege will have their assets restrained, meaning that there are no available funds to satisfy a costs order.[23]

11.57 The CPS put forward an alternative procedure to return control to the investigator, which could perhaps be formalised in the CrimPR. That procedure would be:

(1) the investigator serves a list of seized material on those with an interest in the property;

(2) within a specified period, anyone with an interest in the property can make a claim of privilege and, if they do, their claim must be sufficiently detailed;

(3) within a specified period, the investigator must serve notice of their response, which will either:

(a) acknowledge the claim to privilege and confirm in principle how the material will be sifted;

(b) state whether the claim to privilege is considered unmeritorious, or

(c) state whether the claim to privilege is insufficiently detailed and detail how sifting will be conducted in the absence of more detailed information.

(4) within a specified period, the person who made a claim of privilege will have the opportunity to provide more detailed information about how to locate the alleged legally privileged material; and

(5) an application can be made to the Crown Court for a ruling on how to sift the seized material where the parties cannot agree.

Analysis

11.58 At Recommendation 57,[24] we recommend that whenever electronic material is seized or produced during the execution of a search warrant, protocols setting out how that material is to be examined can be requested by a person with an interest in the property and must be supplied to them within a reasonable time. Search protocols would help a person with an interest in property to decide whether to make an application to the Crown Court to adjudicate on a dispute regarding how their electronic devices are to be examined, a mechanism which we recommend at Recommendation 61.[25] Under this mechanism, an investigator would also be able to seek the Crown Courts approval of the protocol, permitting

---

23 This point was also made by the Metropolitan Police Service and Financial Conduct Authority.

24 See paragraph 17.101 below.

25 See paragraph 17.133 below.

them to press ahead with the investigation. The protocol would therefore be capable of judicial approval or scrutiny.

11.59 In our view, these recommendations achieve our policy objectives while addressing several of the underlying concerns raised by consultees in this section.

(1) Several parties agreed in principle with the Crown Court having a supervisory role in relation to disputes regarding legally privileged material. For instance, the Magistrates Association viewed judicial oversight as vital. We agree, and our recommendations ensure far greater judicial oversight.

(2) The new power would not be reliant on defence participation, which we acknowledge may be difficult to secure. Additionally, even where a defendant is willing to cooperate, a costs order may still be ineffective. Some defendants facing prosecution will have their assets restrained or confiscated, and others will be of very limited means.

(3) If investigators could ask the Crown Court to confirm their approach to sifting material, this would address the FCA's concern with being unable to "press ahead" with examining seized material in accordance with an appropriate managed plan. The new power would therefore return impetus, power and responsibility to the investigator, as suggested by the CPS and SFO. The investigator would retain control of the process and the burden of making investigative decisions, which they are best placed to do.

(4) The new power would be flexible because an application could be made by either an investigator or a person affected by the warrant. This accords with the suggestion made by Dijen Basu QC to recalibrate the section 59 CJPA procedure so that both investigators and property owners can apply to the court for adjudication of disputes.

(5) Our recommendation is sensitive to the concern expressed by the Council of Her Majesty's Circuit Judges over Crown Court judges assuming new areas of responsibility. Our recommendation would in effect be an expansion of the supervisory role which the Crown Court already enjoys under section 59 of the CJPA, especially given that issues concerning the treatment of protected material may already be addressed by a judge during a section 59 hearing.

(6) Having a new Crown Court procedure overcomes the objection raised by some consultees over our provisional proposal, that a person claiming legal privilege should be required to help identify material, on the ground that it would be inappropriate for the state to force individuals to assist with investigations being conducted against them. Under the new procedure, either an investigator or a person with an interest in the material seized could make an application, but there is no compulsion for either to do so.

11.60 This procedure would be complemented by the Code of Practice that we recommend at Recommendation 63,[26] which could also help investigators and occupiers to resolve disputes regarding protected material outside of the courtroom. We note to this end the comments made by the SFO, who stated that in their experience the most productive approach was a co-operative one, and accordingly co-operation should be sought in the first instance before judicial intervention.

---

[26] See paragraph **Error! Reference source not found.** below.

11.61 One issue is that, depending on the scope of the new procedure, the position would not be the same in respect of hard copy material. This would seem to create an artificial distinction between hard copy documents and electronic material. As we write at paragraph 17.72 below, were our recommendations to be taken forward, thought should be given to expanding the regime to all forms of material.

Chapter 12: The treatment of excluded material

INTRODUCTION

12.1 In this chapter we consider reform to the way in which "excluded material" is treated when applying for and executing a search warrant. Excluded material, along with legally privileged material[1] and special procedure material,[2] make up what we term "protected material". That is, categories of material which are either completely exempt from being searched for under warrant or require additional criteria to be met before a search warrant can be issued.

12.2 Excluded material is defined in section 11 of the Police and Criminal Evidence Act 1984 ("PACE"); the definition is also adopted in some other Acts.[3] Excluded material covers the following categories of material, when held in confidence:[4]

(1) personal records which a person has acquired or created in the course of any trade, business, profession or other occupation or for the purposes of any paid or unpaid office ("confidential personal records");

(2) human tissue or tissue fluid which has been taken for the purposes of diagnosis or medical treatment; and

(3) journalistic material which consists of documents or records ("confidential journalistic material").

Personal records and journalistic material are further defined in sections 12 and 13 of PACE respectively. We set out these definitions in the sections which follow.

12.3 For those regimes that adopt the term excluded material, such material may only be obtained pursuant to a search warrant in limited circumstances. Under PACE, for example, in order for a search warrant to be obtained for excluded material the second set of access conditions under paragraph 3 of schedule 1 must be satisfied in addition to the criteria under paragraph 12.

12.4 Under regimes which do not use this term, the material which falls under the PACE definition of excluded material may not require additional criteria to be met before a search warrant is issued beyond the criteria for issuing an ordinary warrant. We expressed the view in our consultation paper that the law governing the treatment of excluded material is unprincipled and consulted on introducing a more uniform set of rules.

12.5 In this chapter, we consider the following specific matters relating to excluded material on which we consulted:

---

1 We discuss the treatment of legally privileged material in Chapter 11 of this report.

2 We discuss the treatment of special procedure material in Chapter 13 of this report.

3 Ivory Act 2018, s 24(2)(b); Higher Education and Research Act 2017, sch 5, para 6(5)(b); Psychoactive Substances Act 2016, s 44(2)(b); Armed Forces Act 2006, s 83(4); Extradition Act 2003, s 174(3)(a); Proceeds of Crime Act 2002, s 379; Terrorism Act 2000, sch 5, para 4(a).

4 Police and Criminal Evidence Act 1984, s 11(1).

(1) obtaining search warrants in respect of confidential personal records;

(2) obtaining search warrants in respect of confidential journalistic material;

(3) abolishing the second set of access conditions under paragraph 3 of schedule 1 to PACE; and

(4) strengthening the protection of excluded material and special procedure material in cases of seizure not under warrant.[5]

12.6 We make two recommendations in this chapter, which relate to the three categories of excluded material listed at paragraph 12.2 above. We conclude that the law governing access to confidential personal records, human tissue, tissue fluid and confidential journalistic material under PACE is too restrictive and arbitrary. However, we do not make firm recommendations due to the significant impact that reform would have on each category of material and the need for further consideration and consultation before any reform takes place. Some of these implications are outside the scope of our review since they relate to other statutory powers. Accordingly, we recommend that the Government considers whether the right balance is struck between the prevention and investigation of serious crime and the specific public interests that each category of excluded material seeks to protect and, if not, whether the law ought to be reformed.

PERSONAL RECORDS

The current law

The definition of "personal records" and "in confidence"

12.7 As set out at paragraph 12.1 above, excluded material defined in section 11 of PACE covers personal records which a person has acquired or created in the course of any trade, business, profession or other occupation or for the purposes of any paid or unpaid office and which are held in confidence.[6]

12.8 The term "personal records" is then defined in section 12 of PACE as covering documentary and other records concerning an individual (whether living or dead) who can be identified from them and relating to:

(1) their physical or mental health;

(2) spiritual counselling or assistance given or to be given to them; or

(3) counselling or assistance given or to be given to them, for the purposes of their personal welfare, by any voluntary organisation or by any individual who—

(a) by reason of their office or occupation has responsibilities for their personal welfare; or

(b) by reason of an order of a court has responsibilities for their supervision.

---

5 The provisions which are discussed in this section permit the seizure or production of both excluded material and special procedure material. To avoid repetition in the next chapter on special procedure material, we discuss what the position should be in respect of both excluded material and special procedure material.

6 Police and Criminal Evidence Act 1984, s 11(1)(a).

12.9 A person holds a personal record, human tissue or tissue fluid in confidence if they hold it subject to:[7]

(1) an express or implied undertaking to hold it in confidence; or

(2) a restriction on disclosure or an obligation of secrecy contained in any enactment, including an enactment contained in an Act passed after PACE.

The provisions of PACE relating to excluded material

12.10 The circumstances in which excluded material can be obtained by investigators in criminal investigations vary. In summary:

(1) it is no longer possible to use any pre-PACE provisions which authorised an investigator to apply for a search warrant to search for excluded material;[8]

(2) schedule 1 to PACE provides a restrictive set of access conditions permitting a production order or search warrant to be sought for excluded material;

(3) a small number of PACE provisions permit the seizure or production of excluded (or special procedure) material which are not dependant on a search warrant;[9] and

(4) provisions enacted after PACE contain differing approaches to excluded material.

We now discuss these rules in further detail.

12.11 Following the enactment of PACE, any search warrant provision passed *before* PACE under which a search warrant could be authorised to search for excluded material (or special procedure material) can no longer do so.[10] Search warrants under section 8 of PACE may not be issued in respect of excluded material or special procedure material.[11] Nor may excluded material or special procedure material be seized in the course of a search.[12] However, legally privileged, excluded and special procedure material may be seized under sections 50 and 51 of the Criminal Justice and Police Act 2001 ("CJPA"), which requires each category material to be sifted off-site and returned.[13]

---

7 Police and Criminal Evidence Act 1984, s 11(2).

8 Police and Criminal Evidence Act 1984, s 9(2).

9 Police and Criminal Evidence Act 1984, ss 18(2), 19(2) and (3), 20(1) and 32(9).

10 Police and Criminal Evidence Act 1984, s 9(2). Material in the possession of a person who acquired or created it in the course of any trade, business, profession or other occupation or for the purpose of any paid or unpaid office and which relates to a matter in relation to which HM Revenue and Customs have functions, is neither excluded material nor special procedure material for the purposes of any enactment such as is mentioned in the Police and Criminal Evidence Act 1984, s 9(2). See Police and Criminal Evidence Act 1984 (Application to Revenue and Customs) Order 2015 (SI 2015 No 1783), art 6.

11 Police and Criminal Evidence Act 1984, s 8(1)(d).

12 Police and Criminal Evidence Act 1984, s 8(2).

13 Criminal Justice and Police Act 2001, ss 54 and 55.

12.12 Schedule 1 to PACE does, however, provide a procedure for obtaining access to excluded material and special procedure material.[14] Excluded material can be obtained under the "second set of access conditions".[15]

12.13 Unlike the first set of access conditions for special procedure material, the second set of access conditions are very restrictive. We summarise the access conditions at paragraphs 12.15 to 12.16 below. For both sets of access conditions, the default position under schedule 1 to PACE is to obtain a production order where either of the conditions are met.[16] If, however, further conditions are met,[17] such as that the service of notice of an application for a production order may seriously prejudice the investigation, an investigator may apply for a search warrant.[18]

12.14 The powers of seizure and production under sections 18, 19, 20 and 32 of PACE[19] provide no exclusion for special procedure and excluded material and therefore both can be obtained under these provisions. We discuss reform to these provisions at paragraphs 12.193 to 12.219 below.

12.15 The second set of access conditions under schedule 1 to PACE is fulfilled if three conditions are met:

(1) there are reasonable grounds for believing that an indictable offence has been committed and that there is excluded material on the premises;

(2) but for section 9(2) of PACE (which prevents access to excluded material under a pre-PACE statute), a search of such premises for the material could have been authorised by the issue of a warrant to a constable; and

(3) the issue of such a warrant would have been appropriate.

12.16 The effect of the second set of access conditions is that a constable can only apply for a production order (or search warrant) if they can direct the issuing authority to a pre-PACE search warrant provision under which they could have appropriately applied for a warrant for excluded material.

Case law relating to the second set of access conditions

12.17 Case law indicates that there are few, if any, pre-PACE search warrant provisions that would have allowed a search for confidential personal records. In *R v Central Criminal Court ex parte Brown*, McCowan LJ, quashing a search warrant under the second set of access conditions in respect of medical records, observed that there was no enactment which would have authorised the issue of a warrant to a constable to seize the material in question.[20]

---

14 Special procedure material can be obtained under the "first set of access conditions" under the Police and Criminal Evidence Act 1984, sch 1, para 2, which is discussed in detail in the next chapter.

15 Police and Criminal Evidence Act 1984, sch 1, para 3.

16 Police and Criminal Evidence Act 1984, sch 1, para 4.

17 Police and Criminal Evidence Act 1984, sch 1, para 14.

18 Police and Criminal Evidence Act 1984, sch 1, para 12.

19 We provide a description of these provisions at paragraph 12.194 below.

20 *R v Central Criminal Court ex parte Brown*, *The Times* 7 September 1992.

12.18 A similar conclusion was reached in *R v Singleton* by Farquharson LJ in respect of dental records.[21] In that case, human bite marks were found on the body of a murdered girl. The appellant was arrested for murder but refused to provide a sample of his tooth marks. The appellant's dentist voluntarily handed over his dental records. An expert found that there was a general match between the cast made from the appellant's teeth and the bite marks which were found on the body of the girl. The appellant was convicted and appealed. Although dismissing the appeal, the Court of Appeal accepted that if the prosecution had made an application under the second set of access conditions, the Circuit judge would have been bound to refuse it as there were no pre-PACE powers under which the dental records could have been sought.

12.19 Medical records were also at issue in *R v Cardiff Crown Court ex parte Kellam*.[22] The body of a young woman was found. She had been stabbed 83 times. The police believed the suspect to be an in-patient from a psychiatric hospital on day release. The police approached the hospital asking for details of patients who were absent from the hospital on day release at the time. The hospital responded that, in order to be seen to protect their patients' confidentiality, they would only provide the information if ordered to do so by the court.

12.20 A production order was issued for special procedure material under the first set of access conditions. A consultant forensic psychiatrist at the hospital successfully brought a judicial review to set aside the production order on the grounds that records of admission to and discharge from hospital constituted excluded material under section 11 of PACE, rather than special procedure material. Evans LJ reached the conclusion "with considerable reluctance", writing:

> I question whether Parliament could have intended that the exemption of "personal records" should place such a restriction upon the investigation of serious crime as the appellants contend that it does. We were not referred to any parliamentary material, but Professor Zander in the (*sic*) The Police & Criminal Evidence Act 1984 (2nd ed.) attributes the width of the statutory definition to "the fierce campaign waged in particular by the British Medical Association, the bishops and Citizens Advice Bureau" (p.34).

12.21 Morland J, concurring, wrote that the words of PACE:

> must be given their ordinary and natural meaning. This is so even if the result may seriously impede Police investigations into a terrible murder and allow a very dangerous man to remain at large and a real risk to others. Parliament defines "excluded material", as a matter of public policy, presumably, because it considered that the confidentiality of records of identifiable individuals relating to their health should have paramountcy over the prevention and investigation of serious crime. It is not for the Courts to question whether Parliament has struck the right balance or unreasonably over-emphasised the importance of confidentiality.

12.22 The Divisional Court in that case also referred to an academic article which itself referred to an unsuccessful attempt to obtain access to hospital and out-patient records made by an English police force. The record was sought of a man suspected of murder who had himself

---

21 *R v Singleton* [1995] 1 Cr App R 431, 438.

22 *R v Cardiff Crown Court ex parte Kellam, The Times* 3 May 1993.

sustained injuries during the killing. The argument that the records were administrative rather than personal records was rejected by the Circuit judge.

Other statutory provisions under which excluded material may be available

12.23 The power to obtain excluded material under provisions enacted *after* PACE depends on the particular regime concerned. For example, excluded material cannot be obtained in any circumstances through a production order or search warrant under the Proceeds of Crime Act 2002.[23] Enforcement regimes enacted after PACE under which there is no exclusion of the categories of material which comprise excluded material (confidential personal records, human tissue, tissue fluid or confidential journalistic material) permit the material to be sought under a warrant.[24]

12.24 Schedule 5 to the Terrorism Act 2000 uses the definition of excluded material from PACE and provides a procedure for obtaining access to such material. Unlike PACE, the Terrorism Act 2000 has a single set of access conditions for production orders which more or less mirror the first set of access conditions under PACE in relation to special procedure material.[25] As with PACE, a search warrant can be obtained to search for excluded material where further conditions are met.[26]

12.25 The statute book contains powers to require the production of confidential personal records which relate to non-criminal investigations, such as powers provided to HM Senior Coroner[27] and the Care Quality Commission.[28]

The consultation paper

12.26 Quite apart from issues of access, in the consultation paper, we formed the provisional view that basing access to excluded material on the date of enactment of the statutory power under which the material is sought and the identity of the person seeking the material may lead to arbitrary results. We considered that there may be merit in a simplified set of rules providing a more uniform level of protection, with exceptions where appropriate.

12.27 In respect of confidential personal records, we considered that the situation could be simplified by the introduction of a uniform scheme in respect of criminal investigations. That is, the rule could be the same whether the investigation is being carried out by a police officer or not, and whether it is under PACE or under a statute passed before or after PACE.

12.28 We recognised a number of reasons why personal records ought to have a high level of protection. These reasons related to the importance of confidentiality, not wanting to dilute the level of protection currently afforded to personal records and the impression given by some stakeholders that personal records are rarely sought in criminal investigations. At the same time, we recognised that there will be instances where personal records are relevant to an investigation. In addition to the cases cited above, these might include cases of serious medical malpractice or offences of intentionally or recklessly transmitting a sexual infection.

---

23 Proceeds of Crime Act 2002, ss 348, 354 and 379.

24 For example, Criminal Justice Act 1987, s 2; Financial Services and Markets Act 2000, ss 171 to 176.

25 Terrorism Act 2000, sch 5, para 6.

26 Terrorism Act 2000, sch 5, para 12.

27 Coroners and Justice Act 2009, sch 5.

28 Health and Social Care Act 2008, s 64.

We were therefore interested in consultees' views on whether the current law constitutes an undesirable fetter on the investigation of these offences.

12.29 Another question we considered was whether the views of patients should be taken into account when a search warrant is applied for and the medical records are not those of the suspect(s). The law recognises that an individual has an interest in the confidentiality of their medical records. There is no absolute right to object to their disclosure, but the individual has a right to be informed of the application in advance, and to make representations before any order is made. At the same time, we recognised impediments if the patients are unknown or deceased.

12.30 In light of the above, we provisionally proposed that:[29]

(1) there should be a uniform rule for the availability of search warrants in respect of medical and counselling records, irrespective of the particular power under which the warrant is sought and the identity of the person applying for or executing the warrant;

(2) that rule should provide that medical and counselling records are excluded from the scope of search warrants in all cases, whatever the statutory source of the power to issue a search warrant; and

(3) there should be a tightly circumscribed exception to this exclusion in the case of investigations where medical and counselling records are central to the issues investigated.

12.31 We also invited consultees' views on whether:

(1) if medical records are to remain within the scope of search warrants, then in those instances where the patient is not the suspect, they should have the right to be informed and make representations before a warrant is issued or a production order is made; and

(2) a similar uniform rule ought to exist in respect of human tissue or tissue fluid which has been taken for the purposes of diagnosis or medical treatment and which a person holds in confidence under section 11(1)(b) of the Police and Criminal Evidence Act 1984.

Consultation responses

12.32 Twenty-one consultees[30] provided comments on the treatment of personal records.

---

29 Consultation Question 44.

30 City of London Economic Crime Academy; NHS Counter Fraud Authority; Department for Work and Pensions; Professor Richard Stone; HM Council of District Judges (Magistrates' Courts); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; Northumbria Law School Centre for Evidence and Criminal Justice Studies; The Law Society; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; Bar Council & Criminal Bar Association; Metropolitan Police Service; National Crime Agency; Serious Fraud Office; Financial Conduct Authority.

A uniform rule

12.33 Nearly all consultees who responded agreed that there ought to be a uniform rule in respect of medical records.[31] The Crown Prosecution Service ("CPS") considered that the lack of uniformity of the availability of warrants in terms of powers and applicants has no apparent or defensible logic. The Northumbria Law School Centre for Evidence and Criminal Justice Studies described the current law as inconsistent, complex and difficult to justify. Dijen Basu QC, in agreement, considered there should be a uniform rule for the ability of search warrants *and production orders* to target medical and counselling records.

12.34 The Financial Conduct Authority ("FCA") recognised that rationalisation seemed appealing. However, they pointed out that the relevance of medical or counselling records to differing types of investigations may vary considerably. At present, there is no restriction under the Financial Services and Markets Act 2000 on searching for personal records. In the circumstances, the FCA were opposed to the imposition of additional statutory restrictions to the scope of their search powers. They had not experienced particular difficulties in the exercise of their search powers with respect to medical records. In their view, the addition of specific additional exemptions to their warrant regime could create unnecessary difficulties.

A general prohibition on access

12.35 Quite apart from whether there should be a uniform rule, there was for the most part agreement on what that rule should be. In particular, the majority of consultees agreed with the starting principle that medical and counselling records should be excluded from the scope of search warrants in all circumstances.[32]

12.36 The CPS agreed with the rule that it should not be possible to obtain medical and counselling records by way of a search warrant and that a person should expect confidentiality when consulting a medical practitioner or counsellor. This rule was said to underpin the faithful and effective operation of medicine and counselling.

12.37 However, both the Bar Council and the Criminal Bar Association ("CBA") voiced concerns about the fettering of the current rights of an investigator to obtain such material under powers outside section 8 of PACE warrants.

---

31 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; Northumbria Law School Centre for Evidence and Criminal Justice Studies; The Law Society; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; Bar Council & Criminal Bar Association; Metropolitan Police Service; National Crime Agency.

32 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; The Law Society; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; Bar Council & Criminal Bar Association; Metropolitan Police Service.

An exception to the general prohibition on access

12.38 The majority of consultees also agreed with the caveat that there should be tightly circumscribed exceptions to the above prohibition in the case of investigations where medical and counselling records are central to the issues investigated.[33]

12.39 Consultees reported particular problems with the second set of access conditions under PACE. The NHS Counter Fraud Authority ("NHSCFA") explained that, notwithstanding their need to obtain police assistance to apply for search warrants, the current system of obtaining medical records is unsatisfactory. There is no pre-PACE legislation under which the material could have been sought, consequently it is impossible to satisfy the second set of access conditions in schedule 1.[34] Therefore, the only way to obtain the material is through cooperation. Given their statutory remit, there is every likelihood that evidence in their cases will include excluded material.

12.40 The National Crime Agency noted that, in criminal investigations into individuals or hospital trusts, investigations into medical records may form part of a legitimate line of enquiry. They appeared to welcome express provision for access to medical and counselling records whenever they are required for criminal investigations (and not just where the second set of access conditions in schedule 1 to PACE are satisfied). As a practical matter, they noted that, in respect of counselling records, the National Crime Agency may not know who the patients are until they seize records. However, they noted that where patients are interviewed or are not suspects they often hand over records voluntarily.

12.41 The City of London Police Economic Crime Academy recommended a clear and practical access route to gather excluded material, in particular access to medical records. They stated that medical records are frequently sought during investigations, many of which concern either allegations of fraud committed by medical practitioners and dentists, or investigations into insurance fraud. They stated that the second set of access conditions, and in particular the requirement that there be an appropriate pre-PACE power, is the root of the problem preventing access to important evidence.

12.42 One police force shared details of an ongoing investigation in which the second set of access conditions has caused serious difficulties.[35] The police force is carrying out a complex abuse investigation relating to multiple offences of gross-negligence manslaughter, wilful neglect and ill-treatment involving over a dozen deaths in care homes.

12.43 Independent legal advice has indicated that search warrants for patients' records could not be obtained as there is no pre-PACE power under which the target material could have been sought. In this case, the police have to rely upon the goodwill of the care home company to make records available to them after the death of a resident which may be associated with safeguarding concerns. The company may be culpable in that death. The police will never know whether all documentation has been provided and, if provided, whether it is in its original state.

---

33 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; The Law Society; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; Bar Council & Criminal Bar Association; Metropolitan Police Service.

34 Police and Criminal Evidence Act 1984, sch 1, para 3(b).

35 We have anonymised the name of the police force and the description of the case.

12.44 The police force contended that the lack of police powers to obtain such material seriously undermines the effectiveness of police investigations, would seem perverse to the administration of fair justice, and would undoubtedly undermine the confidence of the public in the criminal justice system if widely known. They suggested that unscrupulous care providers could easily evade criminal scrutiny if the limited police powers were widely known. The police force stated that adult safeguarding is becoming an area of increasing national concern, and as the population ages this concern is likely to increase. For this reason, they argued that the lack of police powers in this area will likely lead to increasing investigative problems and associated public dissatisfaction if not addressed.

12.45 In addition to concerns about the restrictive conditions in the second set of access conditions under PACE, consultees also raised more general concerns. The Serious Fraud Office ("SFO") explained that medical records may need to be seized under search warrants in appropriate cases. They also expressed concern that changes to their search warrant powers may inadvertently make changes to their production notices under section 2(3) of the Criminal Justice Act 1987 ("CJA").

12.46 The SFO also made the point that a court may authorise a regulator such as the General Dental Council or General Medical Council to access patient records in connection with a disciplinary investigation, provided that disclosure constitutes a necessary and proportionate interference with patient confidentiality and privacy rights under article 8 of the European Convention on Human Rights ("ECHR"). In their view, broadly equivalent powers should be available for criminal investigations into serious or complex fraud as for disciplinary investigations into fitness to practise.

12.47 The CPS agreed that there should be a clear and genuinely rare exception to permit access to personal records for the most serious offences in which they are required. They considered that this should be placed on a statutory footing and be subject to judicial oversight rather than dependent on practitioners applying the guidance issued by their professional body.

12.48 The Northumbria Law School Centre for Evidence and Criminal Justice Studies argued that careful consideration is required when deciding which circumstances should justify access to medical and counselling records. They noted that orders or warrants in relation to personal records can be of benefit to the holder of the records. Guidance from the General Medical Council currently provides:[36]

> You must not disclose personal information to a third party such as a solicitor, police officer or officer of a court without the patient's explicit consent, unless it is required by law, or ordered by a court, or can be justified in the public interest. You may disclose information without consent to your own legal adviser to get their advice.[37]
>
> Disclosing personal information may be justified in the public interest if failure to do so may expose others to a risk of death or serious harm. The benefits to an individual or to society

---

36 General Medical Council, *Confidentiality: good practice in handling patient information* (25 May 2018), available at https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality.

37 General Medical Council, *Confidentiality: good practice in handling patient information* (25 May 2018) at para 93.

of the disclosure must outweigh both the patient's and the public interest in keeping the information confidential.[38]

Such a situation might arise, for example, if a disclosure would be likely to be necessary for the prevention, detection or prosecution of serious crime, especially crimes against the person. When victims of violence refuse police assistance, disclosure may still be justified if others remain at risk, for example from someone who is prepared to use weapons, or from domestic violence when children or others may be at risk.[39]

12.49 The Northumbria Law School Centre for Evidence and Criminal Justice Studies explained that these can be difficult decisions given the competing interests, meaning that advice from a Caldicott Guardian[40] or legal adviser may be sought. Therefore, judicial authorisation of a production order or search warrant is arguably preferable to reliance on a doctor's public interest justification for three main reasons.

(1) It would avoid the need for the relevant clinical teams (and/or their advisers) to balance the competing interests as they may not be best placed to assess the relevance of the confidential information to the investigation.

(2) It could be argued that this approach may be less damaging to the relationship of trust between doctor and patient.

(3) It would offer greater protection to the doctor and reduce anxiety regarding the possibility of legal action based on breach of the duty of confidence or an article 8(1) ECHR claim should the patient consider the wrong conclusion has been reached.

12.50 As for how the exception should be framed, we received a number of views. Dijen Basu QC agreed that personal records should be excluded, save where centrally relevant, either for fraud offences (for example, by health professionals in the NHS) or to cure the problem which arose in *R v Cardiff Crown Court ex parte Kellam* (where a psychiatric hospital would not provide details of patients who had been out on day release at the time of a murder, discussed at paragraphs 12.19 to 12.21 above).

12.51 The Bar Council and the CBA had concerns as to how "central to the issues investigated" is defined and would prefer the test to be where "there are reasonable grounds to believe that medical and counselling records would provide evidence relevant to an important issue in the investigation". It would then be for the applicant to satisfy the tribunal that the medical records of a non-suspect are relevant to an important matter.

12.52 The Northumbria Law School Centre for Evidence and Criminal Justice Studies suggested that the test should be whether relevant issues cannot be properly resolved without access to medical or counselling records.

12.53 The FCA argued that, if we were to recommend a rule of general exemption of personal records, consideration should be given to an across the board iniquity exception and/or

---

38 General Medical Council, *Confidentiality: good practice in handling patient information* (25 May 2018) at para 64.

39 General Medical Council, *Confidentiality: good practice in handling patient information* (25 May 2018) at para 65.

40 A Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly. All NHS organisations and local authorities which provide social services must have a Caldicott Guardian.

public interest test. It was observed that the rights protected by these rules are qualified rights (rather than an absolute protection of the scope of legal privilege) and so the FCA were of the view that this should be reflected in the law.

A patient's right to be informed and make recommendations

12.54 Seven consultees[41] agreed that, in cases where a search warrant or production order is made in respect of medical or counselling records and the patient is not the suspect, they should have the right to be informed and make representations before a warrant is issued or a production order is made.

12.55 The Northumbria Law School Centre for Evidence and Criminal Justice Studies considered that this would be appropriate in light of article 8 of the ECHR. The National Crime Agency agreed, noting that where the patient is not the suspect this might lead to the voluntary handing over of medical records, negating the need for a warrant.

12.56 The Bar Council and the CBA foresaw, at least in theory, a significant risk of tipping-off and destruction of relevant material were a non-suspect to have the right to be informed of the warrant prior to its execution. On the other hand, where there is no such risk, the sensitivity of the material is such that the non-suspect ought ordinarily to have the right to object.

12.57 The Bar Council and the CBA suggested tentatively that one possible solution might be for the default position to be notification, but to allow for the court to dispense with notification (on an application without notice) if a sufficiently strong justification can be shown, for example where there is a real risk of tipping off or destruction of material, sufficient to outweigh the patient's privacy.

12.58 The Magistrates Association argued that it should not just be the person who is subject to a warrant whose views are taken into account, but any patients whose records may be accessed, especially as they will not be aware of an investigation. The Magistrates Association wondered whether it would be possible to allow medical records in those exceptional circumstances to be within the scope of search warrants but a process be put in place by which the detail of the records cannot be accessed without permission from the respective patient. Investigators could therefore access the meta-data of name and contact details without express permission, but for the most private medical/counselling details, a further application process would be necessary.

12.59 Six consultees disagreed with the notification of non-patient suspects. Professor Richard Stone considered that, in principle, notice should be given, however this could be very cumbersome in practice and lead to significant delays. The Justices' Clerks' Society saw difficulties in informing persons (who are not suspects) about proposed searches and did not think this appropriate.

12.60 Dijen Basu QC did not consider that it is practicable in every case to require that every patient have the right to make representations before a warrant or production order is sought, or indeed when the material is being sifted. The Metropolitan Police Service ("MPS") pointed out that the police may not know the identity of those whose medical records are on

---

[41] Council of Her Majesty's Circuit Judges; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; Northumbria Law School Centre for Evidence and Criminal Justice Studies; Bar Council & Criminal Bar Association; National Crime Agency.

premises before the search warrant is executed. The FCA remained concerned about the risk of tipping-off.

The treatment of human tissue and fluid

12.61 The majority of consultees agreed that a similar uniform rule ought to exist in respect of human tissue or tissue fluid under section 11(1)(b) PACE 1984.[42] The CPS saw the logic of extending the rules discussed above as the same public interest arguments apply.

Analysis

A uniform rule

12.62 On reflection, we see force in the comments made by the FCA that a uniform scheme of identical statutory access conditions is not in itself desirable. Uniformity should not be pursued for its own sake. This is for the same reason that we were dissuaded from creating uniform statutory safeguards across all criminal investigation warrants. For one, the language could not be harmonised. For example, the access conditions for a production order under the Terrorism Act 2000 differ in crucial respects from those under PACE as "the order is sought for the purposes of a terrorist investigation".[43]

12.63 More fundamentally, a uniform approach is not appropriate as the strength of the arguments for and against access to confidential personal and counselling records varies depending on the type of investigation. Each statutory regime, and potential modification of the rules which apply to personal records, would have to be considered on its own terms to determine whether such reform would be desirable. In some cases, the protection of confidential personal records would be strengthened, in other cases it would be weakened.

12.64 We are fortified in this view following a meeting with the UK Caldicott Guardian Council to discuss the protection afforded to confidential medical records.[44] We were cautioned against pursuing a "one-size-fits-all" model as the justifications for the level of protection afforded to personal records will vary.

12.65 Another problem with seeking a uniform rule is drawing a meaningful boundary as to where such a rule ends: the boundary between criminal and civil or regulatory provisions can be an elusive one. If a uniform rule in respect of criminal investigations was introduced, agencies with a dual role investigating criminal and civil matters, such as the FCA and Competition and Markets Authority, could end up with incoherent enforcement regimes.

12.66 While identical access conditions may seem desirable, they may fail to account for nuances within particular enforcement regimes. For example, the NHSCFA, which investigates fraud within the NHS, will invariably be seeking confidential medical records as evidence of criminality. A comparison can be made with HMRC, who will usually be seeking business records which constitute special procedure material under section 14 of PACE. This would

---

42 Professor Richard Stone; Crown Prosecution Service; Council of Her Majesty's Circuit Judges; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Dijen Basu QC; Bar Council & Criminal Bar Association; National Crime Agency.

43 Terrorism Act 2000, sch 5, para 6(2)(a).

44 UK Caldicott Guardian Council meeting (12 February 2020). Meeting minutes can be viewed at https://www.ukcgc.uk/news/2020/02/council-meeting.

seem to be the reason why an exception to the prohibition on seeking excluded and special procedure material under a pre-PACE enactment has been created for HMRC.[45]

12.67 In summary, we consider that, while uniform safeguards may be desirable in principle, each regime must be carefully considered. In the next section, we consider specifically the PACE regime, as it is the regime of which we received the most analysis from consultees.

Should confidential personal records be obtainable under PACE?

12.68 In our view, the regime to seek access to confidential personal records under the second set of access conditions in schedule 1 to PACE is too restrictive, thereby impeding serious criminal investigations. This conclusion is borne out by case law[46] and fortified by the anonymised police investigation referred to at paragraphs 12.42 to 12.44 above, illustrating that the problem remains a significant one.

12.69 We consider below two separate issues around the second set of access conditions. The first issue relates to the way the conditions operate, and the second relates to the underlying policy.

12.70 As regards the first issue, there are three problems with the way that the second set of access conditions work at present. First, the requirement in paragraph 3(b) of schedule 1 to PACE that there be an appropriate pre-PACE power is impractical. An investigator must trawl through previous search warrant provisions to find one which may be appropriate.[47] We have heard anecdotally that some law enforcement agencies have had to spend time and money obtaining independent legal advice to try and ascertain if a warrant could have been sought for their investigation to satisfy this access condition. While certain Criminal Procedure Rule forms provide a note with a non-exhaustive list of potential provisions,[48] each case will require careful analysis on its own facts, as the issue of a warrant under the pre-PACE power must "have been appropriate".[49]

12.71 Secondly, we regard the fact that the availability of confidential personal records in criminal investigations turns on the existence of pre-PACE power under which the material could have been sought to be an arbitrary rule. We understand that the underlying policy is to preserve the position prior to the enactment of PACE, however, we consider that a more principled set of access conditions should apply focused on the value and relevance of the material.

12.72 Thirdly, the second set of access conditions do not themselves require the offence being investigated to be indictable, the material to be relevant evidence or the order or warrant to be in the public interest. These are significant safeguards which are not present due to the way in which the conditions currently operate, which is in effect a saving provision for pre-PACE provisions. Nonetheless, as a court must exercise its discretion whether to issue an order or warrant compatibly with human rights, the court will be engaged in a similar

---

45 Police and Criminal Evidence Act 1984 (Application to Revenue and Customs) Order 2015 (SI 2015 No 1783), art 6.

46 See paragraphs 12.17 to 12.22 above.

47 For a discussion of the problem see Alex Davidson, "Production Orders: R (BBC) v Newcastle Crown Court (Case Comment)" [2020] *Criminal Law Review* 247, 252.

48 See page 10 of the "Application for a search warrant under PACE schedule 1, paragraph 12, CrimPR 47.30", available at http://www.justice.gov.uk/courts/procedure-rules/criminal/forms.

49 Police and Criminal Evidence Act 1984, sch 1, para 3(c).

exercise to that which would be conducted when considering the public interest.[50] Furthermore, paragraph 3(c) of schedule 1 to PACE requires the court to consider whether the issue of the warrant is "appropriate", which is likely to encompass these matters.[51]

12.73 As regards the second issue, we consider that the underlying policy in respect of the high level of protection afforded to confidential personal records is highly questionable. The provisions relating to excluded material and special procedure material were added to the Police and Criminal Evidence Bill following a high volume of anxiety expressed by doctors, journalists and others;[52] it was originally envisaged that excluded material would not be obtainable at all.[53] Against this approach it was argued that:

> The line which ought to be drawn is not that which has been drawn in these amendments —which is that confidential information in files that are held by people in certain privileged occupations is exempt. It does not matter how serious the offence is or what the consequences will be if the police do not get that information: the Government say that that material will be exempt. That is not a fair balance. It is one of the rare issues in this Bill where the balance has been drawn against the police to an unacceptable extent. That has been done because the Government have given in to the campaign that was engineered by the press.[54]

12.74 The requirement that there be an appropriate pre-PACE power, and the lack of such powers has resulted in a near total prohibition on obtaining confidential personal records. For this reason, we consider that there is a strong argument that the circumstances under which PACE permits access to confidential personal records should be amended to redress the balance.

12.75 A number of other reasons have led us to this conclusion. We have examined the current mechanisms to obtain such material and concluded that they are unsatisfactory. There are two principal mechanisms. The first is to exercise other powers of production or seizure under PACE, and the second is to seek voluntary production (including under a "data sharing arrangement"). We address each of these in turn below.

12.76 As mentioned above, it may be possible for investigators to obtain confidential personal records under other powers in PACE. These are the powers of production or seizure under section 18, 19, 20 or 32 of PACE.[55] These routes, however, do not necessarily involve judicial oversight. The provisions also require as a pre-condition either grounds for arrest, or lawful entry onto premises. A health care professional holding the records will not necessarily be liable to arrest. The police may also be unable to effect lawful entry onto premises.

12.77 Another way to seek to obtain the material is by seeking voluntary production from (1) a patient; (2) the health care professional; or (3) another agency who can exercise compulsory

---

50 Alex Davidson, "Production Orders: R (BBC) v Newcastle Crown Court (Case Comment)" [2020] *Criminal Law Review* 247, 252.

51 Police and Criminal Evidence Act 1984, sch 1, para 3(c).

52 *Hansard* (HC), 3 May 1983, vol 42, col 117.

53 *Hansard* (HC), 3 May 1983, vol 42, cols 39 to 40 and 101 to 102.

54 *Hansard* (HC), 3 May 1983, vol 42, col 85.

55 We provide a description of these provisions at paragraph 12.194 below.

powers in respect of the material. The circumstances in which requests may be made vary, however, broadly speaking, we have identified two methods: making informal requests or under what we have termed a data sharing arrangement. Data sharing arrangements have no legal basis; rather we use this term to describe a more formalised means of requesting voluntary production.

12.78 The first option to seek to obtain medical records will therefore be for an investigator to request voluntary production from the patient or other person whom the medical records concern. The shortcomings of this method are clear: the patient may be unknown, as was the case in *Kellam*, an unwilling suspect, like in *Singleton,* or deceased, which is the case in the anonymised example given to us by a police force.

12.79 The second option is for the investigator to request voluntary production from the health care professional or organisation that holds the patient records. This is the most frequent avenue by which law enforcement agencies obtain medical records. On a case by case basis, an investigator without a production order, warrant or other compulsory power of production may ask for a patient's health records to be disclosed voluntarily under paragraph 10 of schedule 1 to the Data Protection Act 2018 (which provides an exception to the prohibition on processing sensitive personal data where this is necessary for the "prevention or detection of an unlawful act").

12.80 As alluded to above, law enforcement agencies may also enter into a formal or informal data sharing arrangement with health care professionals or other agencies. For example, guidelines published by the UK Caldicott Guardian Council in collaboration with the National Crime Agency indicate a formal data sharing arrangement to assist the police in tracing missing persons.[56]

12.81 While health professionals have the power to disclose personal records to the police, there is no obligation to do so. Disclosure will breach the common law duty of confidence unless the patient consents. A breach of confidence may also be justified if it is in the public interest. General guidance on public interest disclosures for health professionals is provided by the British Medical Association ("BMA"):[57]

> A disclosure in the public interest is a disclosure that is essential to prevent a serious threat to public health, national security, the life of the individual or a third party, or to prevent or detect serious crime. This includes crimes such as murder, manslaughter, rape, treason, kidnapping and abuse of children or other vulnerable people. Serious harm to the security of the state or to public order and serious fraud will also fall into this category. In contrast, theft, minor fraud or damage to property, where loss or damage is less substantial, would generally not justify the breach of confidence necessary to make the disclosure.

12.82 For doctors, the General Medical Council (GMC) provides more specific guidance on when a disclosure may be justified in the public interest:[58]

---

56 Available at https://www.ukcgc.uk/news/2019/5/22/sharing-information-with-the-police-to-help-trace-missing-persons-the-process-considerations-and-legal-basis.

57 British Medical Association, *Access to Health Records* (November 2019) p 8.

58 General Medical Council, *Confidentiality: good practice in handling patient information* (25 May 2018) paras 64 and 65.

> If it is not practicable or appropriate to seek consent, and in exceptional cases where a patient has refused consent, disclosing personal information may be justified in the public interest if failure to do so may expose others to a risk of death or serious harm. The benefits to an individual or to society of the disclosure must outweigh both the patient's and the public interest in keeping the information confidential. … Such a situation might arise, for example, if a disclosure would be likely to be necessary for the prevention, detection or prosecution of serious crime, especially crimes against the person. When victims of violence refuse police assistance, disclosure may still be justified if others remain at risk, for example from someone who is prepared to use weapons, or from domestic violence when children or others may be at risk.

12.83 Consent of the patient may be impossible if the patient's identity is unknown, or the patient is dead. While disclosure without consent may be justified in the public interest, there is no obligation on the doctor to disclose patient records. The doctor may prefer not to disclose without a court order, even in the face of a serious crime, as was the case in *Kellam*.

12.84 We also agree with the Northumbria Law School Centre for Evidence and Criminal Justice Studies that voluntary production may damage the relationship of trust between a professional and their patient or client and cause anxiety on the part of the professional due to the possibility of legal action. Additionally, as we have seen from the anonymised example provided by a police force, the professional may in fact be the suspect, meaning that a request for production cannot be confidently made.

12.85 While data sharing arrangements may bring about greater clarity and consistency in practice, such arrangements may only address isolated reasons for which investigators seek access to medical records. Nor can data sharing arrangements completely overcome the problems identified in paragraphs 12.83 and 12.84 above.

12.86 The third and final option of which we have been made aware is that an investigator may seek to enter into a data sharing arrangement with HM Senior Coroner or the Care Quality Commission (CQC), both of whom have statutory powers to compel the production of documents.[59] However, this too is not a satisfactory solution to the wider problem. These production powers are narrow in their ambit and so will be applicable in limited circumstances. The organisation concerned can only compel the production of documents for the purpose of its regulatory or other functions. It follows that an organisation is unlikely to use its powers to compel the production of medical records on behalf of an investigator, but rather disclose to an investigator those documents already obtained as part of an ongoing investigation. This method therefore requires a pre-existing investigation with sufficient overlap that relevant medical records have been obtained and for the organisation to be comfortable disclosing the records to a law enforcement agency.

12.87 Where the holder of the records is a suspect, the same problem arises as identified at paragraph 12.84 above: the power relies on the goodwill and honesty of the organisation to comply fully with the request, which they may not wish to do where the material would inculpate them in serious criminality. While the CQC has powers to enter regulated premises and seize documents,[60] this is only exercisable where it considers it necessary or expedient

---

59 Coroners and Justice Act 2009, sch 5; Health and Social Care Act 2008, s 64.

60 Health and Social Care Act 2008, ss 62 to 63. Provisions which empower a coroner, when authorised by or on behalf of the Chief Coroner, to enter land, search and seize material have not been brought into force: see Coroners and Justice Act 2009, sch 5, paras 3 to 5.

to do so for the purpose of its regulatory functions.[61] The CQC cannot exercise the powers for the purpose of assisting the police in a criminal investigation. In any event, it is clearly impracticable and undesirable for the investigation of serious crime to require a health and social care regulator to exercise its investigative powers.

12.88 For the reasons above, we have concluded that requesting voluntary production from the person whom the records concern, the holder of the personal records, or another agency with investigative functions, or entering into data sharing arrangements, are not effective solutions to the problems with the second set of access conditions outlined above. To the extent that such methods are practicable, we consider that the question remains whether it would be desirable for there to be a legal mechanism to obtain judicial authorisation to compel production or effect a search of premises where other means have been exhausted or are bound to fail.

12.89 Another reason why we consider that the circumstances under which confidential personal records are obtainable under PACE should be amended is that, since the enactment of PACE, the introduction of the Criminal Procedure and Investigations Act 1996 has led to the formalisation of the duty to pursue all reasonable lines of enquiry. This means that an investigator must take reasonable steps to obtain relevant third-party material, which may include protected material.[62] Accordingly, an investigator should consider recourse to investigative powers, such as production orders or search warrants, in order to view relevant material and discharge their disclosure obligations. This duty forms part of a broader duty to guarantee a fair trial;[63] in some cases, medical records may form exculpatory material. The current position therefore impedes law enforcement agencies in pursuing all reasonable lines of enquiry and identifying potentially exculpatory material.

12.90 We have also taken into account the fact that, contrary to what we understood the position to be from stakeholders when we published our consultation paper, it is in fact common for the police to seek access to health records.[64] According to Dr Chris Bunch, Chair of the UK Caldicott Guardian Council, requests are made by law enforcement agencies to medical professionals for confidential patient records very frequently. These requests cover investigations including offences against the person and child abuse, which fall within the scope of the investigative powers under PACE.

12.91 We also consider that providing a clear avenue to access confidential personal records under PACE would lead to a more consistent practice and better protection. Dr Chris Bunch described the practice of law enforcement agencies as inconsistent, with some requests clearly fishing expeditions. He cited one case in which a police officer picked up case notes unannounced and said they were taking them away. A member of the UK Caldicott Guardian Council considered that approximately 10% of requests from law enforcement agencies met the requisite threshold for disclosure.

12.92 In our view, there should be a clear set of access conditions requiring judicial authorisation through which to obtain confidential personal records. This would remove some of the

---

61 Health and Social Care Act 2008, s 62(1).

62 *R (BBC) v Newcastle Crown Court* [2019] EWHC 2756 (Admin), [2020] 1 Cr App R 16 at [28].

63 Alex Davidson, "Production Orders: R (BBC) v Newcastle Crown Court (Case Comment)" [2020] *Criminal Law Review* 247, 251.

64 British Medical Association, *Access to Health Records* (November 2019) p 8.

uncertainty and inconsistency under the current system and encourage requests to be more specific and properly justified.

12.93 In addition, a more consistent practice and better protection may flow from decision making moving in some instances to a judge. We were informed by the UK Caldicott Guardian Council that there are approximately 18,000 Caldicott Guardians in the UK. The role does not require formal training. In our view, a judge is better placed to determine whether confidential personal records should be accessed. Concerns regarding the categories or amount of material being sought, which a data holder would be able to raise were a request made, could be incorporated into any procedure which is devised.

12.94 We have also taken into account anecdotal evidence from police forces that search warrants under section 8 of PACE have been used erroneously to obtain personal records in criminal investigations. Such innocent failures to recognise that such records are excluded material indicate that investigators and judges are unaware that police do not have this power. This clearly jeopardises criminal investigations and makes the police susceptible to civil litigation.

12.95 It is for all the reasons above that we consider that there is a powerful argument that confidential personal records should be obtainable under PACE in different circumstances to those in which they are available now. We are conscious that the definition of personal records under section 12 of PACE covers more than just medical records on which we have focused, such as documents relating to spiritual counselling. We do not consider that the nature of these other types of personal records undermines our analysis. We do, however, accept below that more detailed consultation would be necessary prior to any law reform being taken forward.

When should personal records be obtainable pursuant to a search warrant under PACE?

12.96 We turn now to consider in what circumstances a constable should be permitted to obtain personal records pursuant to a search warrant under PACE. In our consultation paper, we provisionally proposed that, where medical or counselling records are central to the issues being investigated, there should be tightly circumscribed exceptions to a general prohibition on obtaining personal records under a search warrant. We agree with consultees that the phrase "central to the issues being investigated" is not free from ambiguity. It also fails to take into account the gravity of the alleged offence, a point that was made during a discussion with the National Data Guardian Panel.[65]

12.97 On careful reflection, we have concluded that a public interest test would be a desirable condition. In particular, we see merit in moving confidential personal records into the first set of access conditions, which currently apply to special procedure material, and which are set out in paragraph 2 of schedule 1 to PACE.[66] Under these conditions, material is available under a search warrant if it is relevant, likely to be of substantial value to the investigation, alternative methods of obtaining the material are not possible and its disclosure is in the public interest. We have reached this conclusion for a number of reasons.

12.98 First, the alignment of excluded material and special procedure material has occurred already in the production order and search warrants regime under the Terrorism Act 2000.[67]

---

65 National Data Guardian Panel meeting (18 December 2019).

66 We set out the first set of access conditions at paragraph 13.11 below.

67 Terrorism Act 2000, sch 5, para 5.

The access conditions under which confidential personal records can be sought under the Terrorism Act 2000 are broadly modelled on the first set of access conditions under PACE.[68] Given that the investigations for which confidential personal records may be sought under PACE include very serious offences against the person, we consider that there is an equally strong public interest in there being a similar power in PACE through which to seek access to the material.

12.99 Secondly, many consultees agreed that a public interest test would be appropriate. For example, such a test was advocated by the FCA. As they note, the prohibition on obtaining personal records reflects the rights under article 8 of the ECHR, which are qualified rights. This can be compared to the absolute prohibition on obtaining legally privileged material. It was said that this important distinction would be better reflected in the law with this amendment. Those present during the National Data Guardian Panel meeting[69] which we attended also were not averse to a public interest test, nor were members with whom we met on the UK Caldicott Guardian Council.[70]

12.100 Discussions with the British Medical Association's medical ethics department after the close of our consultation period seemed to suggest that it viewed a public interest test as acceptable, provided the GMC's and BMA's ethical guidance is taken into account, in particular the threshold for disclosures in the public interest.

12.101 Similar discussions with the General Medical Council suggested that it saw benefits to this approach. However, the GMC observed that, while a doctor may not be best placed to assess the relevance of the information to a criminal investigation, equally judges are not best placed to assess the other factors that might weigh against disclosure. These factors would be those which affect both the public and the patient's interest in keeping the information confidential.

12.102 In our view, on balance, a Circuit judge, as a legally trained judicial officeholder, would still be better placed to make a decision properly apprised of the reasons which militate against disclosure. In reaching this view, we have taken into account the observation made at paragraph 12.93 above that the level of training undertaken by a Caldicott Guardian varies.

12.103 Thirdly, a public interest test allows for an open-textured analysis which reflects the fact-sensitive nature of criminal investigations. There will of course be circumstances where confidential personal records should not be disclosed. A public interest test would allow the courts to take account of the case as a whole and properly distinguish those circumstances where confidential personal records should be accessed from those in which they should not. This would include taking into account the public interest in maintaining confidential medical care and avoiding what is termed "negative health seeking behaviour" whereby the potential for court orders or warrants risks dissuading individuals from accessing health care services. As discussed above, in our view, a Circuit judge is properly placed to weigh these interests.

12.104 We have considered whether incorporating a public interest test for medical records would blur the distinction between excluded material and special procedure material. However,

---

68 Terrorism Act 2000, sch 5, para 6.

69 National Data Guardian Panel meeting (18 December 2019).

70 UK Caldicott Guardian Council meeting (12 February 2020). Meeting minutes can be viewed at https://www.ukcgc.uk/news/2020/02/council-meeting.

because a public interest test gives rise to such an open-textured and fact-sensitive analysis, we have concluded that a public interest test, and the courts' approach to considering interferences with Convention rights, would ensure that the importance of confidentiality associated with personal records is accounted for. Therefore, the courts may well consider that the public interest in the confidentiality of medical records is far greater than the confidentiality in special procedure material.

12.105 Fourthly, we note BMA[71] and GMC[72] guidance, which indicates that health professionals and doctors currently consider whether disclosure of confidential personal records is in the public interest when requested to disclose them. We regard a Circuit judge as better suited to weigh up the competing public interests in criminal investigations. We note in particular that where a record is held on a confidential basis, the holder may be unwilling to disclose it for fear of being sued for breach of confidence by the person from whom they received it. This problem is alleviated by moving the decision-making process into the hands of a judge.

12.106 Fifthly, the wishes of the person who the material concerns, if known, can be factored into any analysis.[73] We accept that notifying patients and receiving representations from them could be cumbersome. Taking into account consultees' responses, we consider that a system of patient notification may be impracticable in some cases.

12.107 Sixthly, we consider that the scheme under the first set of access conditions would operate proportionately in practice. Paragraph 2(b) of schedule 1 to PACE requires that other methods of obtaining the material have been tried without success or have not been tried because it appeared that they were bound to fail. In practice, requests will therefore likely be made in the first instance to the medical professional, health centre or trust. Where these are exhausted, a production order may be applied for. Were the conditions under paragraph 14 of schedule 1 to PACE met, for example if the person holding the records was a suspect, a search warrant could be applied for instead. Accordingly, we do not consider that the amendment would lead to a proliferation of warrants to search for and seize confidential personal records being issued. A judge should also be able to spot potential fishing expeditions.

12.108 We agree with consultees that the same approach ought to be adopted in respect of human tissue and tissue fluid taken for diagnostic purposes or health treatment and held in confidence, as the underlying policy arguments have equal application.

12.109 While we consider the case for reform to be a strong one, for the reasons set out at paragraph 12.6 above, we do not make a firm recommendation for reform. Modification of the access conditions in PACE would also change the law for production orders, as they share the same access conditions. Production orders are obtained far more frequently than search warrants as they are the default power under schedule 1 to PACE. To change the law only in respect of search warrants would render the law complex and incoherent.

12.110 Coupled with the above, our focus has been on medical records. Counselling and spiritual records also fall within the definition of personal records; however, we have not received

---

71 British Medical Association, *Access to Health Records* (November 2019) p 8.

72 General Medical Council, *Confidentiality: good practice in handling patient information* (25 May 2018) paras 64 and 65.

73 *R (BBC) v Newcastle Crown Court* [2019] EWHC 2756 (Admin), [2020] 1 Cr App R 16 at [54].

enough evidence regarding how changes would affect these services. More generally, we consider that further consultation is needed with special interest groups.

Recommendation 42

12.111 We recommend that the Government considers whether the law governing access to confidential personal records, human tissue and tissue fluid under the Police and Criminal Evidence Act 1984 strikes the right balance between (1) the prevention and investigation of serious crime; and (2) the protection of the confidentiality of health and counselling records, and whether the law ought to be reformed.

CONFIDENTIAL JOURNALISTIC MATERIAL

The current law

The definition of "journalistic material" and "in confidence"

12.112 Journalistic material is defined in section 13 of PACE as material which is in the possession of a person who has acquired or created it for the purposes of journalism. Such material constitutes "special procedure material" under section 14(1)(b) of PACE.

12.113 Where journalistic material consists of documents or records and is held in confidence, the material is elevated to the category of "excluded material" under section 11(1)(c) of PACE. Under section 11(3) of PACE, a person holds journalistic material in confidence if:

(1) the person holds it subject to:

(a) an express or implied undertaking to hold it in confidence; or

(b) a restriction on disclosure or an obligation of secrecy contained in any enactment, including an enactment contained in an Act passed after PACE; and

(2) it has been continuously held (by one or more persons) subject to such an undertaking, restriction or obligation since it was first acquired or created for the purposes of journalism.

The definition of "for the purposes of journalism"

12.114 A key ingredient for material to be classified as journalistic material under PACE is that it must have been acquired or created "for the purposes of journalism". Therefore, for the purposes of PACE, the question is not one of status (ie whether a person is a journalist) but one of *purpose*.

12.115 PACE does not provide a statutory definition of the phrase "for the purposes of journalism". Nor is the phrase defined in the other statues in which it appears.[74] The Supreme Court

[74] See, for example, Crime (Overseas Production Orders) Act 2019, s 12; Data Protection Act 2018, s 174(1)(a); Investigatory Powers Act 2016, s 264(2); Tax Collection and Management (Wales) Act 2016, s 98(2); Police Act 1997, s 100. The Crime and Courts Act 2013, s 42(7) defines "news-related material" as (1) news or information about current affairs; (2) opinion about matters relating to the news or current affairs, or (3) gossip about celebrities, other public figures or other persons in the news.

considered the phrase in the context of the Freedom of Information Act 2000 in *Sugar v British Broadcasting Corporation*,[75] favouring a narrow construction.

> Information should only be found to be held for the purposes of journalism … if an immediate object of holding the information is to use it for one of those purposes.[76]
>
> The central question to be asked … will be … whether there remains any sufficiently direct link between the BBC's continuing holding of the information and the achievement of its journalistic purposes.[77]

12.116 Lord Neuberger MR, giving judgment in the same case earlier in the Court of Appeal, held:

> The question whether information is held for the purposes of journalism should thus be considered in a relatively narrow rather than a relatively wide way.[78]

12.117 The phrase "for the purposes of journalism" was also considered in the Leveson Inquiry into the culture, practices and ethics of the British press ("the Leveson Inquiry"). Leveson LJ recommended in the Leveson Inquiry report that:

> The Home Office should consider and, if necessary, consult upon … whether PACE should be amended to provide a definition of the phrase "for the purposes of journalism" in s13(2) [of PACE].[79]

The accessibility of journalistic material

12.118 As excluded material, confidential journalistic material is treated similarly to confidential personal records.

12.119 Any search warrant provision passed before PACE under which a search warrant could be authorised to search for journalistic material (confidential or otherwise) can no longer be used to search for journalistic material.[80] For example, a search warrant could have been issued to search for journalistic material under section 9(1) of the Official Secrets Act 1911 where an offence under that Act was suspected.

12.120 Search warrants under section 8 of PACE may not be issued in respect of journalistic material.[81] Nor may journalistic material be seized in the course of a search.[82] An exception to these exemptions is provided by the seize and sift powers under CJPA, which requires excluded material to be sifted off-site and returned.

---

75 *Sugar v British Broadcasting Corporation* [2012] UKSC 4, [2012] 1 WLR 439. Leveson LJ stated that he saw no reason why the construction of the phrase "for the purposes of journalism" by the Supreme Court ought not be different in the context of the Police and Criminal Evidence Act 1984.

76 *Sugar v British Broadcasting Corporation* [2012] UKSC 4, [2012] 1 WLR 439 at [67] by Lord Phillips.

77 *Sugar v British Broadcasting Corporation* [2012] UKSC 4, [2012] 1 WLR 439 at [106] by Lord Brown.

78 *Sugar v British Broadcasting Corporation* [2010] EWCA Civ 715, [2010] 1 WLR 2278 at [55]. Cited with approval by *Sugar v British Broadcasting Corporation* [2012] UKSC 4, [2012] 1 WLR 439 at [84] by Lord Walker.

79 The Leveson Inquiry, vol 4, para 9.11.

80 Police and Criminal Evidence Act 1984, s 9(2).

81 Police and Criminal Evidence Act 1984, s 8(1)(d).

82 Police and Criminal Evidence Act 1984, s 8(2).

12.121 Non-confidential journalistic material can be obtained under PACE by applying for a production order or search warrant under the first set of access conditions. Confidential journalistic material requires an application under the second set of access conditions. As discussed above, the effect of the second set of access conditions is that a constable can only apply for a production order (or search warrant) if they can direct the issuing authority to a pre-PACE search warrant provision under which they could have appropriately applied for a warrant for excluded material.

12.122 As in the case of confidential personal records, there are some investigative powers, enacted after PACE, which treat journalistic material, including that held in confidence, in a different, less restrictive way. It is also worth noting that the powers of seizure and production under sections 18, 19, 20 and 32 of PACE provide no exclusion for journalistic material.[83]

The consultation paper

12.123 As with medical records, we considered in our consultation paper that there should be a single rule for all cases. We observed that most warrants for the investigation of serious crime are issued under section 8 of PACE, which does not permit the search or seizure of confidential journalistic material except in highly exceptional circumstances. For this reason, we considered that it made sense for the standard for less serious or more specialised investigations under post-PACE regimes to be raised to match that in PACE, rather than for the protection under PACE to be diluted. We were also unable to see why the standard in financial and similar investigations under powers enacted after PACE should be lower.

12.124 We observed that there are several arguments for the protection of journalistic material, first and foremost being the importance of the freedom of the press. Any limitation imposed on the protection afforded to journalistic material risks a "chilling effect"[84] and warrants the highest level of scrutiny in the view of the European Court of Human Rights ("ECtHR").[85]

12.125 The ECtHR has repeatedly emphasised that the protection of journalistic sources is one of the cornerstones of freedom of the press.[86] The importance of the protection is further recognised in domestic legislation in section 10 of the Contempt of Court Act 1981 and section 12 of the Human Rights Act 1998. Confidential journalistic material therefore requires particular protection.

12.126 Accordingly, we provisionally proposed that:

(1) there should be a uniform rule for the availability of search warrants in respect of confidential journalistic material, irrespective of the particular power under which the warrant is sought and the identity of the person applying for or executing the warrant; and

---

83 We summarise these provisions at paragraph 12.194 below.

84 *Ashworth Hospital Authority v MGN Ltd* [2002] UKHL 29, by Lord Woolf CJ at [61].

85 *Goodwin v United Kingdom* (1996) 22 EHRR 123.

86 *Roemen and Schmit v Luxembourg* (2003) App No 51772/99 at [46]; *Saint-Paul Luxembourg SA v Luxembourg* (2013) App No 26419/10 at [49].

(2) that rule should provide that confidential journalistic material should be excluded from the scope of search warrants in all cases, whatever the statutory source of the power to issue a search warrant.

12.127 Importantly, we invited consultees' views on whether there should be any exceptions to this exclusion and, if so, what those exceptions should be.

12.128 We also provisionally proposed that the statutory regime under schedule 5 to the Terrorism Act 2000 ought not to be amended. This was owing to the judgment in *Malik*,[87] which suggested to us that amending the Terrorism Act 2000 would involve interrupting a carefully crafted statutory regime for investigating, detecting and prosecuting terrorism offences.

Consultation responses

12.129 Nineteen consultees[88] answered this question.

A uniform rule

12.130 Seventeen consultees[89] agreed that there should be a uniform rule for the availability of search warrants in respect of confidential journalistic material. Dijen Basu QC stated that there should be a uniform rule for search warrants *and production orders* in respect of confidential journalistic material.

12.131 The FCA opposed the introduction of a uniform rule, for the reasons they gave at paragraph 12.34 above. In short, the relevance of confidential journalistic material to differing types of investigations may vary considerably. At present, there is no restriction under the Financial Services and Markets Act 2000 on searching for journalistic material. In the circumstances, the FCA were opposed to the imposition of additional statutory restrictions on the scope of their search powers. In their view, the addition of specific additional exemptions to their warrant regime could create unnecessary difficulties.

A general prohibition on access in all cases

12.132 There was little support[90] among consultees for a uniform rule that confidential journalistic material should be excluded from the scope of search warrants in all cases.

12.133 The News Media Association ("NMA") did support such a complete exclusion. They argued that this should apply irrespective of the particular power under which the warrant is sought, the identity of the person applying for or executing the warrant and the investigating

---

87 *R (Malik) v Manchester Crown Court* [2008] EWHC 1362 (Admin), [2008] 4 All ER 403.

88 Crown Prosecution Service; Professor Richard Stone; HM Council of District Judges (Magistrates' Courts); Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Guardian News and Media; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; News Media Association; The Law Society; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; Bar Council & Criminal Bar Association; Metropolitan Police Service; National Crime Agency; Serious Fraud Office; Financial Conduct Authority.

89 Professor Richard Stone; HM Council of District Judges (Magistrates' Courts); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Guardian News and Media; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; News Media Association; The Law Society; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; Bar Council & Criminal Bar Association; Metropolitan Police Service; National Crime Agency.

90 News Media Association; Guardian News and Media; Professor Richard Stone.

authority, to avoid any potential bypass through the use of other statutory powers. Their justification centred on the right to freedom of expression, the importance of freedom of the press and the concomitant importance of the protection of journalistic sources.

12.134 A significant number of consultees[91] disagreed with a rule that exempts confidential journalistic material in all cases.

12.135 The Birmingham Law Society ("BLS") considered that a complete exclusion would fail to cater for potential unforeseeable circumstances. Similarly, Dijen Basu QC considered that there will be serious cases in which it is necessary, exceptionally, to gain access to such material.

12.136 Dijen Basu QC also suggested that, if warrants and production orders can no longer be sought for confidential material, this will make the use of post-arrest searches under sections 18 and 32 of PACE more likely in cases where confidential journalistic material is relevant and important.

12.137 The Bar Council and the CBA regarded our position as inconsistent as we had proposed to retain the power to obtain confidential journalistic material under schedule 5 to the Terrorism Act 2000. They pointed out that investigations under PACE may concern cases of murder, rape or serious offences against children.

12.138 The SFO, opposing the proposal, noted again that this proposal might frustrate their power to seize confidential journalistic material under a warrant. In addition, the proposal might remove such material from the ambit of their production notices due to the drafting of section 2 of the CJA. They argued that Parliament has purposely not extended such safeguards for journalistic material to their regime and that the current safeguards provide a well-balanced statutory scheme.

12.139 A number of suggested exceptions were put forward. The National Crime Agency considered that there should be an exception whenever such material is needed because it is central to the criminality being investigated. In their view, this exception should be available in all criminal investigations.

12.140 The Bar Council and the CBA suggested that such material should be subject to a proportionality test, to be applied by a Circuit judge rather than a magistrate.

12.141 The FCA strongly opposed the proposal that there be a blanket exemption for confidential journalistic material. They proposed the creation of a statutory test along the lines applied in *Malik*[92] under the Terrorism Act 2000. The test should balance the weight and nature of the right interfered with against the degree to which the order sought has a clear and compelling justification. As set out in the scenarios in paragraph 10.53 above, the FCA envisaged circumstances in which there may be clear and compelling reasons to seek a warrant for "purportedly" journalistic material where there is a danger that it might be destroyed or tampered with. The FCA also considered that this should operate in the alternative or in addition to the iniquity exception.

---

91 Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Dijen Basu QC; Bar Council & Criminal Bar Association; Metropolitan Police Service; National Crime Agency; Serious Fraud Office; Financial Conduct Authority.

92 *R (Malik) v Manchester Crown Court* [2008] EWHC 1362 (Admin), [2008] 4 All ER 403.

12.142 The BLS suggested that confidential journalistic material should be made subject to a search warrant only after a High Court Judge has been satisfied that this is in the interests of (wider) justice, and the journalist has been given an opportunity to make representations.

12.143 The Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate suggested an exception if there is a serious risk of harm to a person. Dijen Basu QC suggested that there ought to be an exception for the investigation of offences which are serious enough to carry a potential life sentence.

Exception to the prohibition on access in terrorism cases

12.144 The majority of consultees[93] agreed that the statutory regime under schedule 5 to the Terrorism Act 2000 ought not to be amended. The Law Society considered that terrorism investigations are obviously of a different nature to other investigations, and that the specific statutory regime under schedule 5 to the Terrorism Act 2000 had been drafted for that particular purpose and so ought to remain.

12.145 In contrast, the Guardian News and Media ("GNM") considered that the uniform rule should apply to the statutory regime under schedule 5 of the Terrorism Act 2000. They fully supported the Government in its aims of reducing terrorism, however, they had concerns that the Terrorism Act 2000, as it stands, is incompatible with article 10 of the ECHR.

12.146 Accordingly, the GNM submitted that there should be a uniform regime that ensures that journalistic material and journalistic sources have more robust and comprehensive protections than at present, irrespective of whether investigations and proceedings relate to terrorism or any other crime. This would have the benefit of certainty for journalists and their sources, while reducing the risk of potential abuse of the Terrorism Act 2000 by authorities, which is all the more important in the current political and economic climate where the threat to the UK from international terrorism is severe. It was argued by the GNM that there is a very real risk that if proper safeguards are not included certain types of journalism "will die on the vine".

12.147 The NMA argued similarly that the Terrorism Act 2000 and other counter-terrorism legislation should be amended insofar as these provide any lesser degree of protection for journalistic activities, journalistic material and journalistic sources, including the lower access conditions which make it easier to obtain journalistic material. They also noted that the media has strongly objected to any proposals for the reduction of journalistic protections or alignment with the lesser protections under the Terrorism Act 2000.

Analysis

A uniform rule

12.148 As is the case in respect of confidential personal records, we see force in the comments made by the FCA that a uniform scheme of identical statutory access conditions is not in itself desirable. Uniformity should not be pursued for its own sake as the strength of the arguments for and against access to confidential journalistic material varies depending on the type of investigation.

---

[93] Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; The Law Society; Magistrates Association; Dijen Basu QC; Metropolitan Police Service; National Crime Agency.

12.149 To be clear, while uniform safeguards may be desirable in principle, each regime must be carefully considered. For this reason, we once again consider specifically the PACE regime, as it is the regime of which we received the most analysis from consultees.

12.150 As for the Terrorism Act 2000, despite the submissions made by the NMA and the GNM, we remain of the view expressed in our consultation paper that these provisions should not be amended. In our view, the production order and search warrant regime in this Act strikes an appropriate balance between the competing interests at play.

12.151 As an example of such balancing, we note the recent production order applications made by the MPS under the Terrorism Act 2000 for non-confidential journalistic material which was not broadcast relating to interviews with Shamima Begum, who travelled to Syria in 2015, then aged 15, to join ISIS. HHJ Mark Dennis QC, refusing the applications, ruled that there was no pressing social need to override the article 10 rights of the journalists, nor were there reasonable grounds for believing that it was in the public interest for the material sought to be produced.

Should confidential journalistic material be obtainable under PACE?

12.152 With the exception of media organisations, consultation responses indicated clear support that confidential journalistic material should be obtainable under PACE in exceptional circumstances. We acknowledge that the protection of journalistic sources is one of the cornerstones of freedom of the press.[94] We recognise that changes to the level of protection of confidential journalistic material may have a chilling effect on journalism, as journalists, in certain circumstances, will not be able to guarantee to sources that they will remain anonymous.

12.153 Article 10 ECHR, however, is not absolute. We consider there to be strong arguments that there should not be an absolute blanket exemption to obtaining production orders and search warrants for confidential journalistic material under PACE. For one, confidential journalistic material *can* currently be obtained under PACE using pre-PACE powers; in *R (British Sky Broadcasting Ltd) v Central Criminal Court* production orders were sought for journalistic material which included material held in confidence, relying on section 9 of the Official Secrets Act 1911 as the pre-PACE provision.[95]

12.154 In addition, we consider that there will be limited circumstances in which confidential journalistic material will be central to the investigation of serious crime such that the interference with article 10 rights by a production order or search warrant will be justified and proportionate. Moreover, the arguments for making available confidential journalistic material are less compelling than in the context of personal records. We have not been provided with any examples of confidential journalistic material that could not be obtained pursuant to a production order or search warrant, but ought to have been obtainable in order to investigate a criminal offence effectively.

12.155 As with personal records, the problems with the second set of access conditions fall into two categories. First, the requirement in paragraph 3(b) of schedule 1 to PACE that there be an appropriate pre-PACE power is impractical and arbitrary for the reasons set out at paragraphs 12.70 to 12.72 above. In summary, an investigator must trawl through previous

---

94 *Roemen and Schmit v Luxembourg* (2003) App No 51772/99 at [46]; *Saint-Paul Luxembourg SA v Luxembourg* (2013) App No 26419/10 at [49].

95 *R (British Sky Broadcasting Ltd) v Central Criminal Court* [2011] EWHC 3451 (Admin), [2012] QB 785 at [5].

search warrant provisions to find one which may be appropriate. It should be clearer on the face of the statute whether access can be granted. This would be of benefit to both investigators and the holders of information so that they understand clearly in what circumstances the material they hold can be searched for or production requested.

12.156 Secondly, the effect of the second set of access conditions is that there is effectively a blanket exemption for confidential journalistic material, except in cases involving the Official Secrets Acts. It may therefore be argued that the regime is too restrictive, with the potential to impede serious criminal investigations. After all, Parliament has provided multiple powers under PACE through which confidential journalistic material can be obtained,[96] recognising that there are circumstances in which confidential journalistic material ought to be obtainable. Production orders or search warrants may be sought under PACE in relation to offences of murder or serious sexual offences. It is arguable that it should be possible to make an application to access confidential journalistic material in such cases.

12.157 We have also heard anecdotal evidence that post-arrest seizure powers under sections 18 and 32 may be used to obtain confidential journalistic material when the holder of the material is liable for arrest. Although legally permissible under the statute, the exercise of these powers to obtain confidential journalistic material may be regarded as undesirable. Amending the production order and search warrants regime may alleviate the use of these powers as a means to obtain confidential journalistic material and avoid incentivising the misuse of arrest.

12.158 For this reason, we consider that there is an argument that PACE should be amended to permit access to confidential journalistic material in clearer circumstances than it does at present. A number of other reasons, similar to those discussed in respect of personal records, support this position.

12.159 First, the current mechanisms to obtain such material are unsatisfactory. As we have mentioned, one possibility is to exercise powers of production or seizure under section 18, 19, 20 or 32 of PACE.[97] These routes, however, do not necessarily involve judicial oversight, nor will an individual holding the records necessarily be liable to arrest.

12.160 Another way to seek to obtain the material is by voluntary production, which is highly unlikely in relation to confidential journalistic material.

12.161 Secondly, we note again the shifting legislative landscape since the enactment of PACE in 1984 in the form of the CPIA. An investigator must take reasonable steps to obtain relevant third-party material, which may include journalistic material.[98] The current position may therefore impede law enforcement agencies in pursuing all reasonable lines of enquiry and identifying potentially exculpatory material.

12.162 Another reason which may justify confidential journalistic material being obtainable under PACE is the widening pool of material that may be regarded as being acquired or created for the purposes of journalism. The phrase seems wide enough to capture material acquired or

---

96 Police and Criminal Evidence Act 1984, ss 18, 19, 20 and 32. We provide a description of these provisions at paragraph 12.194 below.

97 We summarise these provisions at paragraph 12.194 below.

98 *R (BBC) v Newcastle Crown Court* [2019] EWHC 2756 (Admin), [2020] 1 Cr App R 16 at [28].

created by the burgeoning number of individuals who use the internet and social media platforms to inform others of events. As Article 19 observe:

> In common with many other aspects of modern life, the Internet has transformed the way in which we communicate with one another. Where the printed press and broadcast media were once the main sources of information, the Internet has made it possible for any person to publish ideas, information and opinions to the entire world. In particular, blogging and social media now rival newspapers and television as dominant sources of news and information. Unsurprisingly, these developments have also called into question the very definition of 'journalism' and 'media' in the digital age. It has also raised difficult questions of how the activities of bloggers and 'citizen journalists' can be reconciled to existing models of media regulation.[99]

12.163 This shift from professional to lay journalism would not have been envisaged by Parliament when PACE was enacted in 1984. The consequent expansion of material that may be regarded as journalistic material arguably makes it more important that there is a narrow and exceptional avenue through which confidential journalistic material is obtainable in criminal investigations under PACE.

12.164 On balance, in our view confidential journalistic material should be obtainable under PACE in very limited circumstances, albeit we consider that the case for permitting such access is less compelling than that in respect of confidential personal records. For this reason, we go on to consider in what circumstances confidential journalistic material should be obtainable under PACE.

In what circumstances should confidential journalistic material be obtainable under PACE?

12.165 As with personal records, we consider that there is an argument that alignment with the first set of access conditions might be desirable. These advantages have been set out above in respect of confidential personal records at paragraphs 12.97 to 12.107 above. We make the following additional points.

12.166 First, a uniform scheme for confidential journalistic material, personal records and the other categories of material which will constitute excluded material might be regarded as desirable for the sake of simplicity and clarity. However, we have repeatedly made the point that uniformity should not be pursued for its own sake. Just as there are arguments for having different access conditions for the same material across different regimes, there are arguments for having different access conditions under the same regime for confidential personal records and confidential journalistic material. Accordingly, we do not regard our conclusion at paragraph 12.97 above (that moving confidential personal records into the first set of access conditions would be desirable) to be, without more, a compelling reason to adopt the same position for confidential journalistic material.

12.167 Secondly, in the context of confidential journalistic material, the idea of applying the first set of access conditions to such material had the most support from consultees. In addition, other suggested approaches – such as risk to life and the severity of the sentence – could factor into the court's evaluation when deciding whether to exercise its discretion.

12.168 Thirdly, the first set of access conditions may be said sufficiently to reflect the high importance of confidential journalistic material. The court would no doubt have in mind

---

[99] Article 19, *The Right to Blog* (2013) p 1.

section 10 of the Contempt of Court Act 1981, which emphasises the importance of the protection of journalists' sources, as well as relevant case law. As the Divisional Court observed in the case of *Malik*:

> The importance of the right and the weight of the justification required for an interference that compels a journalist to reveal confidential material about or provided by a source has been frequently stated both in Strasbourg and in our courts. It is sufficient to refer to *Goodwin v United Kingdom* (1996) 22 EHRR 123 at [39] and [40] "protection of journalistic sources is one of the basic conditions for press freedom" and "limitations on the confidentiality of journalistic sources call for the most careful scrutiny by the court"; *Tillack v Belgium* (Application no 20477/05, 27 November 2007) at [53]; *John v Express Newspapers* [2000] 1 WLR 1931 at [27] where the court of appeal said: "Before the courts require journalists to break what a journalist regards as a most important professional obligation to protect a source, the minimum requirement is that other avenues should be explored"; and *Ashworth Hospital Authority v MGN Ltd* [2002] UKHL 29, [2002] 1 WLR 2033 at [61] where Lord Woolf CJ said that disclosure of a journalist's sources has a chilling effect on the freedom of the press and that the court will "normally protect journalists' sources".[100]

12.169 As with confidential personal records, human tissue and tissue fluid, we are unable to make a firm recommendation for reform of the circumstances in which confidential journalistic material is obtainable under PACE.

12.170 For one, modification of the access conditions in PACE would change the position for both production orders and search warrants, as they share the same access conditions. This reasoning applies to other regimes where search warrants are predicated on non-compliance with, or an inability to obtain, an order.[101] We did not consult on changes to production orders. More to the point, production orders are obtained far more frequently than search warrants, as they are the default power, with search warrants obtainable if further conditions are satisfied. Law reform would therefore have profound consequences on the law governing production orders.

12.171 More fundamentally, unlike confidential personal records, we are less convinced that change should be made to the availability of confidential journalistic material given the lack of evidence that we have seen that there is a problem in practice. Reform along these lines would be highly controversial and no doubt cause great concern to the media. Further detailed consultation and consideration must precede any reform.

12.172 The above being said, we consider that there is an arguable case that the law governing access to confidential journalistic material under PACE does not strike the right balance between the prevention and investigation of serious crime and the protection of journalistic sources. As a result, we recommend that the Government considers whether the law ought to be reformed.

---

100 *R (Malik) v Manchester Crown Court* [2008] EWHC 1362 (Admin), [2008] 4 All ER 403 at [45]. See also *Re Fine Point Films' Application for Judicial Review* [2020] NICA 35 at [55].

101 Criminal Justice Act 1987, s 2(3) to 2(5).

Recommendation 43

12.173 We recommend that the Government considers whether the law governing access to confidential journalistic material under the Police and Criminal Evidence Act 1984 strikes the right balance between (1) the prevention and investigation of serious crime; and (2) the freedom of the press and the protection of journalistic sources, and whether the law ought to be reformed.

ABOLISHING THE SECOND SET OF ACCESS CONDITIONS

The current law

12.174 The second set of access conditions under paragraph 3 of schedule 1 to PACE governs access to both excluded and special procedure material when a pre-PACE power exists which could have authorised such access. It is unlikely, if ever, that special procedure material will be obtained under the second set of access conditions given that it can be obtained through the less stringent first set of access conditions.

The consultation paper

12.175 In the consultation paper, we invited[102] consultees' views as to whether the second set of access conditions ought to be abolished. There were three reasons which led us to ask this question.

12.176 First, we considered that, if both confidential medical records and confidential journalistic material were made exempt from disclosure in all circumstances, as they almost are under PACE, the second set of access conditions under schedule 1 to PACE could be abolished without replacement.

12.177 Secondly, discussions with stakeholders suggested that the second set of access conditions is rarely used, and that it could be abolished without adversely affecting law enforcement powers.

12.178 Thirdly, stakeholders reported that they find the second set of access conditions extremely hard to navigate.

12.179 We noted that the second set of access conditions were likely introduced only for the sake of caution, in order to preserve any possibility of obtaining these records which *might* have existed (contingent as they are on the identification of a pre-PACE power which could have authorised access). In our view, it was not entirely clear that the second set of access conditions were necessary, particularly in light of our provisional proposals above. We invited views as to whether the second set of access conditions ought to be abolished.

Consultation responses

12.180 Eighteen consultees[103] answered this question: 13 agreed;[104] and five expressed other views.[105] The majority of consultees agreed that the second set of access conditions should

[102] Consultation Question 46.

be abolished. However, there were differences in opinion as to whether a new set of access conditions should be introduced in its place, and if so what those conditions should be.

12.181 The NMA and GNM considered that the second set of access conditions could be abolished if a new uniform rule were adopted exempting all confidential journalistic material from the scope of all search warrants, irrespective of the source of the power or the identity of the executor. All other consultees, however, considered that there should be a route to access excluded material including confidential journalistic material.

12.182 The CPS noted that the second set of access conditions appears to have been introduced out of caution to preserve access to material which a pre-1984 provision provided for (or where the public interest in the first set of access conditions is not made out). It was said to preserve a not particularly logical set of pre-1984 provisions. In those circumstances, the CPS agreed that the second set of access conditions ought to be abolished provided sufficient consideration is given to:

(1) what material the first set of access conditions should permit access to; and

(2) the important point of principle as to what exceptions, if any, should apply to excluded material.

12.183 Dijen Basu QC agreed that the second set of access conditions should be abolished, with any pre-PACE enactments relevant to it and thought still necessary (for example, the Official Secrets Act 1911) being used in part to shape the relevant carve-outs in relation to excluded material.

12.184 The MPS also considered that the second set of access conditions should be abolished. The requirement that there should be a pre-PACE 1984 statutory provision was said to be arbitrary and out-dated. It was argued that whether or not a warrant should be issued should be consistent and related to current, not historic, provisions.

12.185 The NHSCFA, who investigate high value economic crime within the NHS, informed us that, as their investigations often involve NHS employees, patient records are sought. However, in its current state, the second set of access conditions make it impossible to obtain excluded material (in the form of patient records) without cooperation as there is no pre-PACE provision under which a warrant could be sought.

---

[103] NHS Counter Fraud Authority; Crown Prosecution Service; Professor Richard Stone; HM Council of District Judges (Magistrates' Courts); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Guardian News and Media; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; News Media Association; The Law Society; Dijen Basu QC; Bar Council & Criminal Bar Association; Metropolitan Police Service; National Crime Agency; Serious Fraud Office.

[104] Professor Richard Stone; HM Council of District Judges (Magistrates' Courts); Crown Prosecution Service; Senior District Judge (Chief Magistrate) Council of Her Majesty's Circuit Judges; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; News Media Association; The Law Society; Dijen Basu QC; Bar Council & Criminal Bar Association; Metropolitan Police Service.

[105] NHS Counter Fraud Authority; Crown Prosecution Service; Guardian News and Media; National Crime Agency; Serious Fraud Office.

12.186 The National Crime Agency accepted that applications for excluded material under the second set of access conditions are relatively rare but queried how confidential journalistic material and medical records/human tissue/fluid would otherwise be obtained.

12.187 The SFO had no observations on this subject given that they use a separate statutory regime. The SFO noted, however, the importance of ensuring that there was no effect on their powers under section 2 of the CJA.

Analysis

12.188 Case law indicates that the second set of access conditions has been used to obtain confidential journalistic material. As we wrote at paragraph 12.153 above, in *R (British Sky Broadcasting Ltd) v Central Criminal Court* production orders were sought for journalistic material which included material held in confidence, relying on section 9 of the Official Secrets Act 1911 as the pre-PACE provision.[106] As a consequence, the case for abolishing the second set of access conditions could not be made out solely on the ground that it is never used.

12.189 It is also important to bear in mind that abolishing the second set of access conditions would not affect other regimes which permit access to material which would constitute excluded material under PACE. As noted by the SFO, this includes their regime under the CJA.

12.190 As indicated above, there is an argument that the second set of access conditions is too restrictive and excluded material, particularly confidential personal records, should be moved to the first set of access conditions. If this were the case, the second set of access conditions could be abolished as there would be no need for it.

12.191 However, it would be inappropriate to repeal the second set of access conditions at this time, as it would make it impossible to obtain a production order or search warrant for excluded material under PACE. While the test under the second set of access conditions is highly restrictive, and in our view both impractical and arbitrary, it does allow for excluded material to be obtained in some limited cases, such as Official Secrets Acts cases. The second set of access conditions is therefore better than having no access conditions for excluded material and so should not be abolished without a more wholesale restructuring of the regime, for which we consider there are strong arguments.

12.192 For this reason, we agree with the weight of consultees that the second set of access conditions should only be abolished if a more principled and coherent set of rules governing access to excluded material is provided in its place.

THE PROTECTION OF EXCLUDED MATERIAL AND SPECIAL PROCEDURE MATERIAL IN CASES OF SEIZURE NOT UNDER WARRANT

The current law

12.193 If excluded or special procedure material is found in the course of a search authorised by a warrant under section 8 of PACE, it may not be seized under section 8(2) of PACE. The power of seizure only extends to "anything for which a search has been authorised under subsection (1) above", and subsection (1) specifically exempts from the search warrants

---

106 *R (British Sky Broadcasting Ltd) v Central Criminal Court* [2011] EWHC 3451 (Admin), [2012] QB 785 at [5].

regime “items subject to legal privilege, excluded material or special procedure material”. These types of material are treated in a similar way under a large number of other search warrant provisions.

12.194 The position of excluded material and special procedure material (but not legally privileged material) is different for seizures not under a warrant, in two specific instances:

(1) **The arrest powers** – the power of seizure under sections 18[107] and 32[108] of PACE, concerning the search of premises of a person who is under arrest, excludes legally privileged material. There is no exclusion for special procedure and excluded material;

(2) **The premises powers** – the same is true of the powers under sections 19[109] and 20[110] of PACE, which give a constable who is lawfully on any premises power to seize anything other than legally privileged material which they have reasonable grounds for believing to be evidence of an offence or obtained in consequence of the commission of an offence, and to be in danger of loss or destruction.

The consultation paper

12.195 In the consultation paper, we noted that it could be argued that the position under these powers should be brought into line with that under a warrant, and that excluded and special procedure material should be exempt from seizure under the arrest and premises powers. Otherwise, the exemption in section 8 of PACE is largely ineffective, because:

(1) this difference increases the incentive to arrest a suspect in order to search the premises, rather than apply for a search warrant; and

(2) even if the investigator is present on the premises to execute a warrant, section 19 of PACE can always be used to circumvent the exemption in section 8 of PACE, as the investigator can always claim that there is a danger of the loss, alteration or destruction of excluded or special procedure material, especially in the case of electronic material.

12.196 In particular, it is strongly arguable that excluded material at least (medical and counselling records and confidential journalistic material) should be put in the same position as legally privileged material, so that it cannot be seized consequent on arrest. According to Colvin and Cooper, the special protection afforded to legally privileged, excluded and special procedure material ensures that PACE is compliant with the ECHR, since each category of

---

107 Police and Criminal Evidence Act 1984, s 18: a constable may enter and search any premises occupied or controlled by a person who is under arrest.

108 Police and Criminal Evidence Act 1984, s 32: a constable may enter and search any premises in which an arrested person was when arrested or immediately before he was arrested for evidence relating to the offence.

109 Police and Criminal Evidence Act 1984, s 19: general powers of seizure and production of material that either has been obtained in consequence of the commission of an offence or is evidence in relation to an offence can be exercised by a constable whenever lawfully on premises.

110 Police and Criminal Evidence Act 1984, s 20: certain powers of seizure are construed as including a power to require information stored in electronic form and accessible from the premises to be produced in a visible, legible and transportable form.

material falls within a right guaranteed within the ECHR.[111] As a result, if the law fails adequately to protect this material, a breach of ECHR rights may be established.

12.197 However, it could be argued that the arrest and premises seizure powers reflect emergencies, where the main concern is to search as widely as possible and secure all possibly relevant material against destruction.

12.198 Accordingly, we invited[112] consultees' views on whether excluded and special procedure material ought to be exempted from seizure under the arrest and premises seizure powers in sections 18, 19, 20 and 32 of the Police and Criminal Evidence Act 1984.

Consultation responses

12.199 Nineteen consultees[113] answered this question: eight agreed;[114] seven disagreed;[115] and four expressed other views.[116] Of those consultees who agreed, a number of arguments were put forward in support.

12.200 The GNM and the NMA supported the exemption of excluded and special procedure material from seizure as it would ensure consistency of protection of journalistic material and protection of sources. It would prevent the circumvention of press freedom protections, reduce any threat to sources and avoid any disruption of investigation or publication.

12.201 The GNM argued that if the arrest powers are to remain untouched, they must be subject to express safeguards to protect journalists under PACE. Specifically, they must enable journalists to assert journalistic privilege and seek legal advice.

12.202 The Law Society argued that a failure to apply the same rule to a seizure made otherwise than under a warrant could be non-compliant with the ECHR, and would be inconsistent with other domestic legislation. They also suggested that it could encourage the arrest of individuals in order to gain access to protected material that would otherwise be exempted.

12.203 The Magistrates Association also agree that excluded and special procedure material ought to be exempted from seizure in other PACE provisions. The reason given was that the ECHR requires that the law must protect such material, and the protections within section 8

---

111 M Colvin and J Cooper, *Human Rights in the Investigation and Prosecution of Crime* (2009) p 138.

112 Consultation Question 49.

113 Professor Richard Stone; HM Council of District Judges (Magistrates' Courts); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Guardian News and Media; Guardian News and Media; Insolvency Service; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; News Media Association; Independent Office for Police Conduct; The Law Society; Magistrates Association; Dijen Basu QC; Bar Council & Criminal Bar Association; Metropolitan Police Service; National Crime Agency.

114 Professor Richard Stone; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Guardian News and Media; Birmingham Law Society; News Media Association}.; The Law Society; Magistrates Association.

115 Insolvency Service; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Dijen Basu QC; Bar Council & Criminal Bar Association; Metropolitan Police Service; National Crime Agency; Serious Fraud Office.

116 HM Council of District Judges (Magistrates' Courts); Crown Prosecution Service; Guardian News and Media; Independent Office for Police Conduct.

of PACE would be ineffective if not reflected in other provisions, as these other provisions could be used to bypass section 8 of PACE.

12.204 Against this, a number of consultees disagreed with exempting excluded and special procedure material from seizure under PACE. The National Crime Agency, Insolvency Service and Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate explained that seizure may occur following an arrest where it is feared that material will be destroyed. In some cases, seizure of such material may prevent the loss of life or serious injury to another.

12.205 Dijen Basu QC believed strongly that excluded and special procedure material should not be exempted from seizure pursuant to the statutory powers of police officers flowing from sections 32, 18 and 19. He observed that it is very doubtful that an arrest of a suspect would be held to be lawful if its sole purpose was to seek to carry out a search – whether for special procedure, or excluded material or otherwise.

12.206 Dijen Basu QC explained that the paradigm example of a warranted search is that of an innocent person having their premises searched for evidence of crimes in which they are not involved. In contrast, a search following an arrest targets a specific person suspected of being guilty of one or more offences. For this reason, there are strong reasons why officers should be able to enter premises to arrest a suspect for indictable offences, and to search the premises in which they find the suspect as well as other premises occupied or controlled by him. Accordingly, Dijen Basu QC argued that to place strictures on the police when searching upon arrest would be unnecessarily to throw obstacles in their path which could be exploited by well-resourced offenders prepared to use proceedings as a means of impeding police investigations.

12.207 The Bar Council and the CBA also did not agree that exempting excluded and special procedure material was appropriate. Whilst the question focusses on PACE, they noted that other law enforcement agencies are sometimes only able to progress their investigations when the police exercise PACE powers on their behalf. For example, powers to search and seize material from individuals upon arrest may be exercised in circumstances where the investigating agency does not have grounds to apply for a search warrant under another statutory power.

12.208 The Bar Council and the CBA therefore considered that, if the exemption to arrest powers were extended to apply to excluded and special procedure material, other law enforcement agencies may be adversely affected. They gave the example of the Competition and Markets Authority, who might be seriously hampered in a cartel investigation where the "doctored" company accounts only exist as an attachment to an email that is saved on a suspect's phone. For the avoidance of doubt, the Bar Council and the CBA stated that the exemption for material subject to legal privilege should be protected and remain distinct from the treatment of excluded and special procedure material.

12.209 This point was also made by the SFO, who noted that they did not themselves have any power of arrest and that where arrests are necessary in their investigations they are reliant on other agencies such as the police. They argued that if special procedure material (and to a lesser extent excluded material) were to be exempted from PACE arrest powers, the relevant powers would become very ineffective instruments in the context of investigations into serious economic crime.

12.210 The MPS considered that the consultation should be limited to search warrants and their effects and not extend beyond that remit to the reduction of policing powers relating to

warrantless searches. The MPS was very concerned that the burden of identifying a new and different power to deal with this material will be confusing to officers on the ground and prone, therefore, to add to the likelihood of things going wrong, contrary to the desire to simplify and streamline procedures.

12.211 Some consultees were less concerned by the exemption of excluded and special procedure material given the existence of seize and sift provisions. HM Council of District Judges (Magistrates' Courts), whilst not considering it appropriate to pass any view on the proposal, presumed that it was proposed that section 50 CJPA (authority to seize in order to search and sift) would still apply in the circumstances. This would potentially allay concerns that the police would be impeded from acting swiftly during emergencies.

12.212 The CPS acknowledged the logic of bringing other powers into line with the powers available for warrants and production orders, subject to clarification of the rules governing iniquitous material, and the power to exercise seize and sift.

12.213 The Independent Office for Police Conduct considered that the reason these provisions do not explicitly prohibit the seizure of this material is likely to be related to the risk that evidence of criminal activity will be destroyed or disposed of, were it not to be secured at the time of the search. Were reforms to be considered, then they suggest this material should be incorporated into the "seize and sift" provisions.

12.214 Along similar lines, the Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate said that there is an argument that if, whilst on premises, there is a suspicion that material could be destroyed, it should be seized at the time and any future questions of legality or admissibility dealt with at a later date.

Analysis

12.215 We do not recommend reform to sections 18, 19, 20 and 32 of PACE as it would have wide ramifications for the operation of powers of arrest, seizure and production outside of the search warrants context. Even if recommending reform would not involve stepping outside of our terms of reference, we are nonetheless persuaded that these provisions of PACE should not be amended.

12.216 First, we recognise the concerns expressed by consultees regarding the potential incompatibility of article 8 and article 10 of the ECHR with the arrest and premises powers of seizure, given the lack of adequate protection for excluded and special procedure material. However, the human rights which are engaged are qualified. Accordingly, an interference may be justified where it is in accordance with the law, necessary and proportionate.

12.217 We agree that a core purpose of these powers of seizure is to prevent the interference with or destruction of evidence. In addition, we now understand that the powers dovetail with dual agency investigations where protected material is the target material. A complete exemption of excluded and special procedure material from seizure would therefore significantly weaken the operation of these provisions and could compromise criminal investigations.

12.218 Secondly, we are unconvinced that the seize and sift regime under the CJPA would provide a workable alternative to ensure the seizure of excluded and special procedure material in order to prevent the loss or destruction of evidence. The power to seize and sift under the CJPA requires:

(1) a qualifying power of seizure (not production) that would be exercisable but for the material being mixed with material which the investigator cannot seize;[117] and

(2) the material which cannot be seized to be mixed with material which the investigator can in fact seize.[118]

Therefore, pure protected material would not be subject to seizure under the CJPA.

12.219 Thirdly, there are a number of investigative powers, in addition to powers of seizure under PACE, which do not exempt excluded and special procedure material. For example, there are powers to compel production of any material other than legally privileged material under section 2 of the CJA. Should reform be pursued, it would be necessary to consider in detail a far greater number of powers than those on which we consulted.

[117] Criminal Justice and Police Act 2001, s 50(5).

[118] Criminal Justice and Police Act 2001, s 50(1) and (2).

Chapter 13: The treatment of special procedure material

INTRODUCTION

13.1 In this chapter we consider reform to the way in which special procedure material is treated. Broadly speaking, special procedure material, as defined in section 14 of the Police and Criminal Evidence Act 1984 ("PACE"), includes non-confidential journalistic material and confidential information created or held for business or official purposes, other than legally privileged or excluded material. This definition covers, for example, account details kept by banks.

13.2 Following stakeholder discussions, we asked two questions regarding special procedure material in our consultation paper. The first concerned whether difficulties arose in practice in searches which relate to special procedure material.[1] The second sought views on whether a uniform scheme regarding the availability of special procedure material ought to apply across all search warrant provisions relating to criminal investigations.[2] We received consultation responses concerning several aspects of special procedure material. Accordingly, we discuss the following issues in this chapter:

(1) a uniform scheme for the availability of special procedure material under search warrants relating to a criminal investigation;

(2) the position where the target material includes both special procedure material and ordinary non-protected material;

(3) the position where the target special procedure material is mixed with excluded material which cannot be sought;

(4) the disclosure of non-confidential journalistic material;

(5) expanding the definition of special procedure material; and

(6) issuing further guidance on the meaning of special procedure material.

13.3 In summary, we acknowledge the desirability of amending the law to permit a search warrant to cover both ordinary and special procedure material to prevent the duplication of applications. Similarly, we note the desirability of amending the law to permit a production order to be obtainable where, if target material is mixed with excluded material, it is reasonably practicable for a person to comply with the terms of a production order by segregating the target special procedure material. However, recommending such reform would significantly affect the law governing production orders, on which we did not directly consult. We do, however, recommend that Code B of PACE is revised to provide guidance on when material will constitute special procedure material in order to better inform law enforcement agencies and reduce the risk of unlawful search and seizures.

---

1 Consultation Question 47.

2 Consultation Question 48.

DIFFICULTIES IN PRACTICE IN SEARCHES WHICH RELATE TO SPECIAL PROCEDURE MATERIAL

13.4 During pre-consultation discussions, stakeholders expressed the view that difficulties arise in practice in searches which relate to special procedure material. It was said that the statutory definition of special procedural material under section 14 of PACE is sometimes hard to apply. For example, one stakeholder stated that, where a search of business premises will see invoices seized that contain the names and addresses of customers, it is not entirely clear whether this should be regarded as special procedure material or not.

13.5 Stakeholders also raised concern around the position of special procedure material which is held with the intention of furthering a criminal purpose. This led us in our consultation paper to invite consultees' views on whether greater clarity needs to be introduced in defining searches for special procedure material held with the intention of furthering a criminal purpose.[3] We discuss this issue in Chapter 10 above which is devoted to the topic of iniquitous material.

13.6 The general concerns raised by stakeholders regarding the difficulties in practice in searches which relate to special procedure material led us to invite consultees' views on the extent of the problem caused. 18 consultees[4] answered the question. A number agreed that there are particular difficulties in practice in searches which relate to special procedure material.[5] The problems identified by consultees are listed at paragraph 13.2 above, which are discussed in the sections of this chapter which are to follow.

13.7 Before we go on to discuss the issues listed, we note a number of additional points that came out of the consultation responses. The Magistrates Association held a survey of their members for the purpose of responding to our consultation. According to their survey, only 10% of respondents had experience of dealing with applications involving special procedure material. However, 21% of respondents said that they would be comfortable dealing with search warrant applications which involved special procedure material without a legal adviser physically present.

13.8 Consultation responses also indicated uncertainty as to whether District Judges (Magistrates' Courts) have the power to grant production orders, and therefore search warrants, under schedule 1 to PACE.[6]

---

3 Consultation Question 47.

4 City of London Economic Crime Academy; Crown Prosecution Service; HM Council of District Judges (Magistrates' Courts); Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Guardian News and Media; Insolvency Service; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; News Media Association; The Law Society; Northumbria Law School Centre for Evidence and Criminal Justice Studies; Magistrates Association; Dijen Basu QC; Bar Council & Criminal Bar Association; Metropolitan Police Service; National Crime Agency; Serious Fraud Office; Financial Conduct Authority.

5 City of London Economic Crime Academy; Crown Prosecution Service; Guardian News and Media; Insolvency Service.

6 For a discussion of this issue see Alex Davidson, "Production Orders: R (BBC) v Newcastle Crown Court (Case Comment)" [2020] *Criminal Law Review* 247, 250.

A UNIFORM ROUTE TO THE AVAILABILITY OF SPECIAL PROCEDURE MATERIAL

The consultation paper

13.9 In the consultation paper, we observed that the legislative framework dealing with special procedure material is equally as complex as that for excluded material. Similar to excluded material, search warrants under section 8 of PACE and several other search powers may not be issued in respect of special procedure material. Nor may special procedure material be seized in the course of a search. Further, section 9(2) of PACE provides that any statute passed before PACE providing for search warrants to be issued to constables for the purposes of a criminal investigation will cease to have effect in relation to excluded and special procedure material.

13.10 As with excluded material, special procedure material may be obtained in some circumstances, unlike the absolute exemption afforded to legally privileged material. Section 9 of and schedule 1 to PACE provide a procedure for obtaining special procedure material, which is less onerous than that for obtaining excluded material. This must be authorised by a Circuit judge normally by means of a production order or, if a production order is not practicable for various reasons, by means of a search warrant.

13.11 A production order in respect of special procedure material may be made if the "first set of access conditions" under paragraph 2 of schedule 1 to PACE is satisfied. That is, if:

(1) there are reasonable grounds for believing that an indictable offence has been committed;

(2) there are reasonable grounds for believing that relevant evidence, constituting special procedure material but not including excluded material or legally privileged material, is on the premises;

(3) the judge considers that it is in the public interest to produce it or have access to it; and

(4) other methods of obtaining the material have been tried without success, or have not been tried because it appeared that they were bound to fail.

13.12 A search warrant in respect of special procedure material may only be issued if the above conditions are satisfied and it would not be practicable to make a production order for various reasons set out in paragraph 14 of schedule 1 to PACE.

13.13 These arrangements only apply in the case of investigations conducted by the police or someone with equivalent powers. In any other investigation, the material can be obtained by an ordinary warrant, unless there are other exclusions in the statute which applies to the investigation.

13.14 The availability of special procedure material therefore depends on who is applying for a warrant and under which provision an application is made. As with excluded material, we considered that it would be preferable not to have different rules for the availability of special procedure material depending on whether or not the investigation is being conducted by the police.

13.15 The central argument that we put forward for a uniform scheme was that the police no longer have a monopoly on the investigation of crime, and where other officials are performing

similar functions they should be subject to the same safeguards as the police. If it is not appropriate to entrust the police with the power to obtain these special categories of material by an ordinary warrant, still less is it appropriate to entrust civilian investigators with that power. The need to protect the confidentiality of information held by other persons and bodies is the same in both cases.

13.16 For this reason, we invited[7] consultees' views on whether:

(1) the exemption of special procedure material from search warrant powers under section 9(2) of PACE ought to apply to all criminal investigations, irrespective of whether the investigation is carried out by the police;

(2) the special procedure for applying for production orders and search warrants in respect of confidential business records and non-confidential journalistic material under schedule 1 to PACE ought then to be available in all cases in which those records are exempted from the power to issue a search warrant under (1) above; and

(3) there ought to be an exception to (1) above in the case of search powers for the purposes of specialist investigation where production orders, information requirements or similar procedures are available.

13.17 These amendments would therefore have the effect of requiring all investigators conducting a criminal investigation to use a schedule 1 to PACE procedure when seeking a search warrant for material which would constitute special procedure material under PACE, unless the investigator operates within a specialist regime.

Consultation responses

13.18 20 consultees[8] answered this question. Law enforcement consultees expressed serious concern regarding the consequences of our proposals. The Serious Fraud Office noted that confidential business records are frequently the target material in their investigations. Accordingly, they strongly opposed any restriction on their powers to compel production of, or seize, confidential business records under the Criminal Justice Act 1987.

13.19 In a similar vein, the Financial Conduct Authority strongly disagreed with restricting their powers to obtain confidential business records, which are frequently required in investigations into insider dealing and market abuse. This was also the case in respect of the Competition and Markets Authority, who argued that the current law strikes the right balance between the various interests at play. The Competition and Markets Authority explained that they would be concerned if it became more difficult to obtain special procedure material under competition and consumer protection law as it could significantly hinder their investigations.

---

7 Consultation Question 48.

8 Professor Richard Stone; HM Council of District Judges (Magistrates' Courts); Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Department for Work and Pensions; Kent County Council Trading Standards; Guardian News and Media; Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; News Media Association; Northumbria Law School Centre for Evidence and Criminal Justice Studies; The Law Society; Magistrates Association; Dijen Basu QC; Bar Council & Criminal Bar Association; National Crime Agency; Competition and Markets Authority; Serious Fraud Office; Financial Conduct Authority.

13.20 Kent County Council Trading Standards explained that their entry warrants may include the inspection of confidential business and banking records. The example given was where material is sought relating to a course of business or corroborating consumer complaints and confirming payments have been received by a suspect. Accordingly, Kent County Council Trading Standards explained that they would not want additional restrictions placed on their current powers to access business and banking records. The Department for Work and Pensions also stated that it will seek confidential business records if evidentially relevant to an investigation.

13.21 The Bar Council and the Criminal Bar Association ("CBA") also did not consider the amendments consulted on to be a practical or sensible approach. They pointed out that the power to obtain confidential business records under legislation outside of PACE stems from the fact that such material is directly applicable to the crimes these agencies investigate. Material which constitutes special procedure material under PACE is a necessary and important category of information for their investigations. For these reasons, it was argued that the ability to obtain confidential business records under such warrants should be preserved.

13.22 The Bar Council and the CBA also observed that on these grounds, one could instead argue that section 9(2) of PACE should be *disapplied*, rather than extended, for regional police economic directorates and the City of London Police investigations given that confidential business records will often be the crux of their case.

13.23 In contrast, the Northumbria Law School Centre for Evidence and Criminal Justice Studies stated that a single point for process and procedure where confidential business records and non-confidential journalistic material is involved in criminal investigations would seem desirable. They noted that different processes simply add unnecessary complexity and make future amendments of provisions more difficult and less likely to be consistent. If our proposal was adopted, all investigatory bodies would also be held to the same standard as the police. The Northumbria Law School Centre for Evidence and Criminal Justice Studies accepted that difficulty might arise when determining the point at which an investigation by a regulatory body becomes a criminal investigation.

13.24 Both the News Media Association ("NMA") and the Guardian News and Media ("GNM") considered that special procedure material – including all non-confidential journalistic material – should be excluded from the scope of all search warrants, irrespective of whether the investigation is carried out by the police, or by other investigation and enforcement authorities, specialist or otherwise.

13.25 In principle, the GNM supported the position that all non-confidential journalistic material should only be obtainable under a uniform production order regime mirroring schedule 1 to PACE. The NMA also stated that non-confidential journalistic material should only be obtainable under the production order procedure provided that confers improved protection for freedom of expression and press freedom.

13.26 In the NMA's view, it would be logical and coherent on freedom of expression and press freedom grounds for the journalistic material exemption always to apply in any case in which an investigative power would allow access to journalistic material by satisfaction of less stringent criteria than those found in PACE.

Analysis

13.27 After carefully considering consultees' responses, we are no longer of the view that it would be desirable to extend the schedule 1 procedure to all criminal investigation warrants. This is primarily for the same reason we were dissuaded from a uniform scheme in respect of excluded material.

13.28 First, each regime, and the effect amendment will have, should be considered separately. Sweeping legislative amendments cannot be made without careful consideration of each regime and how it will affect an agency's investigative powers. Connected to this is the fact that introducing a uniform scheme will inadvertently affect other investigative powers beyond search warrants which agencies have at their disposal. For example, compulsory production powers would require amendment. These amendments would therefore fundamentally alter not just search warrant regimes but entire enforcement regimes.

13.29 Secondly, looking at particular regimes, we agree that special procedure material is likely to be central to a considerable number of agencies' investigations. As we have observed, it is for this reason an exception to the prohibition on seeking excluded and special procedure material under a pre-PACE enactment has been created for HMRC.[9] We therefore agree with the Bar Council and the CBA that there is an argument that the exclusion of special procedure material (other than non-confidential journalistic material) should in fact be disapplied for regional police economic directorates and the City of London Police given the centrality of confidential business records to their investigations.

13.30 Any amendments would therefore have to be adapted to the context of other enforcement regimes in which the dominant purpose of the powers will be to obtain material which falls under the definition of special procedure material. However, accounting for such nuances and avoiding burdensome conditions may defeat the purpose of imposing a uniform scheme of protection, especially if, in reality, the statutory conditions imposed are likely to be met in virtually all instances in which access is sought.

13.31 Thirdly, we agree with the Northumbria Law School Centre for Evidence and Criminal Justice Studies that it would be difficult to delineate between criminal and non-criminal investigations. We identified this issue in the context of extending the statutory safeguards under sections 15 and 16 of PACE.[10] Therefore, it would be difficult to draw a meaningful boundary as to where a uniform rule ends: as we explained in the previous chapter, the boundary between criminal and civil or regulatory provisions can be an elusive one.

13.32 Fourthly, we do not think that the simplification of investigatory powers is a strong justification for uniformity. Each regime has been carefully crafted for the particular agencies using it and the nature of their investigations. Accordingly, agencies are familiar with their specific statutory regimes. It is therefore unlikely that errors will flow from different agencies having recourse to differently crafted regimes.

13.33 Fifthly, we accept a common thread through these powers is that access to special procedure material involves an interference with a person's article 8 rights which on its face justifies consistent safeguards. However, article 8 of the European Convention on Human Rights ("ECHR") is a qualified right. Further, there is likely to be a far more muted public

---

9 Police and Criminal Evidence Act 1984 (Application to Revenue and Customs) Order 2015 (SI 2015 No 1783), art 6.

10 See paragraphs 2.27 to 2.30 above.

interest in the protection of confidential business records in investigations into fraud, revenue, customs, company, commercial and insolvency offences. Even where procedures to obtain special procedure material which are less stringent than schedule 1 PACE exist, it does not follow that the balance of the competing interests is not appropriately struck.

13.34 Having reached this view, we turn to consider whether, under PACE and other search warrant regimes, material which falls under the definition of special procedure material is not adequately protected. We have received no evidence to lead us to conclude that the current level of protection afforded to such material under any regimes requires amendment.

SPECIAL PROCEDURE MATERIAL MIXED WITH ORDINARY MATERIAL

Consultation responses

13.35 The City of London Police Economic Crime Academy stated that, generally speaking, the category of special procedure material is understood. However, they raised issues regarding mixed material. They contended that confusion surrounds the issue of business records held by suspects themselves, particularly where a mix of special procedure material and ordinary material not subject to this description is sought. Further, the existence of two distinct routes to obtaining material (ordinary material under section 8 of PACE and special procedure material under schedule 1 to PACE) was said to be unsatisfactory and can lead to the investigator obtaining both a section 8 warrant and a schedule 1 warrant for the same premises.

13.36 Dijen Basu QC also observed that problems arise where the target material is at the margins of satisfying the definition of special procedure material or where some of the target material does satisfy it and some does not. In his experience, the courts have tended to 'gloss over' these problems in practice when ordinary material is searched for under a schedule 1 warrant by observing that those subject to a schedule 1 warrant for special procedure material enjoy greater protection than under a section 8 warrant. For example, a schedule 1 warrant can only be issued by a Circuit judge and not a magistrate.

13.37 Dijen Basu QC could not see a good reason for the regimes for special procedure material and for ordinary material to be treated by PACE as mutually exclusive. He also made the point that paragraph 12 of schedule 1 to PACE, which sets out the power to issue a warrant, does not expressly limit the scope of the warrant to special procedure material. Dijen Basu QC considered that it would seem entirely unnecessary for a schedule 1 warrant to be held to have been unlawfully issued simply because the target material was not, in fact, special procedure material, but could have been sought under a section 8 warrant which would have been granted in the circumstances and with fewer safeguards.

13.38 Dijen Basu QC also stated that this potential difficulty will be avoided by the application of section 31(2A) and (3A) of the Senior Courts Act 1981. These provisions provide that claims for judicial review are generally to be dismissed if the outcome for the applicant would have been substantially the same if the conduct complained of had not occurred.

Analysis

13.39 It is important to distinguish between three different scenarios:

(1) a search where the target material consists solely of special procedure material;

(2) a search where the target material includes both ordinary material and special procedure material; and

(3) a search where the target material consists solely of ordinary material.

13.40 The statutory access conditions for a search warrant under paragraph 2 of schedule 1 to PACE could be met in both scenarios (1) and (2) above. This is because the first set of access conditions are fulfilled if there are reasonable grounds for believing that there is material which consists of or *includes* special procedure material.[11] Therefore, a schedule 1 PACE warrant could be obtained in the example given by the City of London Police Economic Crime Academy where a mixture of special procedure material and ordinary material is sought. For this reason, we regard reform as unnecessary.

13.41 It is worthwhile also considering the appropriateness of a schedule 1 PACE warrant in scenario (3). In our view, the first set of access conditions under paragraph 2 of schedule 1 would not be fulfilled if there were no grounds for believing that the material included special procedure material.

13.42 *Fitzgerald* is a case which demonstrates the approach indicated by Dijen Basu QC, where the Divisional Court was unimpressed by the claimant's argument that the police should have proceeded under a section 8 PACE warrant as the target material was iniquitous material in which there could be neither confidence nor privilege.[12] The court observed that proceeding under a schedule 1 PACE search warrant actually increased the safeguards for the claimant.[13]

13.43 In light of this decision, and the observations made by Dijen Basu QC, we also consider it unlikely that obtaining a schedule 1 PACE warrant for ordinary material will lead to arguable grounds for quashing a search warrant.

SPECIAL PROCEDURE MATERIAL MIXED WITH EXCLUDED MATERIAL

Consultation responses

13.44 Difficulties in practice were also identified by the Crown Prosecution Service ("CPS") where special procedure material is mixed with excluded material in the context of production orders. In its experience, an individual served with a production order may refuse to comply with the order because the target data is mixed with excluded material which cannot be sought. For example, an investigator may seek details of payments to particular sources. These payments may be held by the recipient of a production order on a payments database which also contains excluded material. The investigator cannot be provided with the entire database, nor is there an obligation for the recipient to sift and provide the special procedure material.

13.45 In the CPS's view, on an *inter partes* application, the respondent should not be able to rely on special procedure material being mixed with excluded material and the burden of sifting the two as a reason for a production order not to be granted. The CPS therefore suggested that paragraph 2(a)(ii) of schedule 1 to PACE should be amended to read:

---

11 Police and Criminal Evidence Act 1984, sch 1, para 2(a)(ii).

12 *Fitzgerald v Preston Crown Court* [2018] EWHC 804 (Admin) at [69].

13 *Fitzgerald v Preston Crown Court* [2018] EWHC 804 (Admin) at [69].

That there is material which consists of special procedure material or includes special procedure material and [that the specific material sought and which the respondent is capable of identifying] does not also include excluded material on premises specified in the application, or on premises occupied or controlled by a person specified in the application (including all such premises on which there are reasonable grounds for believing that there is such material as it is reasonably practicable so to specify).

13.46 This amendment was said to reflect, in respect of production orders, the obligations which PACE imposes elsewhere, such as in section 19(4) PACE for a person to produce information stored in any electronic form in a form in which it can be taken away.

Analysis

13.47 The issue expressed by the CPS relates predominantly to production orders rather than search warrants. Saying that, a search warrant for special procedure material under PACE can only be granted where the first set of access conditions for the grant of a production order is fulfilled.[14]

13.48 We agree with the CPS that a person should not be able to resist the grant of a production order merely on the grounds that to sift special procedure material from excluded material would impose a burden, so long as it would not in fact be unduly burdensome. In reaching this conclusion, we have taken into account the fact that, were a search warrant executed on the premises, section 50 CJPA would empower an investigator to seize excluded material which contained special procedure material in order to sift out the excluded material. Similarly, section 19(4) of PACE would require an occupier to produce any information stored on a device.

13.49 The access condition that the target material does not also include excluded material is clearly designed to prevent the production of excluded material. While excluded material would remain protected from production under the CPS's proposal by requiring a respondent to perform a sift, there will clearly be instances where this would be unduly burdensome for an individual, even within the time limit imposed by the order.

13.50 One answer to this is for more time to be provided to comply with the order.[15] We also note the exception to the duty of an investigator to sift material seized pursuant to section 50 CJPA where it is not reasonably practicable to sift the material.[16] We consider it right that the respondent to a production order should be able to avoid performing a sift in similar circumstances. A respondent to a production order would otherwise be held to higher standards than those to which an investigator is held.

13.51 We agree that amending the first set of access conditions in this respect would be desirable. Once again, we make no formal recommendation for reform as any amendment would fundamentally alter the operation of production orders, on which we did not directly consult.

---

14 Police and Criminal Evidence Act 1984, sch 1, para 12(a)(i).

15 Police and Criminal Evidence Act 1984, sch 1, para 4.

16 Criminal Justice and Police Act 2001, s 53(3)(c).

DISCLOSURE OF NON-CONFIDENTIAL JOURNALISTIC MATERIAL

Consultation responses

13.52 The GNM considered it necessary to amend the law governing access to special procedure material. The GNM was particularly concerned with non-confidential journalistic material which is capable of revealing sources. In particular, the GNM referred to the risks that can be posed to sources by "jigsaw identification" from the seizure of material, which refers to a collection of information that, when placed together, leads to the identification of an individual.

13.53 The GNM explained that source protection is obviously fundamental to public interest investigative journalism, which frequently depends on leads provided by anonymous or confidential informants. The GNM is routinely approached by potential whistleblowers and other sources who have information that they want to disclose but are fearful about the potential consequences. They seek reassurance that the organisation will do everything it can to protect their identities. This accepted duty of trust lies at the heart of much of journalists' work. These principles are invariably challenged when a production order application is made in respect of special procedure material.

Analysis

13.54 We recognise the concerns raised by the GNM in relation to the protection of sources. We agree that the protection of sources lies at the heart of journalists' work. The importance of the protection of sources has been underlined on a number of occasions by the European Court of Human Rights and is acknowledged in section 10 of the Contempt of Court Act 1981.

13.55 As we state at paragraph 12.153 above, article 10 of the ECHR is not absolute and therefore we do not consider that journalistic material should be exempt from disclosure in all cases. In our view, the answer to the concerns raised by the GNM lies in the application of the public interest test under paragraph 2(c) of schedule 1 to PACE. The court must also take into account article 10 of the ECHR when exercising its discretion to grant a search warrant or production order, which invariably overlaps with the public interest analysis and will include consideration of the protection of journalists' sources.

EXPANDING THE DEFINITION OF SPECIAL PROCEDURE MATERIAL

Consultation responses

13.56 The Northumbria Law School Centre for Evidence and Criminal Justice Studies stated that some consideration should be given to the interaction between confidential information held for business purposes and information held under the General Data Protection Regulation ("GDPR"). In particular, whether the latter category should be included in the definition of special procedure material, for example as a type of protected data.

Analysis

13.57 The GDPR applies to the "processing" of "personal data". Processing means acquiring and subsequently storing or using data.[17] Personal data is information that relates to an identified

[17] Data Protection Act 2018, s 3(4).

or identifiable individual and therefore includes names, identification numbers, location data and online identifiers.[18] Personal data may also comprise "special category data"[19] or "criminal offence data",[20] which are subject to tighter safeguards for processing. Special category data covers:

(1) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(2) genetic data, or biometric data, for the purpose of uniquely identifying an individual;

(3) data concerning health; and

(4) data concerning an individual's sex life or sexual orientation.

13.58 The processing of personal data by competent authorities for "law enforcement purposes",[21] such as the police investigating a criminal offence, is outside the GDPR's scope. Instead, this type of processing is subject to the rules in Part 3 of the Data Protection Act 2018. Under Part 3, a data controller in relation to personal data is responsible for, and must be able to demonstrate, compliance with the six data protection principles and the two safeguarding measures set out at sections 35 to 42 of the Data Protection Act 2018. Particular safeguards apply to "sensitive processing",[22] which involves the processing of special category data.

13.59 We have considered the desirability of expanding the definition of special procedure material to cover personal data or special category data under the GDPR. In practice, if such material were to be re-categorised as special procedure material, then investigators would have to apply for a schedule 1 warrant, and fulfil the first set of access conditions, if they wished to search for any documents which contained personal data or special category data.

13.60 In our view, this proposal is undesirable for a number of reasons. The definition of personal data under the GDPR is extremely wide, making it highly likely that the vast majority of documents investigators wish to search for contain some form of personal data. Therefore, if personal data were to be categorised as special procedure material there would be a huge increase in the number of schedule 1 warrants applied for. Schedule 1 applications are more resource-intensive than section 8 applications.

13.61 For this reason, there would need to be exceptionally good reasons to categorise personal data as special procedure material. In our view, such reasons have not been made out. In reaching this view, we observe that ordinary material is still subject to a number of protections under a section 8 warrant: an investigator must satisfy the court that documents containing personal data are likely to be relevant evidence and of substantial value to the

---

18 Data Protection Act 2018, s 3(2); General Data Protection Regulation (EC) No 679/2016, Official Journal L 119 of 4.5.2016 p 1, art 4(1).

19 Data Protection Act 2018, s 10; General Data Protection Regulation (EC) No 679/2016, Official Journal L 119 of 4.5.2016 p 1, art 9.

20 Data Protection Act 2018, s 10; General Data Protection Regulation (EC) No 679/2016, Official Journal L 119 of 4.5.2016 p 1, art 10.

21 DPA 2018, s 31: the prevention, investigation detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

22 DPA 2018, s 35(3).

investigation of the offence,[23] and they must comply with the safeguards in sections 15 and 16 of PACE.

13.62 There is, however, a stronger case for special category data to be categorised as special procedure material given that it is of particular sensitivity and therefore deserving of particular protection.

13.63 On balance, we remain of the view that the definition of special procedure material should not be expanded, even to include special category data. The conditions for granting an ordinary section 8 PACE warrant in our view offer sufficient protection. We consider that the safeguards under the Data Protection Act 2018 scheme adequately protect the processing by law enforcement of personal data and special category data. We do not regard expanding the definition of special procedure material either necessary or desirable in itself simply to bring parity between the Data Protection Act 2018 and PACE.

FURTHER GUIDANCE ON THE MEANING OF SPECIAL PROCEDURE MATERIAL

Consultation responses

13.64 Under section 14(2)(b) of PACE, material, other than journalistic material, can only qualify as special procedure material if it is held "in confidence" or subject to a restriction or obligation of secrecy contained in an enactment. The Insolvency Service considered that this aspect of the definition of special procedure material can cause difficulty in determining whether material is "held in confidence" or not. It was said that a definition which incorporates the detail of personal information would bring clarity to this area.

13.65 HM Council of District Judges (Magistrates' Courts) considered that, in relation to material held for business purposes, guidance as to what is and is not likely to be considered as confidential would be helpful in considering applications for special procedure material. The National Crime Agency also stated that examples need to be provided of what constitutes special procedure material as there is confusion amongst individuals. The Magistrates Association considered that, if there is any lack of clarity in relation to the definition of special procedure material, it would be important for this to be amended so there was consistent application of the definition.

13.66 HM Revenue and Customs stated that better guidance would assist in respect of material which is held in confidence. It was said that greater clarity on the definition of special procedure material would be most welcome. The current definition was said to be hard to apply on the facts in certain circumstances, meaning that sometimes an investigator might seek a section 9 PACE warrant from the Crown Court out of an abundance of caution when this work might be helpfully moved to the Magistrates' Courts.

Analysis

13.67 It is evident from consultation responses that investigators find it difficult to ascertain whether material is special procedure material. One police force admitted that officers accidentally applied for a section 8 warrant in relation to special procedure material, which led to litigation and a complex criminal investigation being compromised.

---

[23] Police and Criminal Evidence Act, s 8(1)(b) and s 8(1)(c).

13.68 Another stakeholder, a retired police officer, suggested that seeking section 8 PACE warrants for special procedure material is a common occurrence. This indicates that errors are being missed by the courts when issuing warrants. Additionally, the recent joint inspection of the NCA's search warrant and production order application process suggests that there is uncertainty regarding when documents constitute special procedure material.[24]

13.69 We agree that greater clarity is needed to identify when material constitutes special procedure material, in order to better inform law enforcement agencies and reduce the risk of unlawful search and seizures.

13.70 We do not regard it as necessary to amend the definition of special procedure material under section 14 of PACE. As we see it, the heart of the issue is determining whether material constitutes special procedure material. The problem does not lie with the underlying categories of material which comprise special procedure material. Seeking to expand on the meaning of statutory terms risks rendering the provision less comprehensible.

13.71 Instead, it would be beneficial to provide guidance on when material is likely to constitute special procedure material in Code B of PACE given that the Codes of Practice are designed for investigators and the definition of special procedure material is itself found in PACE.

Recommendation 44

13.72 We recommend that the PACE Strategy Board consider amending Code B of the Police and Criminal Evidence Act 1984 to provide guidance on when material constitutes special procedure material.

[24] HMCPSI and HMICFRS, *A joint inspection of search application and production order processes* (January 2019) para 2.9.

Chapter 14: An introduction to electronic material and the law

INTRODUCTION

14.1 In the following five chapters (Chapters 14, 15, 16, 17 and 18) we consider the application of search warrants and associated provisions to electronic material. We use the term "electronic material" to refer to both devices themselves ("electronic devices"[1]) and data stored in electronic form ("electronic data"). The central question with which these chapters are concerned is: what ought to be the law and procedure when an investigator seeks to obtain electronic data stored on, or accessible from, a device on premises under the authority a search warrant?

14.2 Many of those who responded to our consultation described the application of search warrants to electronic material as the area which is in most need of reform. We agree. The legal framework that currently governs the search and seizure of electronic material was not designed with the ways in which electronic material is now accessed in mind. This means that the current law fails to appreciate the unique features of electronic material and digital investigations. Dramatic technological change has also created legal uncertainty in respect of search warrant regimes. As a result, the current law both inhibits criminal investigations and has significant privacy implications for those whose electronic devices are searched and seized.

14.3 We make several recommendations for reform to the law and procedure governing search warrants in Chapters 15, 16 and 17. These recommendations aim to ensure that the current framework governing search warrants operates effectively in the modern digital world so that evidence of criminality can be secured. At the same time, these recommendations aim to afford robust privacy protections in respect of the obtaining and subsequent treatment of electronic data.

14.4 In Chapter 15 we consider what the law and procedure ought to be when an investigator seeks to obtain electronic data stored "locally" on an electronic device on premises. In Chapter 16, we consider the same question in respect of electronic data stored "remotely" but accessible from a device on premises. In Chapter 17 we consider how electronic material should be treated by law enforcement after it has been seized or copied.

14.5 In Chapter 18 we set out why there is a pressing need for a wider review of the acquisition and treatment of digital material in criminal investigations. There are two principal reasons for this recommendation: the first is that our recommendations involve amendments to the existing framework of search warrants. However, there is an argument that a more fundamental modification of the law is needed. The second reason for recommending a wider review is that there are aspects of the law outside of a search warrants context that suffer from the same underlying issues that we have identified.

---

[1] There are a number of different terms used in legislation and literature to refer to electronic devices: digital devices; data storage devices; electronic storage devices; and digital processing systems. In this report we use the term "electronic devices" in a broad sense to refer to all devices that control and direct electric currents.

14.6 In this chapter we provide an introduction to the topic of electronic material in order to provide essential context for the issues discussed in the next four chapters. We discuss the following matters:

(1) the nature of electronic material, including the key characteristics of electronic devices and electronic data;

(2) an overview of the relevant legal regimes which govern the acquisition and treatment of electronic material;

(3) how searches under warrant for electronic material operate in practice; and

(4) the problems with the current law concerning the acquisition and treatment of electronic material.

THE NATURE OF ELECTRONIC MATERIAL

14.7 In our consultation paper we grouped electronic material into four categories in order to provide a framework for analysing the application of search warrants to electronic material. The categories are:

(1) electronic devices themselves (such as mobile phones or laptops);

(2) electronic data stored locally on devices (that is the files or documents on the hard drive of a device);

(3) electronic data stored remotely within the jurisdiction but accessible from an electronic device; and

(4) electronic data stored remotely outside of the jurisdiction but accessible from an electronic device.

Electronic devices

14.8 Electronic devices pervade our lives. 95% of adults in the United Kingdom own a mobile phone, 76% of whom own a smart phone.[2] 88% of households in the United Kingdom have a home computer.[3] Other examples of electronic devices include laptops, tablets, televisions, cameras and gaming consoles.[4]

14.9 In recent years, we have been witness to the growing phenomenon of the "Internet of Things" as everyday objects are combined with computing devices: watches, fitness trackers, cars. The extension of internet connectivity into these objects means that they can

---

2 https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/pg_global-technology-use-2018_2019-02-05_0-01/.

3 https://www.statista.com/statistics/289191/household-penetration-of-home-computers-in-the-uk/.

4 We set out a number of electronic devices identified by consultees as potentially being the target of a search warrant at paragraphs 15.9 to 15.10 below.

create, store, transmit and receive electronic data. It is estimated that there are currently 20 billion devices worldwide with this functionality.[5]

14.10 There are a number of common features across all electronic devices. Every electronic device has a processor as part of its hardware, often referred to as the central processing unit ("CPU"), which receives, processes and produces data. Software, consisting of programs, which is a type of electronic data, gives instructions that are executed by the processor.

14.11 Data may be stored in two ways on electronic devices:

(1) on an internal storage chip directly accessible by the processor of the electronic device itself ("primary storage"); or

(2) on storage media that is internal or external to the electronic device ("secondary storage").

14.12 Primary storage is often described as "short-term storage" in which the data is "volatile"; this is because primary storage only maintains data while the electronic device is powered on. Secondary storage, on the other hand, will retain data when the device is powered off, meaning that data is "non-volatile" and stored for long term preservation.

14.13 Examples of secondary storage include the internal hard drive of an electronic device and external removable devices such as a USB device or memory card. Hard drives contain partitions, within which there are file systems which structure data.

14.14 Another example of secondary storage is remote servers. Remote servers can be located anywhere in the world. With internet connectivity, data can be transferred to and retrieved from remote servers using an electronic device through the processes of uploading and downloading.

14.15 The capacity of data storage has grown phenomenally: while once a rare and expensive resource, advances in technology have meant that data storage is now much cheaper and of almost limitless capacity.

Electronic data

14.16 Electronic data, in its raw form, is a pattern of seemingly meaningless binary digits.[6] This is rendered intelligible to humans by computers and other electronic devices. Electronic devices can therefore process electronic data into words, sounds or pictures.

14.17 Electronic data is measured in bytes.[7] As with other measurements, the volume of data is described using metric prefixes: kilobytes (1,000 bytes); megabytes (1,000 kilobytes); gigabytes (1,000 megabytes); terabytes (1,000 gigabytes) and so forth. A gigabyte of storage could store approximately 19,000 text documents or 600 photographs. This means

---

5 https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016.

6 See P Fenwick, *Introduction to Computer Data Representation* (2014) pp 14 to 15.

7 Technically speaking, the smallest unit of data measurement is a bit (short for binary digit), of which there are eight in a byte. However, other than measuring internet speed in bits per second, bytes are the conventional unit of measurement used in computing.

that a terabyte of storage would equate to approximately 19 million text documents or 600,000 photographs.

14.18 Humans interact with and produce electronic data at an incredible rate. It is estimated that 1.7 megabytes of data is created every second for every person on earth.[8] It was estimated that there were 33 zettabytes (thirty-three trillion gigabytes) of electronic data worldwide in 2018, which has grown to around 50 zettabytes in 2020.[9]

14.19 Electronic data is therefore an important part of our lives and is becoming more so. For example, one noticeable trend is the prevalence of "cryptoassets" and "cryptocurrency", terms which refer to cryptographically secured electronic data that cannot, according to the current common law definition, be physically possessed but which has value.[10] As a consequence, in some circumstances virtual currencies such as bitcoin are used instead of physical currency.[11] Central banks are now considering adopting cryptocurrencies.[12]

14.20 The connectivity of electronic devices and transfer of electronic data is underpinned and facilitated by network systems. Network systems can be classified in a number of ways.

(1) Personal area networks connect a small number of electronic devices. For example, Bluetooth can be classified as a wireless personal area network. Apple's AirDrop is also a personal area network. Both Bluetooth and AirDrop are private networks.

(2) Local area networks connect computers in a close proximity. These networks may be used by companies, schools or hospitals. The network may be connected by wireless signals or wired cables. Local area networks will typically be private networks. For example, employees of an organisation may have access to their own dedicated "intranet", which is a private computer network.

(3) Wide area networks denote networks that are further apart. The internet – the global system of interconnected networks which links electronic devices worldwide – is an archetypal example of a wide area network. The internet is a public network, as anyone can connect to it. Electronic devices can connect to the internet wirelessly through a WiFi connection.

14.21 Electronic data, too, can be categorised in a number of ways. These categories can have significance within specific legislative regimes, which we discuss further below. Electronic data can be categorised according to its type. For example, metadata is a type of data that provides information about other data, such as when a file was created and by whom.[13]

14.22 Electronic data can also be categorised according to its format. Electronic data may exist in a "native form". This means that the file is in the format created by the authoring application.

---

8 https://www.domo.com/solution/data-never-sleeps-6.

9 https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf at p 6.

10 See UK Jurisdiction Taskforce, *Legal Statement on Cryptoassets and Smart Contracts* (November 2019) para 26.

11 Such currencies are used more as investment vehicles than they are for currency. See A Fairpo, "Taxation of Cryptocurrencies" in D Fox and S Green (eds), *Cryptocurrencies in Public and Private Law* (OUP, 2019).

12 https://www.theguardian.com/technology/2020/jan/21/bank-of-england-to-consider-adopting-cryptocurrency.

13 The Investigatory Powers Act 2016, s 261(3) to (5) uses the term "communications data", which comprises "entity data" (data which identifies or describes a person or thing) and "events data" (data which identifies or describes an event).

For instance, where a document is created in Microsoft Word, the document will exist in native form as a .doc or .docx file. This will likely enable a person to view metadata about the file, such as when it was created and by whom. Electronic data may also exist in a foreign format. For example, if the Microsoft Word document was printed out, scanned, or converted into a PDF format, the file would exist digitally as a picture with a loss of original metadata.

14.23 The accessibility of electronic data to humans may depend on a number of factors. Data may be "hidden data" or "trace data", which can only be accessed by specialists or with specialist equipment. Access to data may also be protected by a number of security features.

(1) Conventional passwords involve a string of characters (letters, numbers and symbols) used for authenticating a user and permitted access to electronic devices or online accounts. Some devices now include biometric authentication: for example, Apple smartphones may use Touch ID and Face ID where a fingerprint or facial recognition unlocks the device or permits access to an online account.

(2) Two-factor authentication, or "2FA" in shorthand, is a security process in which users provide two different authentication factors to verify themselves. Possible verification factors include knowledge factors (such as a PIN or password); possession factors (such as a code generated by a card reader or mobile phone); and inherence factors (such as fingerprint readers, retina scanners, voice recognition, and other forms of biometric data). For example, once a user enters their password for an online banking account, they may be sent a text or email to a pre-disclosed mobile phone number or email address with a code to enter the account. Two-factor authentication has become an increasingly common security feature of online accounts. Some online accounts may use three-factor authentication in order to provide an extra layer of security.

(3) Encryption is the process of encoding data or information in a way that is intended to prevent access to that data by any unauthorised person. Encryption has also become more common as a security feature. Manufacturers of electronic devices are adopting operational systems that encrypt information by default. Service providers are also increasingly offering automatic encryption of data stored in remote storage systems of a kind that prevents even the service providers from being able to decrypt the data.

14.24 For remotely stored data to be retrievable, a connection must exist between the remote server and the device from which access is sought. Electronic data can also be deleted from electronic devices remotely.

Remotely stored data

14.25 Networks, such as local area networks and the internet, mean that electronic data can be accessible from an electronic device yet stored remotely. A greater amount of data is now stored remotely owing to the popularity of "cloud computing", a term used to describe the storage of data on remote servers. These servers are physically hosted in what are termed data centres, server rooms or server farms.

14.26 It is estimated that approximately 2.3 billion people worldwide now use personal remote storage,[14] and that approximately 94% of businesses in the world use remote storage.[15] It is estimated that, in 2020, there is now more data stored by individuals in public remote storage environments than on their electronic devices.[16]

14.27 Electronic devices increasingly rely on remote storage. There are some electronic devices, such as the "Chromebook" laptop, which have very little local storage but instead rely on remote storage.

14.28 A large proportion of remotely stored data is managed, processed and stored in the United States as this is where the data centres of popular companies are located, such as Facebook, Microsoft, Apple, Google and Dropbox. However, these companies maintain an ever-expanding network of data centres all over the world. For example, Google is currently building its second data centre on the island of Taiwan.[17] It is not just on land that data centres may be located: Microsoft has recently obtained a patent to build data centres on the ocean floor incorporated within an artificial reef.[18] Some technology experts consider that in the future data centres may be located in outer space.[19]

14.29 The location of data will have implications for the laws and regulations which apply. Territories will regulate data within their jurisdiction differently, whether it be in the context of criminal law or copyright law. This has also led to the notion of "data havens", whereby data is stored on secure servers in locations where fewer, or more favourable, legal restrictions apply.

14.30 We discuss the implications of remotely stored data in more detail in Chapter 16. In one sense, it is misleading to describe data as having a location. The location of data may change during the course of a day as it is effortlessly transferred and duplicated from data centre to data centre by a service provider for security reasons or to allocate storage capacity efficiently. The data comprising a file may also be fragmented across several jurisdictions. In some cases, in can be difficult for a user or investigator to ascertain in which country particular electronic data is located. The location of electronic data may therefore be both unknown and unknowable.

14.31 It is also worth noting that, from a legal perspective, there may be as many as three potential relevant parties when remotely stored electronic data is concerned: (1) the individual or user who generates the electronic data; (2) the service provider who manages, processes or stores the electronic data; and (3) the state on whose territory the storage facility that stores the electronic data is located.

---

14 https://www.statista.com/statistics/499558/worldwide-personal-cloud-storage-users/.

15 https://media.flexera.com/documents/rightscale-2019-state-of-the-cloud-report-from-flexera.pdf?elqTrackId=372b6798c7294392833def6ec8f62c5c&elqaid=4588&elqat=2&_ga=2.75255952.381106268.1556868633-1445624021.1556868633.

16 https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf at p 10. Public remote storage (often referred to as "public clouds") are owned and operated by third-party service providers. Private remote storage ("private clouds") are maintained on a private network and used exclusively by a business or organisation, although may be hosted by a third-party service provider.

17 See https://asia.nikkei.com/Business/Technology/Google-boosts-Taiwan-data-center-plans-with-850m-investment.

18 See https://www.patentlyapple.com/patently-apple/2020/01/microsoft-wins-a-patent-for-an-environmentally-friendly-ocean-floor-artificial-reef-datacenter.html.

19 See https://www.dsm.net/it-solutions-blog/is-the-future-of-data-centers-in-space.

AN OVERVIEW OF THE RELEVANT LEGAL REGIMES GOVERNING THE ACQUISITION AND TREATMENT OF ELECTRONIC MATERIAL

14.32 This project concerns the law of search warrants. The primary conduct authorised by a search warrant is entry, search and seizure. When electronic material is concerned, however, there are a number of investigation powers under a range of different legal regimes that may be used both prior to and during, or in the alternative to, the execution of a search warrant. These powers allow investigators to request and compel the production of or access to information, interfere with electronic devices and intercept electronic data. We therefore use the term "acquisition" in a broad sense to cover this broad range of conduct.

14.33 There are also a number of legal regimes which set standards, limit and otherwise regulate the acquisition and subsequent treatment of electronic material under a search warrant or other investigation powers. These standards emanate from both domestic and international law.

14.34 We refer to the legal regimes which govern the acquisition and treatment of electronic material as "relevant legal regimes". In this section, we provide an overview of these relevant legal regimes. We do so for several reasons; first, to equip the reader with a broader understanding of the laws which interact with search warrants legislation and to provide essential context for our discussions in the ensuing chapters. Secondly, to enable the reader to understand fully the content of the responses to our consultation, several of which assume knowledge of these relevant legal regimes. Thirdly, to enable the reader to understand how our recommendations would interact with the wider legal framework.

14.35 The relevant legal regimes which we outline in this section are:

(1) powers to search for and seize electronic material under a search warrant;

(2) powers to search for and seize electronic under other statutory provisions;

(3) powers to access and operate electronic devices on premises;

(4) powers to require the production of or access to electronic material;

(5) powers to request legal assistance from other states;

(6) powers to intercept communications;

(7) powers to interfere with equipment and property;

(8) consent as a lawful basis for acquiring electronic material;

(9) powers to retain electronic material;

(10) the duty to provide a record of seized electronic material;

(11) the duty to sift electronic material;

(12) the duty to retain relevant material;

(13) the duty to pursue all reasonable lines of enquiry

(14) the duty to process electronic data lawfully;

(15) human rights law; and

(16) international law.

14.36 We also set out relevant Codes of Practice and guidance documents at the end of this section.

Powers to search for and seize electronic material pursuant to a search warrant

14.37 Criminal investigations now routinely involve the search for evidence stored in electronic form. The successful prosecution of offences including child abuse and exploitation, terrorism, fraud and sexual offences are likely to depend on electronic evidence. Search warrants under the Police and Criminal Evidence Act 1984 ("PACE") and other legislative enactments are therefore commonly applied for to obtain electronic data.

14.38 There are approximately 176 different search warrant provisions. A large proportion of search warrants legislation pre-dates the widespread use of electronic devices and the internet. For example, PACE was enacted in 1984. While sporadic legislative amendments have sought to enable the law to apply to electronic material, several powers of search and seizure are not designed with the unique nature of electronic material in mind.

14.39 Searches for electronic material must therefore fit into the pre-existing law which concerns the search of premises for relevant material. It follows that it is possible to obtain a search warrant to search premises *for* an electronic device, or to search premises *for* electronic data. However, an investigator cannot obtain a warrant expressly authorising the search *of* an electronic device on premises for locally or remotely stored data. There are arguments both ways as to whether search warrants under certain provisions can be drafted in such a way so that electronic devices can be searched for electronic data while on premises. It is in our view even less likely that an investigator can obtain a conventional search warrant authorising the *remote* search of an electronic device (such as a server located within or outside the jurisdiction), which would involve no trespass on the premises on which the electronic device is located.[20]

14.40 Therefore, when an investigator seeks to obtain electronic data through a search warrant, they have two choices: either electronic devices or electronic data may be treated as the target of the warrant. This typically depends on the nature of the investigation and the preferences of particular agencies.

Electronic device warrants

14.41 The first option is to apply for a warrant authorising the search for, and seizure of, an electronic device. This is the most popular form of search warrant when electronic data is sought. The Magistrates Association survey of members revealed that 81% of warrants were drafted in terms of devices. An example of a warrant drafted in terms of electronic devices can be found in the case of *Fitzgerald v Preston Crown Court*, where the warrants authorised officers to search for:

[20] We discuss the arguments for such a power, and its existence as part of the search warrant regimes of other jurisdictions, in Chapter 18. Outside the search warrants context, lawful authority to search for and acquire electronic data may be conferred by a targeted equipment interference warrant under the Investigatory Powers Act 2016, which we discuss at paragraphs 14.57(1) and 14.65 to 14.67 below.

Any electronic storage devices, including but not exclusively mobile phones, computers, lap tops, iPads and any other digital or electronic storage devices.[21]

14.42 The reason why search warrants can be drafted in terms of electronic devices when electronic data is sought is because electronic devices and the data stored thereon are conceptualised as a single item (the "single item theory"). The single item theory has been developed and reaffirmed by the courts on several occasions in respect of different statutory regimes.[22]

14.43 In summary, the single item theory conceptualises an electronic device as a single storage entity. A computer is, on this view, like a book: the data is intrinsically linked with the physical hard drive in the same way that pages are bound to a spine, rather than a filing cabinet from which individual files can be removed. As a consequence, where an investigator seeks electronic data, the whole electronic device may be specified on the face of the warrant, subsequently searched for and then seized.

14.44 The single item theory is therefore a convenient legal fiction which serves a number of functions.

(1) It has allowed the courts to treat the statutory access conditions for the issue of certain search warrant provisions as being met. It has done so in two respects:

(a) Some search warrant provisions require reasonable grounds for believing that the target material is likely to be relevant evidence.[23] An electronic device may satisfy this requirement notwithstanding that it contains large amounts of irrelevant electronic data.[24]

(b) Some search warrant provisions require reasonable grounds for believing that the target material does not consist of or include certain categories of protected material, such as legally privileged material.[25] An electronic device may satisfy this requirement notwithstanding that it is likely to contain protected electronic data provided the wording of the warrant excludes the protected electronic data.[26]

(2) It has allowed electronic devices to be specified on the face of the warrant and meet the requirement under section 15(6)(b) of PACE that the warrant identify, so far as is

---

21 *Fitzgerald v Preston Crown Court* [2018] EWHC 804 (Admin) at [5].

22 *R (Paul Da Costa) v Thames Magistrates' Court* [2002] EWHC 40 (Admin) at [20], [2002] Crim LR 504; *Kent Pharmaceuticals Ltd v Serious Fraud Office* [2002] EWHC 3023 (QB) at [27]; *R (H) v Inland Revenue Commissioners* [2002] EWHC 2164 (Admin), [2002] STC 1354 at [37]; *R (Faisaltex Ltd) v Preston Crown Court* [2008] EWHC 2832 (Admin), [2009] 1 WLR 1687 at [79]; *R (Glenn & Co (Essex) Ltd) v HMRC* [2010] EWHC 1469 (Admin), [2011] 1 WLR 1964 at [32]; *R* (*Cabot Global Ltd) v Barkingside Magistrates' Court* [2015] EWHC 1458 (Admin), [2015] 2 Cr App R 26 at [34] and [38]; *Hargreaves v Brecknock and Radnorshire Magistrates' Court* [2015] EWHC 1803 (Admin), (2015) 179 JP 399 at [37]; *R (A) v Central Criminal Court and another* [2017] EWHC 70 (Admin) at [74], [2017] 1 WLR 3567 at [36]; and *Business Energy Solutions Ltd v The Crown Court at Preston* [2018] EWHC 1534 (Admin), [2019] Crim LR 860 at [75].

23 Police and Criminal Evidence Act 1984, s 8(1)(c).

24 *R* (*Cabot Global Ltd) v Barkingside Magistrates' Court* [2015] EWHC 1458 (Admin), [2015] 2 Cr App R 26 at [38].

25 Police and Criminal Evidence Act 1984, s 8(1)(d).

26 *R (A) v Central Criminal Court and another* [2017] EWHC 70 (Admin) at [81], [2017] 1 WLR 3567 at [43].

practicable, the articles sought.[27] An investigator need not specify on the warrant the electronic data stored on the device.

(3) If there may be protected material on an electronic device, this must be excluded (expressly or impliedly) on the face of the warrant.[28] If the sifting of protected material cannot reasonably be conducted on the premises, seizure of an electronic device should take place under the Criminal Justice and Police Act 2001 regime ("CJPA") as the device contains material which the investigator is not entitled to seize.[29]

14.45 When search warrants are drafted in terms of electronic devices, the search warrant permits a search *for* an electronic device. When electronic devices are located, the search will have been to the extent required for the purpose for which the warrant was issued.[30] Therefore, an electronic device can only be seized or copied on-site. To search an electronic device would require the consent of the owner of the device, unless there is an explicit statutory power to search the device.[31] Another option to obtain relevant data is to use a statutory power to require its production.[32]

14.46 Privacy concerns have been raised by virtue of the fact that investigators are permitted to specify only electronic devices on the face of a warrant and then seize those devices in their entirety. Law enforcement agencies may therefore acquire large volumes of potentially sensitive data only a fraction of which may be relevant to a criminal investigation. We discuss these concerns in more detail below at paragraphs 14.125 to 14.140 below.

Electronic data warrants

14.47 Electronic data can also be treated as the target material, with a search warrant authorising the search for, and seizure of, such data. The Magistrates Association survey of members revealed that 19% of warrants were drafted in terms of electronic data sought on devices. In practice, these types of warrants usually specify categories of electronic data, or categories of material which may exist in hard copy or electronic form. For example, we have had sight of a search warrant drafted in the following terms:

> All records, details, notes and files held whether on computer or otherwise …
>
> All files and correspondence whether by email, letter or otherwise … between customers and/or clients and …
>
> Any material recorded on servers accessible from the subject premises.

14.48 As stated at paragraph 14.39 above, there are arguments both ways as to whether search warrants under certain provisions can be drafted in such a way so that electronic devices can be searched for electronic data while on premises. Thus, it is arguable that a search warrant that authorises a search of premises for electronic data authorises a search *of* an electronic device. If not, an investigator would either have to obtain consent to search a

---

27 *R (A) v Central Criminal Court and another* [2017] EWHC 70 (Admin) at [81], [2017] 1 WLR 3567 at [43].

28 *R (A) v Central Criminal Court and another* [2017] EWHC 70 (Admin) at [84], [2017] 1 WLR 3567 at [46].

29 *R (A) v Central Criminal Court and another* [2017] EWHC 70 (Admin) at [100], [2017] 1 WLR 3567 at [61].

30 Police and Criminal Evidence Act 1984, s 16(8).

31 We discuss statutory powers to operate electronic devices at paragraphs 15.160 to 15.164 below.

32 We discuss statutory powers to require the production of electronic material at paragraphs 18.25 to 18.68 below.

device or seize the device under the CJPA to sift the electronic data off-site. Again, the investigator may also have the power to require the production of relevant electronic data.

14.49 Some search warrants are drafted in hybrid form, specifying both electronic devices and electronic data.

Powers to seize electronic material under other statutory provisions

14.50 When executing a search warrant, investigators may exercise other statutory powers which do not emanate from the authority of the warrant. Accordingly, electronic material may be seized under other statutory provisions. The following are the main statutory powers under which electronic material may be seized:

(1) under PACE, a constable may seize anything which they have reasonable grounds for believing (1) has been obtained in consequence of the commission of an offence or is evidence in relation to any offence; and (2) is necessary to seize in order to prevent it being concealed, lost, altered or destroyed;[33] and

(2) under the CJPA, a person may seize property which contains relevant material in order to sift the property off-site if it is not practicable to identify or segregate the relevant material on premises.[34]

Powers to operate electronic devices

14.51 There are statutory powers which go beyond the search *for* an electronic device and expressly authorise the operation *of* an electronic device. These powers may be exercised when executing a search warrant under particular regimes.

(1) Under schedule 15 to the Data Protection Act 2018, a search warrant authorises investigators, as well as to enter and search premises, to "inspect, examine, operate and test any equipment found on the premises".[35]

(2) Under the Consumer Rights Act 2015, an investigator who enters premises with or without a warrant[36] may, for the purpose of seizing documents required as evidence, require a person with authority to access any electronic device and, if that is not complied with, the officer may "access the electronic device".[37]

(3) Proposed amendments to the Environment Act 1996 would insert a new power permitting investigators "to operate any equipment found on the premises for the purposes of producing [information stored in electronic form and accessible from the premises]".[38]

---

33 Police and Criminal Evidence Act 1984, s 19(1).

34 Criminal Justice and Police Act 2001, s 50.

35 Data Protection Act 2018, sch 15, para 5(1).

36 Consumer Rights Act 2015, sch 5, para 24.

37 Consumer Rights Act 2015, sch 5, para 31.

38 Environment Bill 2019-2021, sch 10, para 5(2).

Powers to require production or access

14.52 There are a number of statutory powers which empower an individual to require the production of, or access to, electronic devices and/or electronic data. Again, these powers may be exercised while executing a warrant. Alternatively, some of these orders may be obtained instead of obtaining a search warrant.

(1) There are various powers to require production without a court order.

(a) Under PACE, a constable who is lawfully on premises may require the production of electronic data if they have reasonable grounds for believing (1) it has been obtained in consequence of the commission of an offence or is evidence in relation to any offence; and (2) it is necessary to require its production in order to prevent it being concealed, lost, altered or destroyed.[39]

(b) Under PACE, certain powers of seizure which apply to constables are construed as including a power to require electronic data to be produced in a visible and legible form.[40]

(c) Under other statutes, there are powers which permit persons other than constables to require the production of electronic material.[41]

There are particular ambiguities as to how the production powers under PACE operate, which we discuss in more detail at paragraphs 18.25 to 18.68 below.

(2) There are powers to apply to a court to obtain a production order under various statutes.[42] A production order typically requires a specified person to produce material within a specified period, give access to the material or state the material's location.

(3) Major investigative agencies can apply for an overseas production order against a person who has possession or control of electronic data, which requires the person to produce or provide access to the data.[43] Such a power can only be applied for where a designated international co-operation arrangement exists and permits such orders. At present, an agreement is only in place with the United States.[44]

(4) There are also powers to assist in obtaining access to electronic devices.

(a) Under the Regulation of Investigatory Powers Act 2000 ("RIPA"), there is a power to impose a disclosure requirement on a person believed to have a key,

---

39 Police and Criminal Evidence Act 1984, s 19(4).

40 Police and Criminal Evidence Act 1984, s 20(1).

41 Criminal Justice Act 1987, s 2(3); Financial Services and Markets Act 2000, ss 171 and 172; Consumer Rights Act 2015, sch 5, paras 14 and 27; Immigration Act 2016, s 48; Enterprise Act 2002, s 194; Competition Act 1998, ss 28A, 65F, 65G and 65H; Armed Forces (Powers of Stop and Search, Search, Seizure and Retention) Order 2009 (SI 2009 No 2056), art 14.

42 Police and Criminal Evidence Act 1984, sch 1; Terrorism Act 2000, sch 5; Proceeds of Crime Act 2000, s 345; Proceeds of Crime Act (External Investigations) Order 2014.

43 Crime (Overseas Production Orders) Act 2019, s 1(1).

44 Overseas Production Orders and Requests for Interception (Designation of Agreement) Regulations 2020 (SI 2020 No 38).

code, password, algorithm or other data which allows access to protected information.[45] Protected information is defined as any electronic data which, without the key to the data, cannot, or cannot readily, be accessed or put into intelligible form.[46] The definition of a "key" is also wide enough to cover cryptographic technology and biometric data.

(b) Under the Terrorism Act 2000, there is a power to request "any information",[47] which may include a password.[48]

Powers to request legal assistance from other states

14.53 Generally speaking, investigative powers cannot operate extraterritorially. For example, the police could not travel to execute a search warrant on premises outside of the UK. Clearly evidence in another jurisdiction could be relevant to a UK criminal investigation. In such instances, there are a number of tools which allow UK law enforcement agencies to request assistance from other states in order to obtain evidence in criminal investigations.

(1) Mutual legal assistance, namely the provision of assistance by one state to another in the investigation and prosecution of crime, is one avenue through which law enforcement agencies may seek to acquire electronic data.[49] Overseas electronic data may be compelled pursuant to a letter of request sent by the UK to a state where the data is stored. This avenue requires the requested state to consider and grant the request.

(2) European Investigation Orders allow EU Member States to request a specific criminal investigatory power be exercised by another state,[50] such as a search warrant. As the regime is based on the principle of mutual recognition, it provides a faster alternative to mutual legal assistance. Once the UK ceases to be an EU Member State, the UK will no longer have access to the European Investigation Order regime.[51]

Powers to intercept communications

14.54 The interception of "communications" (which includes, using our terminology, electronic data) is governed by the Investigatory Powers Act 2016 ("IPA"). There are two ways in which the law governing the interception of communications is relevant for search warrants. First, while intercept evidence is generally inadmissible in legal proceedings,[52] which would

---

45 Regulation of Investigatory Powers Act 2000, s 49.

46 Regulation of Investigatory Powers Act 2000, s 56(1).

47 Terrorism Act 2000, sch 7, para 5(a).

48 See *Rabbani v DPP* [2018] EWHC 1156 (Admin), [2018] 2 Cr App R 28.

49 C Nicholls, C Montgomery, J Knowles, A Doobay and M Summers, *Nicholls, Montgomery, and Knowles on The Law of Extradition and Mutual Legal Assistance* (3rd ed 2013) para 17.01.

50 Directive 2014/41/EU of the European Parliament and of the Council of 3rd April 2014 regarding the European Investigation Order in criminal matters (OJ No L 130, 1.5.2014, p.1); The Criminal Justice (European Investigation Order) Regulations 2017 (SI 2017 No 730).

51 Law Enforcement and Security (Amendment) (EU Exit) Regulations 2019 (SI 2019 No 742), reg 74.

52 Investigatory Powers Act 2016, s 56(1). The contents of a communication and secondary data may be disclosed if the communication is obtained through some but not all forms of lawful interception: see Investigatory Powers Act 2016, sch 3, para 2.

include a search warrant application hearing, it may assist in an investigation which leads to an application for a search warrant. Secondly, law enforcement may carry out conduct amounting to the interception of communications when executing a search warrant. This is because electronic data sought from electronic devices and remote storage accounts will fall under the definition of a communication and therefore engage the provisions of the IPA.[53]

14.55 A person may intercept "communications"[54] in the course of their transmission in the UK if they have lawful authority to do so. An interception takes place where a person performs a "relevant act"[55] in relation to a "telecommunication system"[56] and the effect of that act is to make any "content"[57] of the communication available at a "relevant time"[58] to a person who is not the sender or intended recipient of the communication.

14.56 The following are some of the instances in which a person has lawful authority to intercept communications that are relevant for present purposes.[59]

(1) A person has lawful authority where the interception is carried out in accordance with a targeted interception warrant, mutual assistance warrant, or bulk interception warrant.[60]

(a) A targeted interception warrant authorises or requires a person to secure the interception of communications, the obtaining of "secondary data"[61] (including

---

53 Depending on the delivery status of the electronic data, conduct undertaken when executing a search warrant may amount to (1) the interception of a communication stored in or by a telecommunication system (ie the interception of a "stored communication"); or (2) the interception of a communication that is being transmitted (ie a "live interception"). The interception of a stored communication is lawful if, amongst other circumstances, it is in exercise of a statutory power or in accordance with a court order such as a search warrant (Investigatory Powers Act 2016, s 6(1)(c)(ii) and (iii)), whereas a live interception can only be authorised by an interception warrant or under a limited set of additional circumstances (Investigatory Powers Act 2016, s 6(1)(a) and (b)).

54 Defined in Investigatory Powers Act 2016, s 135(1): "communication" includes (a) anything comprising speech, music, sounds, visual images or data of any description, and (b) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus.

55 Defined in Investigatory Powers Act 2016, s 4(2).

56 Defined in Investigatory Powers Act 2016, s 261(13).

57 Defined in Investigatory Powers Act 2016, s 261(6). Read with Investigatory Powers Act 2016, s 263(4), communications comprise two broad categories of data: (1) "systems data"; and (2) "content". Systems data, as defined in Investigatory Powers Act 2016, s 263(4), means any data that enables or facilitates, or identifies and describes anything connected with enabling or facilitating, the functioning of any systems or services. This will cover email addresses and user IDs.

58 Defined in Investigatory Powers Act 2016, s 4(4): "relevant time" means any time while the communication is being transmitted and any time when the communication is stored in or by the system (whether before or after its transmission). The relevant provisions of the Investigatory Powers Act 2016 that apply in a given case, and the circumstances in which a person has lawful authority to carry out an interception, depend on whether the relevant communication is (1) being transmitted; or (2) a stored communication.

59 Investigatory Powers Act 2016, Part 2, chapter 2 contains several forms of lawful interception (Investigatory Powers Act, ss 44 to 52), only two of which we discuss at paragraphs 14.56(2) (s 44) and 14.56(3) (s 52) below. The other forms of lawful interception, which are not relevant for present purposes, include interception by businesses for monitoring and record-keeping purposes (s 46) and interception by Ofcom in connection with wireless telegraphy (s 48).

60 Investigatory Powers Act 2016, s 6(1)(a).

61 Defined in Investigatory Powers Act 2016, ss 16 and 137: "secondary data" comprises "systems data" and "identifying data". Identifying data as, defined in Investigatory Powers Act 2016, s 263(2) and (3), is data which may

"related systems data"[62]) from communications or the disclosure of anything obtained under the warrant.[63] An "intercepting authority"[64] may apply to the Secretary of State for an interception warrant,[65] which requires various criteria to be met[66] and approval by a Judicial Commissioner[67] (unless the case is urgent[68]).

(b) A mutual assistance warrant authorises or requires an intercepting authority to make either a request for assistance in accordance with an EU mutual assistance instrument or an international mutual assistance instrument or to provide assistance in accordance with the same.[69]

(c) A bulk interception warrant requires the main purpose of the warrant to be intercepting "overseas-related communications"[70] and/or obtaining secondary data from such communications.[71] A bulk interception warrant may authorise the interception of overseas-related communications (and non-overseas-related communications where necessary or unavoidable[72]), the obtaining of secondary data and the selection for examination of intercepted content or secondary data obtained under the warrant.[73]

(2) A person has lawful authority where either the sender and the intended recipient of the communication have each consented to its interception (dual party consent);[74] or if either the sender or the intended recipient has consented (single party consent) and direct surveillance has been authorised under Part 2 of RIPA.[75]

---

be used to identify, or assist in identifying (a) any person, apparatus, system or service; (b) any event; or (c) the location of any person, event or thing.

62 Investigatory Powers Act 2016, s 15(5)(c). Defined in Investigatory Powers Act 2016, s 15(6): "related systems data" means systems data relating to a relevant communication or to the sender or recipient, or intended recipient of a relevant communication.

63 Investigatory Powers Act 2016, s 15(2).

64 Investigatory Powers Act 2016, s 18(1).

65 Investigatory Powers Act 2016, s 18(3).

66 Investigatory Powers Act 2016, ss 19 and 20. Investigatory Powers Act 2016, s 20(2): a targeted interception warrant (or targeted examination warrant) will satisfy the necessity requirement if the Secretary of State considers that the warrant is necessary in the interests of national security; for the purpose of preventing or detecting serious crime; or in the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security.

67 Investigatory Powers Act 2016, s 23.

68 Investigatory Powers Act 2016, s 24.

69 Investigatory Powers Act 2016, s 15(4).

70 Defined in Investigatory Powers Act 2016, s 136(3): "overseas-related communications" are communications sent or received by individuals who are outside the British Islands.

71 Investigatory Powers Act 2016, s 136(2).

72 Investigatory Powers Act 2016, s 136(5).

73 Investigatory Powers Act 2016, s 136(4).

74 Investigatory Powers Act 2016, s 44(1).

75 Investigatory Powers Act 2016, s 44(2).

(3) A person has lawful authority where the interception is carried out in response to a request made in accordance with a relevant international agreement.[76]

14.57 In addition to the cases listed immediately above, a person has lawful authority to intercept a *stored* communication (ie "a communication stored in or by a telecommunication system") in a further three cases.[77]

(1) A person has lawful authority if the interception is carried out in accordance with a targeted or bulk *equipment interference* warrant.[78] We discuss equipment interference in the section below.

(2) A person has lawful authority if the interception is in the exercise of any statutory power that is exercised for the purpose of obtaining information or taking possession of any document or other property.[79] This is said to cover instances where law enforcement agencies search an electronic device pursuant to a search warrant or require the production of electronic data.[80]

(3) A person has lawful authority if the interception is carried out in accordance with a court order made for that purpose.[81]

14.58 It is an offence intentionally to intercept a communication in the course of its transmission, via a public telecommunications system, a private telecommunications system or a public postal service, without lawful authority.[82]

14.59 It is also instructive here to make reference to the Computer Misuse Act 1990 ("CMA 1990"). Sections 1 to 3A of the CMA 1990 contain offences pertaining to "unauthorised access" of or "unauthorised acts" in relation to a computer. For example, it is an offence under section 1 of the CMA 1990 for a person to cause a computer to perform a function with intent to secure unauthorised access and where such person knows that the intended access would be unauthorised. The term "computer" is left undefined so as to prevent any definition becoming obsolete by technological advancement. Lord Hoffmann defined a computer as "a device for storing, processing and retrieving information".[83]

14.60 Section 10 of the CMA 1990 provides that certain law enforcement powers are exempt from the ambit of the CMA 1990 offences, namely:

> Powers of inspection, search or seizure or of any other enactment by virtue of which the conduct in question is authorised or required.[84]

---

76 Investigatory Powers Act 2016, s 52. See the Overseas Production Orders and Requests for Interception (Designation of Agreement) Regulations 2020 (SI 2020 No 38).

77 Investigatory Powers Act 2016, s 6(1)(c).

78 Investigatory Powers Act 2016, s 6(1)(c)(i).

79 Investigatory Powers Act 2016, s 6(1)(c)(ii).

80 Home Office, *Interception of Communications Code of Practice* (March 2018) para 12.14.

81 Investigatory Powers Act 2016, s 6(1)(c)(iii).

82 Investigatory Powers Act 2016, s 3(1).

83 *DPP v McKeown*, *DPP v Jones* [1997] 2 Cr App R 155, 163.

84 Computer Misuse Act 1990, s 10(a).

It follows that where an electronic device is accessed following the execution of a search warrant pursuant to a power which confers such authority, no offence is committed under the CMA 1990.

Powers to interfere with equipment and property

14.61 The interference with electronic devices is principally governed by two regimes. What is called "equipment interference" is governed by IPA, whereas "property interference" is governed by Part III of the Police Act 1997 and the Intelligence Services Act 1994.

14.62 The terms "equipment" and "property" can both be read as covering electronic devices for present purposes.[85] Whether interference falls into either category depends on the purpose for which the interference occurs rather than the material that is the subject of the interference. Generally speaking, where the main purpose of the interference is to obtain electronic data, the conduct will constitute equipment interference, otherwise the conduct will constitute property interference. For example, property interference will be engaged where the purpose of interference is to disable or neutralise an electronic device. The relevance of these legal regimes is that conduct amounting to equipment interference or property interference may occur when executing a search warrant.

Equipment interference

14.63 IPA provides a statutory framework for authorising equipment interference when the European Convention on Human Rights ("ECHR") and/or the CMA 1990 are likely to be engaged. Equipment interference encompasses a broad range of techniques, such as accessing electronic devices remotely to extract electronic data, using a person's login credentials to access electronic data and downloading electronic data from an electronic device.

14.64 More specifically, the equipment interference regime applies where (1) the object with which a person interferes falls within the definition of "equipment"; and (2) the purpose of the equipment interference, and not merely an incidental effect, is to obtain "communications",[86] "equipment data"[87] or other information.

14.65 Equipment interference techniques may amount to conduct which constitutes an offence under the CMA 1990.[88] A person cannot apply for property interference authorisation under Part III of the Police Act 1997 and instead must obtain an equipment interference warrant where (1) the purpose of the interference is to obtain communications, information or equipment data; and (2) the conduct would otherwise constitute one or more offences under the CMA 1990.[89] Property interference can therefore still be used where, say, the purpose of

---

85 Investigatory Powers Act 2016, ss 135(1) and 198(1): "equipment" means equipment producing electromagnetic, acoustic or other emissions or any device capable of being used in connection with such equipment.

86 See footnote 54 above.

87 Defined in Investigatory Powers Act 2016, s 100: "equipment data" means (1) "systems data" (for which see footnote 57); and (2) "identifying data" (for which see footnote 61) which is capable of being logically separated from a communication or other item of information to which it is associated without revealing the meaning of the said communication or information. See also Home Office, *Covert Surveillance and Property Interference Code of Practice* (August 2018) paras 2.22 to 2.23; Home Office, *Equipment Interference Code of Practice* (March 2018) paras 3.37 to 3.38.

88 We discuss the Computer Misuse Act 1990 at paragraphs 14.59 and 14.60 above.

89 Investigatory Powers Act 2016, s 14.

the interference is to disable or neutralise an electronic device so that it cannot be used in the commission of serious crime.

14.66 It follows from the above that an equipment interference warrant is not mandatory where the conduct amounting to interference is authorised by a warrant or other statutory power as, by virtue of section 10 of the CMA 1990, an offence will not be committed.[90]

14.67 Equipment interference warrants authorise physical and remote interference with any equipment for the purpose of obtaining communications or equipment data. As mentioned at paragraph 14.57(1) above, an equipment interference warrant also confers lawful authority on a person to intercept a *stored* communication (ie "a communication stored in or by a telecommunication system").[91] Where equipment interference activity amounts to the interception of the content of a live communication (ie a communication in the course of its transmission) an interception warrant must be obtained. Again, neither warrant is necessary where the conduct amounting to equipment interference or interception is authorised by a warrant or other statutory power.

Property Interference

14.68 Part III of the Police Act 1997 provides that interference with property is lawful if it is authorised under that Part.[92] As indicated at paragraphs 14.64 and 14.65 above, property interference cannot be used by law enforcement agencies where the main purpose of interference with an electronic device is to acquire communications or equipment data. Instead, property interference concerns other non-acquisition purposes, such as to disable an electronic device, in which the acquisition of communications or equipment data may be incidental to the main purpose of the interference.[93]

14.69 Where an "authorising officer"[94] believes that (1) it is necessary to take action for the purpose of preventing or detecting serious crime; and (2) that the taking of such action is proportionate to what the action seeks to achieve, they may authorise the taking of such action in respect of property.[95]

14.70 In an urgent case, where it is not reasonably practicable for an authorising officer to consider an application, authorisation may be exercised by certain other officers.[96] An authorisation shall be in writing, except that in an urgent case an authorisation (other than one given by virtue of section 94) may be given orally.[97] Authorisation persists for three months for law

---

90 Home Office, *Equipment Interference Code of Practice* (March 2018) paras 3.26 to 3.27.

91 Investigatory Powers Act 2016, s 6(1)(c)(i).

92 Police Act 1997, s 92.

93 Home Office, *Equipment Interference Code of Practice* (March 2018) paras 3.37 to 3.40.

94 Defined in the Police Act 1997, s 93(5).

95 Police Act 1997, s 93(1) and (2). The authorising officer must consider whether the end result could reasonably be achieved by other means: see Police Act 1997, s 93(2B).

96 Police Act 1997, s 94.

97 Police Act 1997, s 95(1).

enforcement agencies (or 72 hours if given orally or by virtue of section 94).[98] Written notice of an authorisation must be given to a Judicial Commissioner.[99]

14.71 Additional approval by a Judicial Commissioner is required in certain non-urgent cases where (1) the relevant premises constitutes office premises or a dwelling; or (2) the action is likely to result in any person acquiring knowledge of legally privileged material, confidential personal information or confidential journalistic material.[100] A Judicial Commissioner may cancel, quash or renew authorisation.[101] Authorising officers may appeal against certain decisions made by Judicial Commissioners.[102]

Consent as a lawful basis for acquiring electronic material

14.72 Where it is not practicable to exercise a power of seizure or production, an investigator may seek to acquire electronic material by consent of the owner of the electronic device or data. In some circumstances, legislation provides for consent as a lawful ground for acquiring electronic material. For example, as mentioned at paragraph 14.56(2) above, a person has lawful authority to intercept communications where either the sender and the intended recipient of the communication have each consented to its interception (dual party consent);[103] or if either the sender or the intended recipient has consented (single party consent) and direct surveillance has been authorised under Part 2 of RIPA.[104] Be that as it may, specific data protection issues are engaged by acquiring electronic material through consent. The Information Commissioner's Office has also recently criticised the use of consent as a lawful basis for processing data.[105]

Powers to retain material

14.73 There are a number of overlapping regimes governing the retention of seized material. One or more of these regimes is likely to apply when material is seized following the execution of a search warrant.

(1) Under PACE, there is a general power for constables to retain seized or produced material for so long as is necessary.[106] Where seizure is for the purposes of a criminal investigation, material may be retained for use as evidence at a trial for an offence, for forensic examination or for investigation in connection with an offence.[107] Nothing may

---

98 Police Act 1997, s 95(2). Intelligence agency authorisations last for six months (Intelligence Agencies Act 1994, s 6(2)).

99 Police Act 1997, s 96(1).

100 Police Act 1997, s 97.

101 Police Act 1997, s 103.

102 Police Act 1997, s 104.

103 Investigatory Powers Act 2016, s 44(1).

104 Investigatory Powers Act 2016, s 44(2).

105 Information Commissioner's Office, *Investigation report: Mobile phone data extraction by police forces in England and Wales* (June 2020) pp 53 and 54. Available at https://ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/.

106 Police and Criminal Evidence Act 1984, s 22.

107 Police and Criminal Evidence Act 1984, s 22(2)(a). See also Code B of PACE (2013) para 7.14.

be retained for these purposes if a photograph or copy would be sufficient for that purpose.[108]

(2) Comparable requirements to those above are set out in Code B of PACE.[109] Those who seize material pursuant to a warrant who do not hold the office of constable will therefore be likely to have similar procedures.

(3) Under investigative statutory regimes other than PACE, there may be separate specific powers for investigators to retain seized material.[110]

(4) Under the CJPA, there is a separate general power for constables to retain seized material where it is necessary in order to avoid it being concealed, lost, altered or destroyed.[111]

(5) Under the CJPA, where material is seized pursuant to sections 50 and 51 of the CJPA, there exists a power to retain inextricably linked material where it is not reasonably practicable to separate the material.[112]

14.74 Where seizure is made under sections 50 or 51 of the CJPA in lieu of a power of seizure which otherwise would have been subject to a separate scheme with duties of retention, such as section 22 of PACE, those duties will apply if the scheme is listed in the CJPA.[113] Nothing in the CJPA scheme permits the retention of material which would not be authorised by the separate schemes.

The duty to provide a record of material seized

14.75 When those conducting a criminal investigation seize material, such as following the execution of a search warrant, this may trigger a duty to provide a record of what was seized. This duty arises under different regimes.

(1) Under PACE, where material has been seized in the exercise of a power conferred by any enactment, a constable must, if requested, provide an occupier, or person with custody and control of material immediately before the seizure, with a record of what was seized.[114] Where electronic devices are seized, the duty does not extend to the provision of a composite item by item breakdown of the contents of an electronic storage device.[115] The record must be provided within a reasonable time.[116] A person should be granted access to seized material, allowed to copy it or be provided with a

---

108 Police and Criminal Evidence Act 1984, s 22(4).

109 Code B of PACE (2013) para 7.14.

110 Financial Services and Markets Act 2000, s 176A; Knives Act 1997, s 5(4).

111 Criminal Justice and Police Act 2001, s 50.

112 Criminal Justice and Police Act 2001, s 53.

113 Criminal Justice and Police Act 2001, s 57.

114 Police and Criminal Evidence Act 1984, s 21(1).

115 *Business Energy Solutions Ltd v Crown Court at Preston* [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [116].

116 Police and Criminal Evidence Act 1984, s 21(2).

copy if they so request,[117] unless to do so would prejudice an investigation or proceedings.[118]

(2) Comparable requirements are contained in Code B of PACE.[119] Persons other than police officers who are charged with the duty of investigating offences or charging offenders shall in the discharge of that duty have regard to any relevant provision of a code.[120] For this reason, other investigators who seize material for the purpose of a criminal investigation will be likely to have similar procedures in place.

(3) Under various specific investigative statutory regimes other than PACE, separate duties to provide a record of what was seized arise.[121]

(4) Where seizure occurs under the CJPA, section 52 of that Act requires an investigator to give an occupier or other persons a notice specifying what has been seized, on what grounds, how to apply for its return and attend the initial examination. This seems to be in addition to the duty to provide on request a record of what was seized under PACE. Following the reasoning of Green J, as he then was, in *Business Energy Solutions*,[122] the duty is unlikely to extend to the provision of a composite item by item breakdown of the material seized.

14.76 The Divisional Court has held that non-compliance with the safeguards under section 52 of the CJPA does not necessarily render a seizure under section 50 unlawful. It is a matter to be taken into account on an application under section 59, in judicial review proceedings or under section 78 of PACE to exclude evidence at trial.[123]

The duty to sift electronic material

14.77 A distinct legal regime governs the sifting of seized material where seizure is made under sections 50 or 51 of the CJPA or under a power to which those sections apply.[124] These seizure powers may be exercised following the execution of a search warrant. Section 53 of CJPA sets out how the initial off-site examination of the property seized under sections 50 and 51 of CJPA should take place and what can be retained. Imaging an electronic device amounts to the seizure of any copies made.[125]

(1) An initial examination of the property must be carried out as soon as reasonably practicable, it must be confined to whatever is necessary to determine how much of

---

117 Police and Criminal Evidence Act 1984, s 21(3) to (4).

118 Police and Criminal Evidence Act 1984, s 21(8).

119 Code B of PACE (2013) para 7.16.

120 Police and Criminal Evidence Act 1984, s 67(9).

121 For example, Consumer Rights Act 2015, sch 5, para 28(4)(b).

122 *Business Energy Solutions Ltd v Crown Court at Preston* [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [116].

123 *R (Dulai) v Chelmsford Magistrates' Court* [2012] EWHC 1055 (Admin), [2013] 1 WLR 220 at [52].

124 See Criminal Justice and Police Act 2001, sch 1.

125 *Business Energy Solutions Ltd v Crown Court at Preston* [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [76].

the property can be retained, and in isolation from material seized under any other powers of seizure.[126]

(2) Anything found on that initial examination which cannot lawfully be retained must be separated and returned. As the word “return” has been construed to include within it the idea that no trace or residue of the property is to be left with the authority, the duty to return material not within the scope of the original warrant may include an obligation to delete copied electronic data.[127] The duty to return material applies to each individual copied file as it does to the original device.[128]

(3) Seized property can be retained if it falls within one of the following three categories:

(a) the seized property is property for which the person seizing it had power to search when seizure was made (for example, the seized property falls within the scope of the search warrant);

(b) the retention of the seized property is authorised under section 56 of CJPA; or

(c) the material is something which, in all the circumstances, it will not be reasonably practicable, following the examination, to separate from property falling within either of the two categories above.

(4) The task of determining what material falls outside the scope of the warrant is subject to a broad "reasonable practicability of separation" test. Therefore, investigators need not necessarily undertake the Herculean task of segregation, even if technically possible to do so.[129]

14.78 Section 53 of the CJPA only applies where material has been seized under sections 50 or 51 of the CJPA. Therefore, where a device is specified and subsequently seized under the authority of a search warrant, rather than under section 50 or 51 of the CJPA, the section 53 safeguards do not apply.

The duty to retain relevant material

14.79 Separate duties for investigators arise under the Criminal Procedure and Investigations Act 1996. Section 23(1) of the Act makes provision for the publication of a Code of Practice which sets out how police officers are to record, retain and reveal to the prosecutor material obtained in a criminal investigation, which will include material seized following the execution of a search warrant. As with Code B of PACE, the Code applies only to police officers but other investigators are required to “have regard to it”.

14.80 There is a duty to retain relevant material, or copies of relevant material.[130] That is material which appears to an investigator to have some bearing on any offence under investigation, any person being investigated or on the surrounding circumstances of the case.[131]

---

126 Criminal Justice and Police Act 2001, s 53(2)(a), (b) and (d).

127 *Business Energy Solutions Ltd v Crown Court at Preston* [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [83].

128 *Business Energy Solutions Ltd v Crown Court at Preston* [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [75].

129 *Business Energy Solutions Ltd v Crown Court at Preston* [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [98].

130 CPIA Code of Practice, para 5.1.

14.81 In the context of digital investigations, the Attorney General's Guidelines on Disclosure provide detailed guidance on the procedures to be covered across multiple pieces of legislation. The Guidelines state:

> Where material is retained for evidential purposes there will be a strong argument that the whole thing (or an authenticated image or copy) should be retained for the purpose of proving provenance and continuity.[132]

Therefore, data seemingly falling outside the scope of a warrant may nonetheless constitute relevant material for the purpose of the CPIA.

14.82 All material which may be relevant to the investigation must be retained until a decision is taken whether to commence a prosecution.[133] If a criminal investigation results in a prosecution, all material which may be relevant must be retained at least until the accused is acquitted or convicted or the prosecutor decides not to proceed with the case.[134]

14.83 The duty to retain material in the CPIA is subject to section 22 of PACE (that material may be retained so long as is necessary in all the circumstances), if that applies to the power under which material is seized.[135]

The duty to pursue all reasonable lines of enquiry

14.84 There is a duty on investigators to pursue all reasonable lines of enquiry, whether they point towards or away from the suspect.[136] Accordingly, where material is held on a computer, it is a matter for the investigator to decide which material on the computer it is reasonable to inquire into, and in what manner.[137]

The duty to process data lawfully

14.85 The provisions in Part 3 of the Data Protection Act 2018 on "law enforcement processing" are engaged where personal data is processed by law enforcement, who are deemed a "competent authority" for the purposes of the Act.[138] Personal data will be "processed" within the meaning of the Act where it is acquired and subsequently stored and used.[139] Therefore, where material is seized following the execution of a search warrant, it will be "processed" within the meaning of the Data Protection Act 2018.

---

131 CPIA Code of Practice, para 2.1.

132 Attorney General's Guidelines on Disclosure: Supplementary Guidelines on Digitally Stored Material (2011), para A26. See also *Business Energy Solutions Ltd v Crown Court at Preston* [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [111].

133 CPIA Code of Practice, para 5.7.

134 CPIA Code of Practice, para 5.8.

135 CPIA Code of Practice, para 5.2.

136 CPIA Code of Practice, para 3.5.

137 CPIA Code of Practice, para 3.5.

138 Data Protection Act 2018, s 30(1).

139 Data Protection Act 2018, s 3(4).

14.86 “Personal data” means any information relating to an identified or identifiable living individual.[140] The Data Protection Act 2018 applies key safeguards to the processing of all personal data.[141] By section 34(3) of the Data Protection Act 2018, the law enforcement agency as data controller, “‘must be able to demonstrate its compliance with’ the six data protection principles and the two safeguarding measures set out at sections 35 to 42 of the Act.”[142]

14.87 Particular safeguards apply to “sensitive processing”,[143] which involves the processing of special category data. Personal data is “special category data”[144] if it concerns:

(1) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(2) genetic data, or biometric data, for the purpose of uniquely identifying an individual;

(3) data concerning health; and

(4) data concerning an individual's sex life or sexual orientation.

Human rights law

14.88 Section 6 of the Human Rights Act 1998 makes it unlawful for a public authority to act in a way which is incompatible with the ECHR.[145] Powers of search and seizure predominantly engage article 8 of the ECHR (the right to respect for private life). Such conduct may also engage article 1 of the First Protocol, the right to peaceful enjoyment of possessions, article 10 of the ECHR, freedom of expression, and article 6 of the ECHR, the right to a fair trial, which encompasses the right to remain silent and the privilege against self-incrimination.

14.89 As mentioned, article 8 of the ECHR is the right most likely to be engaged. For an interference with article 8 of the ECHR to be justified, it must satisfy a trilogy of tests: it must be in accordance with law; the interference must pursue a legitimate aim; and it must be necessary in a democratic society.[146] This translates in a domestic setting to the requirements of lawfulness[147] and proportionality.[148]

14.90 There are several matters which are particularly relevant when considering the acquisition and treatment of electronic material. In relation to the use of technology in criminal investigations, the Grand Chamber of the European Court of Human Rights has said:

---

140 Data Protection Act 2018, s 3(2).

141 *R (Catt) v Association of Chief Police Officers* [2015] UKSC 9, [2015] AC 1065 at [8].

142 *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin), [2020] 1 WLR 672 at [85] to [88].

143 Data Protection Act 2018, s 35(3).

144 Data Protection Act 2018, s 10; General Data Protection Regulation (EC) No 679/2016, Official Journal L 119 of 4.5.2016 p 1, art 9.

145 Professor Richard Stone; Northumbria Law School Centre for Evidence and Criminal Justice Studies; Serious Fraud Office.

146 *Beghal v DPP* [2015] UKSC 49, [2016] AC 88 at [119].

147 *R (Gillan) v Commissioner of Police of the Metropolis* [2006] UKHL 12, [2006] 2 AC 307 at [31] and [34]. See also *R (Bridges) v Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin), [2020] 1 WLR 672 at [80].

148 *Bank Mellat v Her Majesty's Treasury (No 2)* [2013] UKSC 39, [2014] AC 700 at [20] and [72].

> The protection afforded by art 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests … any state claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.[149]

14.91 Additionally, the Strasbourg Court has said the following regarding the treatment of electronic data:

> The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored. The domestic law must also afford adequate guarantees that retained personal data was efficiently protected from misuse and abuse. The above considerations are especially valid as regards the protection of special categories of more sensitive data.[150]

14.92 The seizure of entire devices, and use of data extraction methods, which may involve the processing of large amounts of data, therefore requires adequate safeguards.

International law

14.93 The search, seizure and production of data stored remotely overseas also engages principles of international law. Law enforcement agencies cannot act in a way that is incompatible with international law. However, the application to cyberspace of international law principles, such as territoriality and jurisdiction, is challenging.

14.94 As a result, there are no clearly defined rules regarding when powers of enforcement can be exercised in respect of overseas data. Instead, states have been left to determine their own practice by enacting domestic legislation. We discuss the application of international law to electronic material in detail in Chapter 16, which examines the search and seizure of remotely stored material.

Codes of practice and guidance documents

14.95 In addition to the relevant legal regimes that we have detailed above, there are a number of guidance documents and codes of practice pertaining to digital investigations:

(1) The Attorney General's Supplementary Guidelines on Digitally Stored Material, issued in 2011, supplement the Attorney General's Guidelines on Disclosure.[151] The objective of the guidelines is to set out how material satisfying the tests for disclosure can best be identified and disclosed to the defence without imposing unrealistic or disproportionate demands on the investigator and prosecutor.

---

149 *S and Marper v United Kingdom* (2009) 48 EHRR 50 (App No 30562/04) at [112].

150 *S and Marper v United Kingdom* (2009) 48 EHRR 50 (App No 30562/04) at [103].

151 Attorney General's Guidelines on Disclosure: Supplementary Guidelines on Digitally Stored Material (2011). See also, related, the Crown Prosecution Service, *Disclosure – Guidelines on Communications Evidence* (2018).

(2) The Association of Chief Police Officers (the predecessor to the National Police Chiefs' Council ("NPCC")) Good Practice Guide for Digital Evidence, last updated in 2012, sets out certain principles and best practice in respect of digital evidence.[152]

(3) The Forensic Science Regulator produces codes of practice which detail standards and norms of practice to be adhered to by all forensic science practitioners.[153] These include procedures regarding the acquisition, storage, transfer and disposal of electronic data.[154]

(4) The NPCC has produced guidance which sets out requirements regarding the storage, retention and destruction of records and materials that have been seized for forensic examination.[155]

14.96 Individual law enforcement agencies will likely produce their own internal guidance and formulate their own policies on digital investigations tailored to their organisational structure and digital capabilities.

HOW SEARCHES UNDER WARRANT FOR ELECTRONIC MATERIAL OPERATE IN PRACTICE

14.97 With an understanding of the nature of electronic material and the relevant legal regimes which apply to its acquisition and treatment, it is instructive to consider how searches under warrant operate in practice. This requires consideration of digital forensics, the process by which electronic data is extracted from electronic devices and processed for the purpose of obtaining intelligence or for use in criminal proceedings.

14.98 There is no unitary approach which law enforcement agencies take to the execution of search warrants where electronic material is involved. The particular facts of the investigation, digital forensic capabilities of the investigator and internal organisational working practices will all influence how investigations are undertaken where the target material is electronically stored.

14.99 The above being said, there are a number of common features to digital investigations; we provide an overview below. It is also worth mentioning that, on 1 April 2020 a new "Forensic Capability Network" was launched in England and Wales, which aims to deliver specialist forensic science capabilities and share knowledge to create a more unified approach between police forces and boost standards in forensics.

The point at which electronic data extraction takes place

14.100 Where searches of premises are planned in which it is expected that electronic devices will be present, law enforcement agencies may be assisted by digital forensic investigators. These investigators specialise in the recovery and interpretation of electronic data.

---

152 ACPO, *Good Practice Guide for Digital Evidence (Association of Chief Police Officers* (2012).

153 Forensic Science Regulator, *Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System* (2000).

154 Forensic Science Regulator, *Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System* (2000) para 23.

155 NPCC, *Guidance Regarding the Storage, Retention and Destruction of Records and Materials That Have Been Seized for Forensic Examination* (2017).

14.101 Electronic devices may be "imaged" (ie the electronic data copied) while officers are on the premises executing the search warrant. Evidentially, there are benefits to imaging devices on premises: when an electronic device is powered on, investigators may have access to the volatile electronic data within the primary storage of the device. Also, while an electronic device is powered on, officers may benefit from a lack of encryption and/or password protection. Accordingly, otherwise irretrievable electronic evidence may be acquired by imaging the electronic device on the premises.

14.102 It is usually not possible, however, to examine electronic devices on-site for several reasons.

(1) The law enforcement agency may not know what electronic devices are on the premises, or their level of security, and so may not have the requisite digital forensic equipment to extract the target electronic data.

(2) Even with such equipment, electronic devices may be powered off, password protected or encrypted such that electronic data cannot be extracted.[156]

(3) Where extraction is possible, the sheer volume of electronic data may render it impracticable to extract the data on premises. The data extraction devices brought on to the premises may also not be sophisticated enough to target search a device and copy only part of the data on it.

(4) Seizing the electronic device itself may also be necessary in order to:

(a) prove provenance and maintain forensic integrity; and/or

(b) pursue all reasonable lines of enquiry, for example if an initial examination reveals the need for a more detailed examination, or other information generated during the course of the investigation indicates that an electronic device requires a more detailed examination.

14.103 For most search warrant investigations, therefore, instead of imaging devices on the premises, devices will be seized and forensic examination will be carried out "off-site".

14.104 Imaging off-site will take place in a digital forensic laboratory, either in-house by the law enforcement agency or the work will be outsourced to a commercial digital forensics service provider. The ubiquity of electronic devices, and their storage capacity, coupled with the limited resources of law enforcement agencies has meant significant delays in examination. In February and March 2020, a total of 12,122 electronic devices, including computers, tablets and phones, were awaiting examination across 32 police forces in England and Wales.[157] Previous figures published in May 2019 showed that there were 12,667 devices

---

156 See *Dotcom v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745 at [203] in which the New Zealand Supreme Court observed that it was difficult to see how any other course was practically open to the police during the execution of a search warrant other than to take the suspect's computers off-site owing to passwords and encryption.

157 https://www.thetimes.co.uk/edition/news/police-struggling-to-clear-evidence-backlog-of-12-000-devices-rpmhmfnpt.

awaiting analysis across 33 forces.[158] In some cases, there can be a delay of 12 months before an electronic device is analysed.[159]

Types of data extraction

14.105 The amount and type of data extracted from an electronic device depends on the methods used. In relation to mobile phones, there are three levels of data extraction:

(1) **Logical extraction** – this copies all of the electronic data which is visible on an electronic device were an individual to browse through the device. As a consequence, a logical extraction will not normally extract data that has been deleted from the device. A variant of logical extraction is a "file system extraction", which may also recover the files on the system, including those that are hidden.

(2) **Physical extraction** – this recovers a copy of the electronic data held on the memory chip of the device. A physical extraction can sometimes download deleted data, although capabilities vary depending on the nature of the device and the operating system.

(3) **Specialist extraction** – this involves the use of expert or bespoke methods to tackle complex issues or damaged devices. This method of extraction will invariably take place in digital forensics laboratories.

14.106 There are numerous data extraction techniques. For example, one of the most technically difficult ways to extract data from mobile phones is what is known as a "chip off procedure". During a chip off procedure, a phone's memory circuit or chip is removed and attached to an external device. Following the procedure, non-volatile electronic data stored on the memory circuit or chip can be examined and retrieved without the need for a passcode.

14.107 Another point worth noting is that forensic methodology develops incrementally. For example, one recent study suggests that quantum computing will one day be able to break current encryption standards with ease.[160]

Data extraction devices

14.108 Specialist data extraction devices are developed commercially to assist in the recovery of electronic data from electronic devices. These devices are termed digital device triage systems, although colloquially known as "cyber kiosks". The devices are essentially desktop computers which can be connected to electronic devices to enable a speedy examination of electronic data.

14.109 These data extraction devices are produced for and sold to law enforcement agencies.[161] The great majority of police forces in England and Wales now use data extraction devices. The capabilities of certain data extraction devices include the extraction of remotely stored

---

158 https://www.thetimes.co.uk/article/backlog-of-devices-awaiting-police-analysis-leaves-trials-facing-collapse-bgb6zft9x.

159 HM Inspectorate of Constabulary, *Online and on the edge: Real risks in a virtual world* (2015), p 6.

160 C Gidney and M Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits" (2019), https://arxiv.org/pdf/1905.09749.pdf

161 See Privacy International, *Digital stop and search* (March 2018).

electronic data from electronic devices, with one of the products termed the "cloud analyser".[162] One of the ways in which these products work is by extracting login credentials or "tokens"[163] from a device in order to access individuals' accounts.

14.110 It is important to note that the technical capabilities of each law enforcement agency vary depending on the data extraction devices used. As law enforcement agencies contract with different commercial providers, the products will have differing technical capabilities. For example, some data extraction devices are unable to perform a targeted search of electronic devices and extract only that which is relevant, but instead must extract all the electronic data from a device.

14.111 Another reason for a variance in technical capabilities relates to what is in effect a game of cat and mouse between electronic device manufacturers and data extraction companies: each new operating system update on an electronic device may require a revision of the software on data extraction devices to defeat its security. This also means that the capabilities of data extraction tools will vary depending on the brand of electronic device and its operating system.

14.112 We discuss data extraction devices in more detail at paragraphs 18.69 to 18.95 below. At the end of Chapter 18, we recommend a wider review of the law governing the acquisition and treatment of electronic material.

PROBLEMS WITH THE CURRENT LAW

14.113 Electronic material raises novel, complex and sensitive issues in respect of the law governing not only search warrants, but the acquisition and treatment of material generally. The issues that we have identified with the law fall broadly into two categories:

(1) the lack of clear and effective legal bases to acquire electronic material; and

(2) the lack of sufficient safeguards in respect of the acquisition and treatment of electronic material.

The lack of clear and effective legal bases to acquire electronic material

14.114 In the context of search warrants, we have already explained that a large portion of legislation pre-dates the widespread use of the internet and modern computing methods. Accordingly, several powers of search and seizure are not designed with electronic material in mind, or at least the modern features of electronic material.

14.115 This means that there is ambiguity in the law as to whether particular conduct is legally permissible. Resolving these ambiguities reveals, in our view, that law enforcement agencies do not have the powers necessary to obtain digital evidence of criminality effectively. Where powers do exist, there are serious questions over whether they are subject to sufficient safeguards and regulation. We discuss the following issues in this report.

---

[162] See Privacy International, *Cloud extraction technology* (January 2020).

[163] A token is returned to a user when they authenticate successfully to an app or cloud service, thereby enabling the user to access the service without re-entering a username and password. See L Reiber, *Mobile Forensic Investigations, A Guide to Evidence Collection, Analysis, and Presentation* (2019) p 73.

(1) Early on in the project, a number of law enforcement agencies asked us to consider whether the statutory language used in search warrant provisions suffices to cover new forms of technology which may be the target of search and seizure under warrant. We discuss this at paragraphs 15.6 to 15.18 below.

(2) Several stakeholders and consultees expressed concern regarding the wording of certain statutory conditions for the issue of a search warrant, which often involve strained readings to accommodate electronic material. For example, the target material for a search warrant must often not consist of or include items which cannot themselves be the subject of a warrant, such as legally privileged material. Where a search warrant is sought to search for and seize an electronic device which likely contains protected or irrelevant electronic data, there can be confusion as to how a warrant must be framed and the appropriate avenues of seizure. We discuss this at paragraphs 15.19 to 15.34 below.

(3) A small number of search warrant regimes provide explicit powers to operate or access electronic devices. Under the vast majority of other search warrant provisions, it is unclear whether an investigator who is executing a search warrant can search electronic devices on premises and seize electronic data there and then. This ambiguity, which may arise from the wording of the statutory provision itself or the way in which a warrant is worded, rests on the distinction between the search *for* an electronic device and the search *of* such devices. If there is no lawful authority to search electronic devices, then offences of unlawful interception or computer misuse may be committed if devices are searched. We discuss these issues at paragraphs 15.160 to 15.194 below.

14.116 A particular set of issues arises by virtue of the fact that, in the course of executing a search warrant, an investigator may, inadvertently or otherwise, acquire data stored remotely, likely overseas.

(1) A preliminary question is whether the search and seizure of overseas data constitutes an extraterritorial use of enforcement powers. There are conflicting views as to whether particular conduct should be classified as “extraterritorial”. The answer has implications for the reach of the current law. We discuss this at paragraphs 16.28 to 16.60 below.

(2) Another issue is the circumstances in which it is permissible under international law to search for, seize or require the production of overseas electronic data. Current state practice indicates a lack of international consensus on when such conduct is permissible. However, failing to appreciate the international law implications when reforming powers may pose risks to international relations. We discuss this at paragraphs 16.61 to 16.100 below.

(3) It is unclear whether search warrant and other statutory provisions permit investigators to search for and seize remotely stored data. One of the statutory access conditions for the issue of a search warrant is that it is likely that the material is “on” the premises. The condition is unlikely to be satisfied where some or all of the target material is stored remotely. The single item theory will also not hold where the target material is not stored *on* the device itself. We discuss these issues at paragraphs 16.101 to 16.197 below.

(4) Virtually all electronic devices and online accounts are protected by passwords, encryption or two-factor authentication. It is unclear which powers permit the

compelling of passwords, and whether those powers which do permit the compelling of passwords are effective enough. Consequently, it is unclear whether new powers are needed to compel the production of passwords for electronic devices themselves and/or online accounts. We discuss this at paragraphs 16.198 to 16.222 below.

(5) It is unclear the extent to which, if at all, an investigator may modify electronic data in order to prevent interference. Electronic devices and the data stored locally thereon can be seized to prevent interference. However, with the right account details, remotely stored data which may constitute relevant evidence, such as an email account, could still be accessed and modified. Consultees explained that this causes problems in practice and risks the destruction of evidence. We discuss this issue at paragraphs 16.223 to 16.238 below.

14.117 There are two further issues concerning the clarity and effectiveness of the current law that have arisen during the course of this project. The first is the operation of powers of production, such as sections 19(4) and 20(1) of PACE. The second is whether law enforcement require new powers of search which are not connected to premises. However, these issues fall outside of our terms of reference and we make no formal recommendations for reform. We discuss these issues in Chapter 18 in which we call for a wider review of the law governing the acquisition and treatment of electronic material.

14.118 The effects of the problems we have identified are multifarious. In a democratic society, the coercive powers of the state should be clearly defined. Search warrants legislation does not at present explain clearly to law enforcement officers the scope of their coercive powers. This creates inconsistent practice across law enforcement:[164] while some agencies may take advantage of the full suite of digital forensic tools available to them and carry out all sorts of acts when executing a search warrant, other agencies adopt a more cautious approach.

14.119 This creates two concomitant risks. The first is that some law enforcement agencies may be performing coercive acts which constitute a serious infringement of an individual's liberty without lawful basis. Law enforcement agencies may refer vaguely to a selection of statutory provisions as authority for particular acts, which is symptomatic of a lack of clear legislative basis. This is antithetical to the rule of law and risks the unwitting or otherwise commission of civil and criminal wrongs. There is also a real risk of evidence being ruled inadmissible and serious criminal investigations collapsing. An additional set of issues relate to the wider political implications of conduct in respect of remotely stored data that may breach international law. The second risk is that those agencies who take an overly cautious approach may fail to obtain vital digital evidence for the successful prosecution of serious criminal offences.

14.120 Given the sheer number of search warrant provisions on the statute book, there are also unprincipled differences in the powers available across provisions. This means that officers of one agency may be able to carry out acts in respect of electronic material which, say, the police cannot.

---

[164] The Information Commissioner's Office recently found a lack of agreement between different police forces on how to interpret and apply the law relating to data extraction devices. See Information Commissioner's Office, *Investigation report: Mobile phone data extraction by police forces in England and Wales* (June 2020) p 52. Available at https://ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/.

14.121 There is also a cost implication to the current state of the law. In some cases, law enforcement agencies must expend large volumes of resources to sift electronic material off-site in compliance with a legal regime not fit for purpose, unable to efficiently press ahead with criminal investigations. Certain powers that would otherwise facilitate the proportionate search and seizure of electronic material and reduce the workload of investigators are not available. Agencies also spend time and money seeking legal advice in order to ascertain what conduct is legally permissible. For example, we were informed by the Investigatory Powers Commissioner's Office[165] that they receive multiple requests for advice every week from law enforcement agencies concerning accessing electronic material. Legislative ambiguity creates fertile ground for legal challenge and therefore time and money spent in court. While the courts have interpreted search warrants legislation purposively on a number of occasions to ensure that powers do not become ineffective, this has led to strained interpretations.

14.122 There are also reputational implications to the state of the current law, which cut both ways. The inability to secure vital criminal evidence, and the use of coercive powers without a clear legal basis, both risk undermining public confidence in law enforcement agencies.

14.123 Law enforcement agencies should also be able to utilise proportionately the most up to date forensic science techniques, especially where those techniques offer clear public benefits in the investigation of crime. However, without an appropriate legal framework that facilitates modern digital forensic capabilities, there is a risk that law enforcement agencies will not be as efficient, effective and digitally capable as they need to be to investigate crime.

14.124 In light of our conclusions on the current law, in our view, law enforcement agencies do not have the necessary powers to investigate crime in the current digital world and secure electronic evidence.

The lack of sufficient safeguards in respect of the acquisition and treatment of electronic material

14.125 The execution of a search warrant and seizure of material involves a serious infringement of the liberty of the subject.[166] When electronic material is concerned, unique privacy interests are engaged, a point made by the Supreme Courts in a number of jurisdictions.

14.126 In *Dotcom v Attorney-General*, the New Zealand Supreme Court stated that:

> Searches of computers (including smart phones) raise special privacy concerns, because of the nature and extent of the information that they hold, and which searchers must examine, if a search is to be effective.[167]

14.127 In *R v Vu*, Mr Justice Cromwell, giving the judgment of the Supreme Court of Canada, stated that:

---

165 "IPCO" provides independent oversight and authorisation of the use of investigatory powers by intelligence agencies, police forces and other public authorities.

166 *R (Energy Financing Team Ltd) v Bow Street Magistrates' Court* [2005] EWHC 1626 (Admin), [2006] 1 WLR 1316 at [24(1)].

167 *Dotcom v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745 at [191].

> It is difficult to imagine a more intrusive invasion of privacy than the search of a personal or home computer … when connected to the internet, computers serve as portals to an almost infinite amount of information that is shared between different users and is stored almost anywhere in the world.[168]

14.128 Mr Justice Cromwell, once again giving the judgment of the Supreme Court of Canada, in *R v Fearon*, reiterated his observations in *R v Vu*:

> Computers — and I would add cell phones — may have immense storage capacity, may generate information about intimate details of the user's interests, habits and identity without the knowledge or intent of the user, may retain information even after the user thinks that it has been destroyed, and may provide access to information that is in no meaningful sense "at" the location of the search.[169]

14.129 Chief Justice Roberts, delivering the opinion of the United States Supreme Court in *Riley v California*, wrote:

> Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse … Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person.[170]

14.130 Pulling the threads within these various judgments together, what emerges are four key ways in which the infringement caused by the search for and seizure of electronic material is made particularly acute. The first is the sheer volume of data which may be searched and seized. In one reported case in this jurisdiction, devices with a total storage capacity of 53 terabytes were seized under search warrants.[171] The storage capacity of mobile phones in particular has grown sharply, with Privacy International stating:

> You could search a person, and their entire home and never find as much information as you can from searching their phone.[172]

14.131 Big Brother Watch has compared the seizure of mobile phones to:

> Searching someone's property and taking copies of all photographs, documents, letters, films, albums, books and files.[173]

14.132 The second unique dimension to the search for and seizure of electronic material is the increasing likelihood of viewing, seizing and retaining irrelevant data, sensitive personal data and data protected from search and seizure, such as legally privileged material. The data on electronic devices is also more likely to constitute "special category data" under the Data Protection Act 2018, which covers information about an individual's ethnicity, political beliefs,

---

168 *R v Vu* 2013 SCC 60, [2013] 3 SCR 657 at [40] and [41].

169 *R v Fearon* 2014 SCC 77, [2014] SCR 621 at [51].

170 *Riley v California* (2014) 573 US 373 at 17.

171 *Business Energy Solutions Ltd v Crown Court at Preston* [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887.

172 Privacy International, *Digital stop and search* (March 2018). Available at https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf. This point was also made by the Supreme Court of the United States in *Riley v California*, 34 S. Ct. 2473, 2491 (2014).

173 Big Brother Watch, *Digital strip searches: The police's investigations of victims* (July 2019) p 19.

health or sexual orientation. Electronic devices may also be used by multiple people in a household and therefore contain sensitive data pertaining to persons not part of an investigation.

14.133 The third unique feature of the search for and seizure of electronic material is that jurisdictional boundaries may be transcended as electronic data could be stored anywhere in the world. The fourth and final unique feature is that it may not be readily apparent to someone that electronic data has been accessed and copied by law enforcement agencies given the interconnectivity of electronic devices.

14.134 It is for these reasons that there is a need for strong safeguards and clear regulation of the acquisition and treatment of electronic material. Concerns raised by stakeholders and consultees suggest that the current law governing search warrants raises issues regarding individual privacy and may constitute an infringement of article 8 of the ECHR. We have identified the following issues concerning search warrants in this project.

(1) The nature of the search and seizure of electronic material calls for consideration of whether additional criteria ought to be satisfied during the application stage. We discuss this issue at paragraphs 15.57 to 15.82 below.

(2) Questions have been raised regarding the specificity of warrants which concern electronic material. The single item theory means that only the electronic device itself needs to be specified on the face of the warrant, not the target electronic data. We discuss this issue at paragraphs 15.83 to 15.118 below.

(3) Some consultees argued that the seizure of an entire electronic device may be disproportionate in certain circumstances. The single item theory means that an entire device can be seized, even if it is likely to contain protected material and only a fraction of the electronic data is relevant. We discuss this issue at paragraphs 15.119 to 15.159 below.

(4) Issues have been raised in respect of how devices are treated post-seizure, particularly under the CJPA regime. Where investigators are authorised to seize an entire device under the authority of the warrant, several aspects of the CJPA regime do not apply. Even where the CJPA regime does apply, there are difficulties in applying the provisions in investigations which generate large volumes of electronic material. We discuss these issues in Chapter 17.

14.135 Intrusive powers such as search warrants must be subject to proper safeguards to prevent abuse and ensure that the level of intrusion is no more than is necessary. The current law creates a risk that insufficient consideration is given to the necessity and proportionality of the search for and seizure of electronic material. Accordingly, more electronic data may be seized than is necessary. The data that is seized may include vast amounts of data which is irrelevant to the investigation or falls within special categories granted heightened protection under the law. This means that individuals may be left without access to material that is integral to their social lives, academic studies or the running of their business.

14.136 In our view, insufficient attention has been paid to the unique nature of electronic material and the treatment of electronic material once it has been acquired. The current protections afforded under the law apply inconsistently depending on how material is seized. Several of the safeguards themselves are also ambiguous in how they apply to electronic material. The law is also at times a rather blunt instrument in how it prescribes the treatment of material, failing to permit flexibility in how electronic material is treated and examined.

14.137 It follows that it is difficult for individuals to understand their rights regarding the treatment of their property. In addition, the safeguards themselves do not provide individuals with adequate information about how their electronic devices or electronic data will be treated, or the right to challenge how it will be treated.

14.138 From the point of view of the state, law enforcement agencies have been left to develop their own practices regarding the treatment of electronic material, which we regard to be a highly undesirable state of affairs. Deficiencies within the current legal framework have meant that time and expense are spent litigating how material seized under warrants should be treated. The courts have had to find practical solutions within a legal framework that is not fit for purpose.

14.139 The above observations are compounded by a lack of sufficient regulation around new technology. This has meant that law enforcement agencies have been left to set their own boundaries on the use of digital forensic tools. The result is that there is a heightened risk of law enforcement agencies acting incompatibly with human rights, including data protection rights.

14.140 In the following chapters we consider these problems in detail and make recommendations for improving the current legal framework and a more wide-ranging review of the acquisition and treatment of electronic material in criminal investigations.

Chapter 15: Search for and seizure of locally stored electronic material

INTRODUCTION

15.1 In this chapter, we discuss reform to the law relating to the search for and seizure of electronic devices and electronic data stored locally on those devices. In particular, we discuss the following matters:

(1) the legislative terminology used to refer to electronic material which is the target of a search warrant;

(2) satisfying the statutory access condition for the issue of a search warrant when the target of a warrant is an electronic device;

(3) the procedure for applying for a search warrant where electronic material is the target of a search;

(4) specifying electronic material on the face of a search warrant when it is the target of a search warrant;

(5) the seizure of electronic devices when executing a search warrant; and

(6) the search of electronic devices on premises and subsequent seizure of electronic data.

15.2 Search warrant provisions typically initiate a chain reaction: the material that is capable of satisfying the statutory conditions (eg an electronic device which includes irrelevant and legally privileged material) can be the target of a search warrant, and therefore can be specified on the face of the warrant, searched for and seized. However, in this chapter, we isolate each stage and consider specifically how it should operate in respect of electronic material.

15.3 In summary, we reach the following conclusions and make the following recommendations.

(1) All forms of electronic material should be, and under certain regimes are, on their face, capable of being the target of a search warrant.

(2) Search warrant provisions should continue to permit electronic devices to be the target of a search warrant where investigators seek relevant information in electronic form. However, we recommend that search warrant provisions are amended to clarify that, when electronic data is sought, electronic devices can be the target of a search warrant so long as the data satisfies the statutory conditions relating to the target material.

(3) We recommend that the Criminal Procedure Rule Committee consider amending search warrant application forms to require an investigator, when they are seeking to obtain a warrant to search for and seize electronic devices to acquire electronic data, to explain:

(a) in as much detail as practicable what information on devices is sought; and

(b) why they believe that the information is on the device and why the information would satisfy the statutory conditions.

(4) Electronic devices should be capable of being specified on the face of the warrant as the material to be searched for on premises and seized. However, we recommend that search warrants are required to contain two parts when electronic devices are sought for the purpose of obtaining information in the form of electronic data:

(a) the first part should specify the electronic device(s) to be searched for and seized; and

(b) the second part should specify the information on the electronic device(s) that is sought.

(5) Search warrants should continue to permit the seizure or copying of entire electronic devices where it is necessary to do so and safeguards are adhered to. We recommend that search warrant provisions are amended to make clear that the power to seize an electronic device includes the power to copy all or some of the electronic data stored on an electronic device while on premises.

(6) It is unclear whether certain search warrant provisions permit an investigator to search electronic devices while on premises. We recommend that search warrant provisions should be amended to permit an investigator to apply for authority to conduct a search of electronic devices found during the course of a search where it is necessary to do so for the purpose for which the warrant is issued. If granted, the warrant should authorise the search for and copying of any electronic data stored on the device that falls within the information specified in the second part of a search warrant at paragraph (4)(b) above.

15.4 These recommendations aim to strike a fair and appropriate balance between the competing interests of the investigation of crime and the privacy rights of individuals. They would ensure that search warrants are still capable of being obtained without undue delay and executed without unreasonable constraints being placed on investigators. The recommendations would also enhance and clarify law enforcement powers when carrying out a search, ensuring that dynamic, on the spot decisions can be made and relevant evidence secured.

15.5 At the same time, these recommendations ensure that the entire search warrant process recognises the unique features of electronic data and the heightened privacy considerations it raises. They would ensure that proper scrutiny is applied when applying for a search warrant concerning electronic devices. The principles of necessity and proportionality would also be further embedded in the process, decreasing the likelihood of fishing expeditions and unnecessary collection of data. The recommendations would more generally clarify the extent of the state's powers and provide greater transparency to those who are affected by a search.

ELECTRONIC MATERIAL AS THE TARGET OF A SEARCH WARRANT

The current law

15.6 Search warrant provisions typically authorise the search for "material",[1] "articles"[2] or "documents"[3] as the target evidential material. Case law indicates that all of these terms are capable of referring to electronic devices.[4] While there have been challenges to the seizure of electronic devices on the grounds that they did not fall within the statutory language, none has been successful, as far as we are aware.[5]

The consultation paper

15.7 Stakeholders with whom we met before we published our consultation paper suggested that the interpretation of certain words to cover electronic material may involve strained readings of the language used in search warrant provisions. Further, such readings may become more strained as newer forms of technology emerge and become the target of a search warrant. This is important for two reasons: first, search warrant provisions must allow the lawful search and seizure of modern forms of electronic material which may provide evidence of criminality. Secondly, it should be clear whether any given electronic material falls within search warrant provisions and therefore may be the target of a search warrant. Ambiguity also encourages legal challenge.

15.8 In our consultation paper, we invited consultees to share examples of the types of electronic material that investigators seek under a search warrant,[6] in order to assess the adequacy of current search warrant provisions.

Consultation responses

15.9 Thirteen consultees[7] responded to this question. Consultees shared with us a wide range of examples of electronic material which may form the target of a search warrant. In relation to electronic devices, consultees identified items from the common to the less conventional. These included servers, desktop computers, laptops, tablets, phones, cameras, internet routers, hard drives, USB drives, satellite navigation and gaming consoles.

---

1 Police and Criminal Evidence Act 1984, s 8.

2 Protection of Children Act 1978, s 4.

3 Criminal Justice Act 1987, s 2(4).

4 *R (Faisaltex Ltd) v Preston Crown Court* [2008] EWHC 2832 (Admin), [2009] 1 WLR 1687 at [74]; *G v Commissioner of Police for the Metropolis* [2011] EWHC 3331 (Admin) at [5]; *Kent Pharmaceuticals Ltd v Serious Fraud Office* [2002] EWHC 3023 (QB) at [27]; and *Hargreaves v Brecknock and Radnorshire Magistrates' Court* [2015] EWHC 1803 (Admin), (2015) 179 JP 399 at [37].

5 See *R v Customs and Excise Commissioners ex parte Bottlestop* [1997] EWHC Admin 467 in which Forbes J acknowledged that there was an argument that a keyboard and mouse were not "documents", however, he made no conclusive finding on the matter and instead regarded them as "part and parcel" of the computer.

6 Consultation Question 50.

7 City of London Police Economic Crime Academy; Kent County Council Trading Standards; The Law Society; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; Bar Council and the Criminal Bar Association; Metropolitan Police Service; National Crime Agency; Competition and Markets Authority; Financial Conduct Authority; Serious Fraud Office.

15.10 Consultees also identified a number of electronic devices which form part of the 'Internet of Things'.[8] The devices identified were smart fridges, GPS enabled pet chips, smart watches (eg Apple watch), fitness trackers (eg Fitbit) and home automation devices (eg Amazon Alexa or Google Echo).

15.11 Although electronic devices themselves may have inherent evidential value in terms of proving the provenance of electronic data, often it is the electronic data stored on devices which is the target evidential material. Consultees identified a broad range of electronic data which is sought under warrant. This included backup data, logfiles, emails, mail servers, call recordings, car telematics, cryptocurrency and software systems relating to CCTV, customer relationship management or accountancy.

Analysis

The forms of electronic material that can be the target of a search warrant

15.12 As we have indicated, the courts have accorded terms such as "material" and "document" a broad meaning capable of including computers within their definition.[9] For this reason, we consider that the electronic devices listed by consultees are likely to satisfy these and similar statutory definitions (including the terms "anything";[10] "evidence";[11] and "information"[12]) where such devices are the target of a search warrant.

15.13 The broad definitions ascribed to these terms also leads us to conclude that electronic data stored locally (or remotely) will be likely to meet the statutory definitions used to refer to the target of a search warrant. Although not discussed in any consultation responses, for completeness, we consider that cryptocurrency,[13] including a digital wallet[14] or private key,[15] would satisfy the legislative terminology in search warrant provisions.

15.14 Our conclusions are subject to the caveat that each search warrant provision must be considered in the context of its statutory regime. There are also some search warrant provisions where electronic devices would clearly be precluded from being the target of a search.[16]

What forms of electronic material should be able to be the target of a search warrant?

15.15 There are several reasons justifying legislation using broad, all-encompassing terminology. Generally speaking, search warrant legislation in England and Wales does not differentiate

---

8 See paragraph 14.9 above.

9 In the case of the word "document", it may cover a computer where the statutory definition includes "information recorded in any form". See *Kent Pharmaceuticals Ltd v Serious Fraud Office* [2002] EWHC 3023 (QB) at [27].

10 Criminal Justice and Police Act 2001, s 50(1)(a).

11 Animal Welfare Act 2006, s 23(1); Anti-terrorism, Crime and Security Act 2001, s 52.

12 Banking Act 2009, s 83ZL(2)(b)(ii).

13 See paragraph 14.19 above.

14 A digital wallet is a software programme that contains a user's balance and allows the user to make transactions.

15 A private key, which is usually depicted as a series of alphanumeric characters, is used to decrypt electronic data and therefore provide access to cryptocurrency.

16 For example, Animal Welfare Act 2006, s 19(1), which permits the obtaining of a warrant for the purpose of searching for a protected animal where an inspector or constable reasonably believes that a protected animal is on the premises.

between the search of premises for physical objects and electronic material. Search warrant provisions must allow law enforcement agencies to gather both physical and electronic evidence.

15.16 There is a clear benefit in legislation containing definitions broad enough to capture emerging technology. There is an increased risk of definitions becoming out of date where specific terms are used. For example, part 2 of schedule 2 to the Criminal Justice and Police Act 2001 ("CJPA")[17] contains various consequential amendments to replace references to the words "contained in a computer" with the words "stored in any electronic form". The explanatory notes to the CJPA state that these provisions were necessary to deal with developments in technology and the advent of handheld computers and other such devices.

15.17 The use of broad definitions is also justified by considering the distinction between statutory provisions designed to cover those things which can be of evidential value and therefore the subject of a search warrant[18] and statutory provisions which govern the treatment of, or interaction with, electronic devices.[19] In the latter case, more specific terminology may be necessary. The explanatory report to the Council of Europe Convention on Cybercrime[20] also discusses the use of appropriate terminology in search and seizure laws. It recognises that traditional terms (such as "search and seizure") may require updating with more technologically orientated computer terms (such as "access and copy").[21]

15.18 Search warrant provisions should be drafted in such a way that recognises that material in any form may have evidential value and therefore be the target of a search warrant. Search warrant provisions will of course be subject to any statutory conditions which then limit the material that can be targeted, such as legally privileged material.

SATISFYING THE STATUTORY ACCESS CONDITIONS WHEN ELECTRONIC DATA IS SOUGHT

The current law

15.19 As set out in the relevant legal regime section at paragraph 14.43 above, the conceptualisation of an electronic device and the data stored thereon as a single item ("the single item theory") means that, where an investigator seeks specific electronic data, the electronic device on which it is stored may be the target of a search warrant. By way of analogy, where an investigator seeks a specific page from a book, the book itself can be the target of a search warrant.

15.20 In order to accommodate the single item theory within the pre-existing statutory framework, the courts have treated two particular statutory access conditions for the issue of certain search warrant provisions as being satisfied.

---

17 Criminal Justice and Police Act 2001, sch 2, para 13.

18 For example, Police and Criminal Evidence Act 1984, s 8(1).

19 For example, Police and Criminal Evidence Act 1984, ss 19(4) and 20(1) and Data Protection Act 2018, sch 15, para 5(1).

20 Convention on Cybercrime (Budapest, 23 November 2001) ETS No 185. Signed and ratified by the UK and entered into force on 1 September 2011. See https://www.gov.uk/government/publications/convention-on-cybercrime--2.

21 Council of Europe, *Explanatory Report to the Convention on Cybercrime*, para 137.

(1) Some search warrant provisions require reasonable grounds for believing that the target material is likely to be relevant evidence.[22] An electronic device may satisfy this requirement notwithstanding that it contains large amounts of irrelevant electronic data.[23]

(2) Some search warrant provisions require reasonable grounds for believing that the target material does not consist of or include certain categories of material, such as legally privileged material.[24] An electronic device may satisfy this requirement notwithstanding that it is likely to contain such protected electronic data provided the wording of the warrant excludes the protected electronic data.[25] Therefore, if there may be protected material on an electronic device, this must be excluded (expressly or impliedly) on the face of the warrant.[26] If the sifting of protected material cannot reasonably be conducted on the premises, seizure of an electronic device should take place under the CJPA regime as the device contains material which the investigator is not entitled to seize.[27]

15.21 Accordingly, an electronic device with large volumes of irrelevant and protected data can, as a matter of law, satisfy the statutory conditions and therefore be the target of a search warrant so long as there is relevant data stored on the device.

The consultation paper

15.22 In our consultation paper, we suggested that there may be a need to resolve the interpretative challenges within statutory provisions where electronic devices are the target of a search warrant, particularly where they contain protected material.[28] This is because the reading of this statutory access condition seems particularly strained to accommodate the single item theory. We therefore invited consultees' views on whether the legislative framework for applying for search warrants in relation to electronic devices ought to be clarified in order to ensure that search warrants for electronic devices can be granted when electronic data is sought.[29]

Consultation responses

15.23 In response to our consultation, twelve consultees agreed that the legislative framework for applying for search warrants in relation to electronic devices ought to be clarified;[30] and one consultee considered that their legislative framework did not need clarification.[31]

---

22 Police and Criminal Evidence Act 1984, s 8(1)(c).

23 *R* (*Cabot Global Ltd) v Barkingside Magistrates' Court* [2015] EWHC 1458 (Admin), [2015] 2 Cr App R 26 at [38].

24 Police and Criminal Evidence Act 1984, s 8(1)(d).

25 *R (A) v Central Criminal Court and another* [2017] EWHC 70 (Admin) at [81], [2017] 1 WLR 3567 at [43].

26 *R (A) v Central Criminal Court and another* [2017] EWHC 70 (Admin) at [84], [2017] 1 WLR 3567 at [46].

27 *R (A) v Central Criminal Court and another* [2017] EWHC 70 (Admin) at [100], [2017] 1 WLR 3567 at [61].

28 Law Commission, *Search Warrants: Consultation Paper* (2018) CP No 235 para 10.169.

29 Consultation Question 56(1).

30 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Birmingham Law Society; Southern Derbyshire Magistrates' Bench; Northumbria Law School Centre for Evidence and Criminal Justice Studies; Independent Office for Police Conduct; The Law Society; Magistrates Association; Dijen Basu QC; Competition and Markets Authority.

15.24 The Law Society noted that it would be beneficial to both the individual subject to a warrant and investigators to have clarity on the powers available and the extent of them.

15.25 Dijen Basu QC stated that a search warrant should not require an artificial statement on its face that it does not authorise seizure of items subject to legal privilege in order for the warrant to be lawful. He noted that many people's devices will contain legally privileged material as well as excluded material. In his view, the CJPA provisions should expressly cover the seizure of devices.

15.26 The Serious Fraud Office ("SFO") were not convinced that there was any need to change the legislative framework to clarify that computers and devices can be seized under warrant in respect of the CJA. They pointed out that this approach has been available for over 15 years following a long line of consistent case law.[32]

Analysis

15.27 In our view, it is a foundational principle of search warrant regimes that electronic devices should be capable of being the target of a search warrant when electronic data is sought. Where electronic data is sought, the search of premises for a device will always be a necessary prerequisite. Accordingly, it is necessary to highlight and prevent the blurring of the distinction between the search of premises *for* a device and the subsequent search *of* a device for electronic data, a distinction that should be clearer under current search warrant regimes. Maintaining this two-stage distinction by permitting the search for a device reflects the true nature of a premises search warrant and permits the procedural stages to be clearly identified and for appropriate safeguards to attach to each stage. Conceptualising the process as the search of premises for electronic data ignores a vital step and risks failing to appreciate the nature of electronic devices.

15.28 Where electronic material is sought, an electronic device should still be capable of being the target of a warrant and searched for notwithstanding that it contains irrelevant and protected material. The presence of irrelevant and protected material does, however, require robust safeguards to ensure that no more data than necessary is seized. Further, any irrelevant or protected electronic data that is seized must be returned and/or deleted as soon as practicable. These are all matters to which we return in this chapter and the following two.

15.29 We consider that the statutory conditions for the grant of a search warrant should make clear that, when electronic data is sought, electronic devices are capable of being the target of a search and when they are so. The precise circumstances in which an electronic device will be capable of being the target of a search warrant will vary depending on the statutory conditions of the regime concerned. However, as a basic proposition, an electronic device should be capable of being the target of a search warrant where the electronic data sought satisfies the statutory conditions relating to the target material.

15.30 This proposition can be demonstrated by considering the following example in respect of section 8 of the Police and Criminal Evidence Act 1984 ("PACE").

---

31 Serious Fraud Office.

32 *Kent Pharmaceuticals Ltd v Serious Fraud Office* [2002] EWHC 3023 (Admin).

15.31 The police are investigating Lyndon in relation to a possible offence of bribery under section 1(2) of the Bribery Act 2010. It is believed that Lyndon bribed Sebastian in return for a lucrative business contract. The offence requires the prosecution to prove that Lyndon offered, promised or gave a financial or other advantage to Sebastian and intended the advantage to induce or reward Sebastian for improper performance of a relevant function or activity. Intelligence suggests that communications between Lyndon and Sebastian are stored on Lyndon's work laptop. The police seek those communications by obtaining a search warrant to enter and search Lyndon's premises.

15.32 In the above example, Lyndon's work laptop would be capable of being the target of a search warrant if there are reasonable grounds for believing that, in addition to the other statutory conditions, the communications (ie the information sought):

(1) are on an electronic device on premises (section 8(1)(b));

(2) are likely to be of substantial value (section 8(1)(b));

(3) are likely to be relevant evidence (section 8(1)(c)); and

(4) do not consist of or include protected material (section 8(1)(d)).

15.33 We acknowledge the point made by the SFO that electronic devices can already be the target of a search warrant where electronic material is sought under particular regimes. However, in line with the Law Society's observation, amending the statutory conditions would bring clarity to the operation of search warrant regimes for both investigators and those who may be subject to a warrant. This would also require investigators to apply their mind specifically to the presence of electronic data when applying for a search warrant and whether it meets the statutory criteria.

Recommendation 45

15.34 We recommend that search warrant provisions be amended to clarify that, when electronic data is sought, electronic devices can be the target of a search warrant so long as the data satisfies the statutory conditions relating to the target material.

APPLYING FOR A WARRANT TO SEARCH FOR AND SEIZE ELECTRONIC DEVICES

The current law

15.35 At present, when an investigator applies for a search warrant to search for and seize electronic devices, there are no additional procedural steps that must be met beyond those which would be required for other material. Case law indicates, however, that a description of the contents of an electronic device sought should be included in the application form.[33]

[33] *R (A) v Central Criminal Court and another* [2017] EWHC 70 (Admin) at [85], [2017] 1 WLR 3567 at [47].

The consultation paper

15.36 In the consultation paper we considered that the large volume of information that can be obtained from electronic devices justified reconsideration of the procedure when applying for a search warrant to search for and seize electronic devices.[34]

15.37 We provisionally proposed[35] that additional steps should be introduced to require investigators and issuing authorities to consider the necessity and proportionality of the search for and seizure of electronic devices.

15.38 Additionally, we invited[36] consultees' views on whether:

(1) additional criteria ought to be satisfied during the application stage and, if so, what; and

(2) investigators should have to present search protocols or schedules in warrant applications to the issuing authority which would describe the ways in which electronic devices are to be analysed once seized.

Consultation responses

Introducing additional steps to consider the necessity and proportionality of device seizures

15.39 On the question of whether additional steps should be introduced to require investigators and issuing authorities to consider the necessity and proportionality of the seizure of electronic devices: 11 consultees agreed that additional steps should be required;[37] five disagreed;[38] and two expressed other views.[39]

15.40 Several consultees observed that the duty to consider the necessity and proportionality of searching for and seizing devices is already imposed by section 6 of the Human Rights Act 1998, which makes it unlawful for a public authority to act in a way which is incompatible with the European Convention on Human Rights ("ECHR").[40] Professor Richard Stone, however, argued that there would be benefit in making the tests of necessity and proportionality explicit in the application process.

15.41 Other consultees disagreed. Some argued that there are already a number of safeguards attached to warrant applications.[41] In particular, the process of issuing and executing search

---

34 Search Warrants (2018) Law Commission Consultation Paper No 235 para 10.168.

35 Consultation Question 56.

36 Consultation Question 56.

37 Professor Richard Stone; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Birmingham Law Society; Southern Derbyshire Magistrates' Bench; Northumbria Law School Centre for Evidence and Criminal Justice Studies; Independent Office for Police Conduct; The Law Society; Justices' Clerks' Society; Magistrates Association; Privacy International.

38 Crown Prosecution Service; Metropolitan Police Service; Competition and Markets Authority; Financial Conduct Authority; Serious Fraud Office.

39 Kent County Council Trading Standards; Bar Council and the Criminal Bar Association.

40 Professor Richard Stone; Northumbria Law School Centre for Evidence and Criminal Justice Studies; Serious Fraud Office.

41 Crown Prosecution Service.

warrants already includes implicit assessment of the necessity and proportionality of interference with privacy rights under article 8 of the ECHR.[42] It was also said that the statutory access conditions already incorporate necessity and proportionality: the warrant must concern an indictable offence and the material sought must be of substantial value to the investigation.[43]

15.42 Consultees also made constructive arguments against adding what they regarded as unnecessary steps to the application process. They pointed out that the warrant application process should be simple and speedy, which additional steps might jeopardise.[44] Finally, it was brought to our attention that law enforcement agencies often already have internal discussions regarding their approach to searching for and seizing electronic material on premises and therefore consider the necessity and proportionality of device seizures.[45]

15.43 The Bar Council and the Criminal Bar Association ("CBA") also made the point that it may be difficult to anticipate the presence of protected material or the proportionality of seizing a device ahead of search and seizure.

Introducing additional criteria during the application procedure

15.44 On the question of whether additional criteria ought to be satisfied during the application stage when applying for a warrant to search for and seize electronic material: seven consultees agreed that additional criteria ought to be satisfied;[46] and six disagreed.[47]

15.45 The Birmingham Law Society argued that issuing authorities should be obliged to consider the impact of the seizure of electronic storage devices upon a suspect in the same way that they are currently obliged to consider the impact of a search warrant.

15.46 Privacy International were concerned with the paucity of information regarding how individuals' devices are examined. They suggested that search warrant application forms should require particular questions to be answered, and set out a detailed and thoughtful possible list. The questions which Privacy International suggested should be addressed were as follows:

(1) Who is the suspect?

(2) What is the target device?

(3) What information is contained on the target device?

(4) What is the relevant information contained on the target device?

---

42 Serious Fraud Office.

43 Crown Prosecution Service.

44 Crown Prosecution Service.

45 Serious Fraud Office; Kent County Council Trading Standards.

46 Professor Richard Stone; Council of Her Majesty's Circuit Judges; Birmingham Law Society; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; Magistrates Association; Privacy International.

47 HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; The Law Society; Metropolitan Police Service; Financial Conduct Authority; Serious Fraud Office.

(5) How will the information accessed and collected be confined to what is relevant and how will access to and collection of irrelevant data be minimised?

(6) What is the method, extent and duration of the proposed equipment interference measure?

(a) Is the measure remote or physical?

(b) Does the measure exploit a known or unknown vulnerability?

(c) Does the measure use a social engineering technique?

(d) What kind of surveillance will the measure facilitate? (e.g. Does it involve extracting data from a mobile device, remotely turning on a camera or microphone, or logging keystrokes?)

(7) Have all less intrusive methods been exhausted or would they be futile, such that equipment interference is the least intrusive option?

(8) What are the potential risks and damage to the security of the target device and devices generally, as well as of data on the target device and devices generally?

(a) If a vulnerability is exploited, is that vulnerability in widely used systems? In core internet infrastructure? Critical infrastructure? National security systems?

(b) If a vulnerability is exploited, is it likely to spread to non-target systems? Is the vulnerability easy for unsophisticated actors to exploit?

(9) How will potential risks and damage to the device and devices generally be mitigated or corrected?

(10) Will companies whose products or services may be affected be notified?

15.47 The Metropolitan Police Service were not clear what additional criteria should be satisfied. The SFO warned against introducing unnecessary delay into the process, referring to the Supreme Court's observations in *Haralambous* that search warrants should be capable of being obtained speedily.[48]

Requiring search protocols

15.48 On the question of whether investigators should have to present search protocols to the issuing authority in relation to electronic devices to be seized: 12 consultees agreed that they should;[49] and seven disagreed.[50]

---

48 *R (Haralambous) v Crown Court at St Albans* [2018] UKSC 1, [2018] AC 236 at [15].

49 Professor Richard Stone; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Birmingham Law Society; Southern Derbyshire Magistrates' Bench; Northumbria Law School Centre for Evidence and Criminal Justice Studies; Independent Office for Police Conduct; The Law Society; Magistrates Association; Dijen Basu QC; Bar Council and the Criminal Bar Association; Privacy International.

50 HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Metropolitan Police Service; Competition and Markets Authority; Financial Conduct Authority; Serious Fraud Office; HM Revenue and Customs.

15.49 Some consultees explained what they thought search protocols might actually involve in practice. It was suggested that search protocols should set out what information, or type of information, is sought.[51] They should include information on the application form setting out how electronic storage devices or data are to be removed, stored and analysed after seizure.[52]

15.50 It was suggested that a standard protocol could be designed, with a requirement for investigators to take forensic copies of electronic devices if facilities are offered by the occupier and if decryption codes are given as part of that process.[53] Other consultees saw merit in investigators being required to formulate protocols or comply with a new Code of Practice as the price of seizing certain electronic storage devices.[54]

15.51 It was also argued that requiring specific information about the material, type of material or devices to be searched for may prevent speculative searches and "fishing expeditions".[55] The Law Society suggested that search protocols would also assist the investigator and issuing authority in considering the necessity and proportionality of granting a warrant.

15.52 The Bar Council and the CBA noted that academic literature in the United States is divided as to the value and practicality of judges sanctioning and overseeing search protocols. They suggested that further work may be required taking account, for example, of the role played by judges in England and Wales in scrutinizing draft Anton Piller orders.[56]

15.53 The Bar Council and the CBA did suggest, however, that one approach would be for a warrant to contain two parts: one part specifying the device that may be seized; the other part specifying the way in which the information contained on the device should be treated (on the assumption that the whole device will be seized). Under this suggestion, investigators would be encouraged to set out transparently on the face of the warrant how they intend to deal with the data.

15.54 A number of consultees disagreed with the requirement to devise search protocols during the application stage. The main argument advanced was that a search protocol would not be tenable as the types and number of devices which fall in scope of a warrant are unlikely to be known until a warrant is executed.[57] Further, when making the application the law enforcement officer is unlikely to know if devices will be accessible or if owners will cooperate.[58] It was said that it is not until an investigator is on the premises and faced with

---

51 Southern Derbyshire Magistrates' Bench; Northumbria Law School Centre for Evidence and Criminal Justice Studies.

52 Southern Derbyshire Magistrates' Bench; Senior District Judge (Chief Magistrate).

53 Dijen Basu QC.

54 Bar Council and the Criminal Bar Association; HM Council of District Judges (Magistrates' Court).

55 Northumbria Law School Centre for Evidence and Criminal Justice Studies.

56 In the civil law context, a claimant may apply to the High Court for a search order, previously known as an Anton Piller order, which is an interim mandatory injunction. The power of the High Court to grant a search order has been placed on statutory footing by the Civil Procedure Act 1997, s 7 and is governed by the Civil Procedure Rules, Part 25 and Practice Direction 25A. See D Bean, I Parry and A Burns, *Injunctions* (13th ed 2018).

57 Serious Fraud Office.

58 Serious Fraud Office.

the myriad of digital devices that a proportionate search and seizure strategy can be determined.[59] For these reasons, detailed and meaningful protocols could not be drafted.

15.55 A number of other points were raised. One consultee considered that it was unclear how a search protocol will assist the task of the issuing authority.[60] Once again it was emphasised that the search warrant application process should be simple and speedy.[61]

15.56 However, the Crown Prosecution Service ("CPS") acknowledged the potential merit of search protocols at a later stage to provide judicial oversight by ensuring that material is dealt with appropriately and that material is retained only where necessary and proportionate.[62]

Analysis

Introducing additional steps or criteria during the application procedure

15.57 As consultees pointed out, considerations of necessity and proportionality are already built into the statutory access conditions and the application process. Issuing authorities should be cognisant of the significant privacy intrusion that is authorised when issuing a search warrant to search for and seize entire electronic devices. In particular, an issuing authority should consider the full range of distinctive privacy concerns raised by the search and seizure of electronic devices. In granting such authorisation, the function of the issuing authority in providing independent scrutiny is now, more than ever, "a duty of high constitutional importance".[63] Accordingly, the unique privacy interests engaged by the search for and seizure of electronic devices should be specifically addressed in training given to the law enforcement agencies who apply for search warrants and the judicial officeholders who must scrutinise them.

15.58 Quite apart from training, we consider that more explicit questions could be directed for an investigator to answer, and the issuing authority to consider within application forms. This would aid in discharging the duty of full and frank disclosure, scrutinising applications and ensuring that warrants to search for and seize electronic devices are only issued where necessary and proportionate.

15.59 In reaching this conclusion, we recognise that a balance must be struck. Search warrants must be capable of being obtained and executed quickly at an early stage of criminal investigations.[64] For this reason, we do not agree wholesale with the approach suggested by Privacy International that an extensive list of detailed questions should be answered. The questions also seem to involve transplanting the requirements for a targeted equipment interference warrant. We can foresee some questions either not being relevant or the answers not being known. We also agree with the Bar Council and the CBA that it is difficult to anticipate the content of electronic devices ahead of search and seizure. It follows that it will be difficult, if not impossible, for an investigator to detail *all* information, including that which is irrelevant, that will be contained on a target device.

---

59 HM Revenue and Customs.

60 Metropolitan Police Service.

61 Crown Prosecution Service.

62 Crown Prosecution Service.

63 *Attorney General of Jamaica v Williams* [1998] AC 351 at 358 by Lord Hoffman.

64 *R (Haralambous) v Crown Court at St Albans* [2018] UKSC 1, [2018] AC 236 at [15].

15.60 Taking into account the above considerations, there are two ways in which we see value in amending application forms to encourage consideration of the necessity and proportionality of the search for and seizure of electronic devices.

Detailing the information sought on electronic devices

15.61 Case law indicates that a description of the contents of an electronic device sought should be included in the application form.[65] In our view, search warrant application forms should be amended to prompt an applicant to more clearly explain the information sought on devices. This would have several advantages. First, it would make explicit an important observation in case law and would therefore increase the likelihood of adherence to it. Secondly, it would ensure that investigators and issuing authorities consider the precise information sought and whether a warrant to search for and seize electronic devices is appropriate. Thirdly, as we will discuss in the next section, we see a statement of the information sought taking on a significant role as a reference point for the subsequent search of devices, on-site or off-site.

Recommendation 46

15.62 We recommend that the Criminal Procedure Rule Committee consider amending search warrant application forms to require an investigator, when they are seeking to obtain a warrant to search for and seize electronic devices to acquire electronic data, to explain in as much detail as practicable what information on devices is sought.

Detailing how information satisfies the statutory conditions

15.63 At Recommendation 45 above, we recommend that search warrant provisions are amended to clarify that, when electronic data is sought, electronic devices can be the target of a search warrant so long as the data satisfies the statutory conditions relating to the target material. A corollary of amending the statutory conditions for the issue of a search warrant is that consequential amendments would have to be made to the application forms.

15.64 Amendments to the application forms, which would reflect the statutory conditions for the issue of a search warrant, would assist both investigators and issuing authorities when considering the necessity and proportionality of searching for and seizing electronic devices. This is because attention would be focused on both the likelihood that information will be on electronic devices and whether such information would meet the statutory criteria. In cases where a plethora of electronic devices are specified as the target material (for example, desktops, laptops, servers, mobile phones and removable media), this has the advantage of requiring scrutiny to be applied to each and every device and discouraging a dragnet approach.

15.65 To take once again our example in respect of section 8 of PACE and the scenario described at paragraph 15.31 above. If the police were applying for a search warrant to search Lyndon's premises for his work laptop to acquire communications between him and Sebastian, they would have to explain why they believe that the communications between Lyndon and Sebastian:

(1) are on Lyndon's work laptop on his premises;

---

65 *R (A) v Central Criminal Court and another* [2017] EWHC 70 (Admin) at [85], [2017] 1 WLR 3567 at [47].

(2) are likely to be of substantial value to the investigation;

(3) are likely to be relevant evidence; and

(4) do not consist of or include protected material.

Recommendation 47

15.66 We recommend that the Criminal Procedure Rule Committee consider amending search warrant application forms to require an investigator, when they are seeking to obtain a warrant to search for and seize electronic devices to acquire electronic data, to explain why they believe that the information is on the device and why the information would satisfy the statutory conditions.

Requiring pre-search protocols

Defining pre-search protocols

15.67 Pre-search protocols could take a number of forms. We have described such protocols, broadly speaking, as involving the investigator presenting information on how electronic material will be searched for, seized and examined. This could conceivably either be approved or modified by the issuing authority.

15.68 Pre-search protocols could, however, take a different form. Instead, the issuing authority could initiate pre-search protocols by imposing conditions on how the search, seizure and subsequent treatment of electronic material is conducted. For example, the issuing authority could set conditions on the face of the warrant regarding what devices can be seized, the deadline by which devices should be returned to the owner and how any extracted electronic data should be searched.

15.69 The practice of pre-search protocols features in other jurisdictions. Rule 41(e)(2)(B) of the United States' Federal Rules of Criminal Procedure permits the seizure of electronic devices for later off-site examination. However, the rule is silent as to how the procedure is to be conducted. In what was termed a "magistrates' revolt",[66] certain magistrates began requiring "*ex ante* search protocols" setting out how the investigator would carry out the search to ensure its proportionality.

15.70 In New Zealand, the issuing authority is empowered to set conditions under section 103(3)(b) of the Search and Surveillance Act 2012. The section does not limit the types of conditions that can be set, however, it does provide two examples: (1) restricting the time of the execution of the warrant; and (2) a condition that reasonable assistance be provided by an occupier to a person executing a search warrant. If conditions are imposed they must be specified in the warrant.

15.71 The New Zealand Law Commission and Ministry of Justice, in their joint review of their Search and Surveillance Act 2012, recommended that section 103(3)(b) be amended to include a third example of the types of conditions that could be specified in a search warrant: "any condition to minimise the level of intrusion on the privacy of any person likely to be

---

[66] Reid Day, "Let the Magistrates Revolt: A Review of Search Warrant Applications for Electronic Information Possessed by Online Services" (2015) 64 University of Kansas Law Review 491 at 510 to 511.

affected during a search, including a search of a computer system or other data storage device".[67]

Evaluating the efficacy of pre-search protocols

15.72 As the Bar Council and the CBA observe, the academic literature in the United States as to the value and practicality of pre-search protocols is divided. On the one hand, it has been argued that pre-search protocols enable the issuing authority to fulfil their constitutional duty to protect privacy from government overreach.[68] It also has been argued that pre-search protocols should be welcomed as a minimisation procedure: a legitimate judicial role.[69]

15.73 On the other hand, it has been argued that (1) pre-search protocols result in excessive limitations on investigators; (2) the means by which electronic material will be examined is unknowable prior to the execution of a warrant; and (3) magistrates lack the expertise to craft or oversee such protocols.[70] The New Zealand Law Commission and Ministry of Justice joint review, while recommending that their search warrants legislation should emphasise the option of imposing conditions on digital searches, wrote:

> We are not convinced that a requirement to impose conditions would be useful in every case. It seems to us that a certain degree of flexibility is needed when searching electronic devices, given that the searcher is unlikely to know in advance exactly where and in what format the targeted material is stored. There is a risk that investigations would be hindered through the routine imposition of unworkable or unduly prescriptive conditions.[71]

15.74 We have reviewed the arguments on both sides, both those from consultation responses and those from wider literature. In our view, the requirement for an investigator to provide, or for an issuing authority to impose, pre-search protocols or conditions would not be desirable. This is because we consider that the likely benefits to privacy rights of individuals would in most cases be minimal, especially in light of recommendations we make later in the Report, and in any event outweighed by the likely detriment to law enforcement agencies and the investigation, detection and prevention of crime.

15.75 A requirement for an investigator to provide pre-search protocols, or a power for issuing authorities to impose conditions, would place an additional burden on investigators and issuing authorities when seeking to obtain a search warrant, often in times of urgency. There are likely to be a number of unknown variables when executing a search warrant, including the exact number and type of electronic devices that will be on premises, their state of accessibility and how cooperative any occupier will be willing to be. This means that the level of detail that any search protocol could provide would be reduced. Pre-search protocols also risk placing unduly prescriptive conditions on investigators when carrying out a search, thereby potentially unnecessarily constraining law enforcement agencies in the collection of

---

67 New Zealand Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* / *Ko te Arotake i te Search and Surveillance Act 2012*, NZLC R141 (2017) p 202.

68 Paul Ohm, "Massive Hard Drives, General Warrants, and the Power of Magistrate Judges" (2011) 97 Virginia Law Review 1 at 11–12.

69 Emily Berman, "Digital Searches, the Fourth Amendment, and the Magistrates' Revolt" (2018) 68 Emory Law Journal 49 at 55 to 56.

70 Orin Kerr, "Ex Ante Regulation of Computer Search and Seizure" (2010) 96 Virginia Law Review 1241 at 1246.

71 New Zealand Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* / *Ko te Arotake i te Search and Surveillance Act 2012*, NZLC R141 (2017) para 12.64.

relevant evidence. This would be especially so if a standard pre-search protocol was designed that was not tailored to the actual investigation.

15.76 In reaching this conclusion, we have also considered the case of *Fitzgerald* in which search protocols were devised prior to the search.[72] In that case, pre-prepared search protocols caused difficulty for the police when the lawfulness of the warrant was challenged in terms of what should have been included in the application form rather than a separate protocol.[73] This case also indicates that preparing search protocols prior to a search may cause confusion in respect of the appropriateness of certain powers of seizure.

15.77 Crucially, we also consider that pre-search protocols are rendered unnecessary, or at the very least their benefits diminished, by other safeguards that we recommend in order to embed the principles of necessity and proportionality into the search warrants process. To this end, it should be borne in mind that the practice of pre-search protocols in the United States developed to address the lack of prescriptive rules governing the treatment of electronic devices seized or copied on-site. There is no equivalent to the detailed regime concerning the treatment of seized material under part 2 of the CJPA. Although pre-empting recommendations made later in this report, the following recommendations would also, in our view, render pre-search protocols unnecessary.

15.78 First, we recommend a new Code of Practice to regulate search warrant investigations concerning electronic material. The Code would include a set of standards and overarching principles to regulate the search, seizure and subsequent treatment and examination of electronic material. The Code would be flexible enough to apply to a range of scenarios that an investigator may face. The Code could also be updated to take into account developments in technology and digital forensics. Together, these matters would ensure that privacy rights remain adequately protected during the search and seizure of electronic material and the level of intrusion kept to a minimum. We also note that two consultees considered a Code of Practice to be a suitable alternative to search protocols.

15.79 Secondly, we recommend a statutory right for persons to request information on how their electronic devices or data were examined on-site, or will be examined off-site by means of *post*-search protocols. A record of an investigator's on-site search procedure would ensure accountability and enable an individual to know the extent to which their privacy had been interfered with. Post-search protocols concerning off-site examination would serve a similar function and would also have the advantage of being more specific than pre-search protocols as the variables listed at paragraph 15.75 above will be known.

15.80 Thirdly, we recommend a route for investigators to obtain judicial approval of, or for occupiers to challenge, the proposed method of treatment of electronic devices set out in the post-search protocols. Judicial scrutiny would therefore cover the entire search warrants process.

15.81 Finally, we note consultees' suggestions that pre-search protocols should set out the information, or type of information sought, which may prevent speculative searches or "fishing expeditions". Our recommendations concerning the information to be provided when applying for a search warrant should assist in preventing such fishing expeditions. We also

---

72 *Fitzgerald v Preston Crown Court* [2018] EWHC 804 (Admin) at [34].

73 *Fitzgerald v Preston Crown Court* [2018] EWHC 804 (Admin) at [74] and [84].

discuss the level of detail that search warrants should contain regarding the information on devices sought in the next section.

15.82 For these reasons, we do not recommend the introduction of pre-search protocols.

DRAFTING WARRANTS TO SEARCH FOR AND SEIZE ELECTRONIC DEVICES

The current law

15.83 The conceptualisation of an electronic device as a single item means that the device can be specified on the face of a search warrant rather than the information which will exist as electronic data on the device.[74] To return to our example above:

15.84 The police seek communications between Lyndon and Sebastian, which are stored on Lyndon's work laptop. Lyndon's work laptop is capable of being the target of a search warrant. Accordingly, the police may specify on the face of the warrant that the police are authorised to enter Lyndon's premises to search for his work laptop.

15.85 We have cited actual examples of warrants drafted in this way at paragraph 14.41 above. Therefore, there is no requirement for search warrants to specify the underlying information that an investigator seeks which exists as electronic data on the device to be searched for. As we explain at paragraphs 14.47 and 14.49 above, search warrants can, and sometimes do, specify the information which exists as electronic data instead of, or in addition to, electronic devices. This will be necessary where an investigator wishes also to search for the information in hard copy and electronic form.

15.86 Specifying electronic devices, rather than the underlying information sought, on the face of a warrant has been held to satisfy the requirement under section 15(6)(b) of PACE that the warrant identify, so far as is practicable, the articles sought.[75] Further, seizure need not be made under the CJPA as the electronic device is not mixed with, or contained in, something which the investigator is not entitled to seize.

15.87 The only exception to the proposition that a search warrant need only specify electronic devices is where there are reasonable grounds for believing that legally privileged material may be found on the device. In such cases, the wording of the warrant should clearly exclude legally privileged material from that which can be searched for and seized.[76] However, while an express exclusion is to be preferred, an implied exclusion of legally privileged material may suffice.[77]

---

74 *R (A) v Central Criminal Court and another* [2017] EWHC 70 (Admin) at [74], [2017] 1 WLR 3567 at [36].

75 *R (A) v Central Criminal Court and another* [2017] EWHC 70 (Admin) at [78], [2017] 1 WLR 3567 at [40].

76 *R (A) v Central Criminal Court and another* [2017] EWHC 70 (Admin) at [81], [2017] 1 WLR 3567 at [43].

77 *R (A) v Central Criminal Court and another* [2017] EWHC 70 (Admin) at [84], [2017] 1 WLR 3567 at [46].

The consultation paper

15.88 In the consultation paper, we identified a number of advantages and disadvantages to specifying electronic devices rather than information sought on the warrant.[78] The advantages were summarised by Gross LJ in the *R (A)* case:

> For my part, while it is difficult to generalise, there are significant advantages to the warrants—if suitably drafted, as discussed above—identifying the computers or phones sought under section 9 and schedule 1, rather than a necessarily much lengthier list of the contents or classes of contents. … Given its constitutional and practical importance, it is imperative that a warrant is capable of simple and practical execution (the *Energy Financing* case) and is clear on its face. Having regard to the realities of a search, seeking specified items, things or articles rather than a list of electronic contents is potentially much quicker, more practical and less intrusive. It is also much less prone to misunderstandings on the day. The better place for the explanation and description of the contents or classes of contents sought is the application for the warrant before the judge, where the applicant is in any event under a duty to give appropriate disclosure.[79]

15.89 In the consultation paper we also raised some concerns with this approach, which may work to the disadvantage of the occupier or owner of the premises being searched. First, we wrote that search warrants which specify the information sought provide greater detail to the occupier of what material is of relevance.

15.90 Secondly, we observed that the regime in part 2 of the CJPA will more clearly apply if the warrant is drafted in terms of information because the target information will inevitably be mixed with other irrelevant data on the device.[80] This would mean that seizure would have to take place under section 50 of the CJPA. Certain safeguards under part 2 of the CJPA will not apply if an electronic device is seized by means other than sections 50 or 51 of the CJPA. In particular, an individual will be deprived of the safeguards which apply under section 53 of the CJPA relating to the subsequent off-site sifting of electronic data.

15.91 For these reasons, we invited views on the operation of the search warrants regime where warrants are drafted in terms of "devices" to be searched for rather than specifying electronic information to be searched for on the devices.[81] We invited views in particular on whether protected material is adequately protected and whether the single item theory works effectively and fairly in practice.[82]

---

78 Law Commission, *Search Warrants: Consultation Paper* (2018) CP No 235 paras 10.18 to 10.77.

79 *R (A) v Central Criminal Court and another* [2017] EWHC 70 (Admin) at [85], [2017] 1 WLR 3567 at [47].

80 Law Commission, *Search Warrants: Consultation Paper* (2018) CP No 235 para 10.57.

81 Consultation Question 51.

82 Consultation Questions 51(1), (2).

Consultation responses

15.92 Nineteen consultees[83] answered these questions. 12 consultees considered that the single item theory works effectively and fairly in practice.[84] 11 consultees raised issues with the single item theory.[85]

15.93 We also invited views on the operation of the regime where warrants are drafted in terms of "information" rather than specifying devices.[86] We asked in particular for experiences where searches under warrant for information stored in electronic form have created difficulties.

15.94 Consultees made clear that "device warrants" are the most common form of warrants.[87] As we explained at paragraphs 14.41 and 14.47 above, the Magistrates Association survey of members revealed that 81% of warrants were drafted in terms of devices and 19% specified the information sought on devices.

Advantages of specifying electronic devices on the face of the warrant

15.95 Many consultees considered that the single item theory works effectively and fairly in practice.[88] A theme which emerged in support of specifying electronic device was the distinction we discussed at paragraph 15.27 above between the search of premises *for* a device and the subsequent search *of* a device for relevant electronic data. It was emphasised that the search of premises for electronic devices requires decisions to be made dynamically on the spot and is well-served by the specification of entire devices.

15.96 A number of consultees noted that an investigator making an application for a search warrant may have insufficient knowledge to specify with any precision the form the information sought may take.[89] There may be reasonable grounds to believe that an electronic device will contain relevant evidence of an offence as it has been used by a suspect. It does not follow that the investigator will be able to anticipate and identify with precision when drafting a warrant each form which the evidence might conceivably take.

---

83 City of London Police Economic Crime Academy; HM Council of District Judges (Magistrates' Court); Crown Prosecution Service; Senior District Judge (Chief Magistrate); Birmingham Law Society; Southern Derbyshire Magistrates' Bench; Northumbria Law School Centre for Evidence and Criminal Justice Studies; The Law Society; Justices' Clerks' Society; Dijen Basu QC; Bar Council and the Criminal Bar Association; National Crime Agency; Competition and Markets Authority; Privacy International; Financial Conduct Authority; Serious Fraud Office; Kent County Council Trading Standards; Magistrates Association; Metropolitan Police Service.

84 HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Bar Council and the Criminal Bar Association; Crown Prosecution Service; Justices' Clerks' Society; Metropolitan Police Service; National Crime Agency; Serious Fraud Office; Financial Conduct Authority; Insolvency Service; Competition and Markets Authority; Dijen Basu QC.

85 City of London Police Economic Crime Academy; Dijen Basu QC; Kent County Council Trading Standards; Privacy International; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Magistrates Association; Birmingham Law Society; Southern Derbyshire Magistrates' Bench; Northumbria Law School Centre for Evidence and Criminal Justice Studies; Law Society.

86 Consultation Question 52.

87 Senior District Judge (Chief Magistrate); Magistrates Association.

88 HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Bar Council and the Criminal Bar Association; Crown Prosecution Service; Justices' Clerks' Society; Metropolitan Police Service; National Crime Agency; Serious Fraud Office; Financial Conduct Authority; Insolvency Service; Competition and Markets Authority; Dijen Basu QC.

89 Crown Prosecution Service; Insolvency Service; Serious Fraud Office; Justices' Clerks' Society.

This is especially so during the early stages of an investigation. Specifying an entire device therefore prevents an unreasonable constraint being placed on the investigation.[90]

15.97 The SFO noted that specifying electronic devices helps prevent delay. Further, they said that moving away from the single item theory and imposing a blanket requirement for specificity on the warrant would be liable to cause delay or prevent some warrant applications being made.

15.98 Dijen Basu QC pointed out that while warrants may specify entire devices, a more detailed breakdown of the stored material sought will be given during the application procedure. He suggested that this is how the procedure should operate.

15.99 A number of consultees explained that specifying devices makes the execution of a warrant a straightforward process.[91] It is much better that the material sought is clear on the face of the warrant to prevent ambiguity. This is consistent with recent observations by the Supreme Court to the effect that the statutory search warrants scheme is designed to be operated speedily at an early stage in an investigation.[92] This is particularly the case in document-heavy cases.[93]

15.100 Dijen Basu QC also noted a further practical benefit to law enforcement. He pointed out that warrants which specify the devices sought reduce the risk of investigations being prejudiced. To require investigators to itemise the material of interest would be to reveal their knowledge of the criminality in question. Co-conspirators may be 'tipped off' where an investigator discloses their interest in certain electronic material. The current system allows the occupier to obtain the information relied on for the warrant in time to challenge the seizure and retention. Further, the information disclosed in the application form may be reduced, redacted or delayed in order to avoid prejudice.

Disadvantages of specifying electronic devices on the face of the warrant

15.101 Several consultees described problems with the single item theory, and specifying devices on the face of the warrant.[94] Privacy International pointed out that the drafting of warrants on the basis of devices does not limit the volume of information that can be extracted.[95]

15.102 Kent County Council Trading Standards observed that drafting warrants in terms of devices may be difficult where it is not known what devices will be on premises. The CPS accepted that identification, wherever possible, of the nature of material that the investigator seeks

---

90 Justices' Clerks' Society.

91 HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Bar Council and the Criminal Bar Association; Metropolitan Police Service; Serious Fraud Office.

92 *R (Haralambous) v Crown Court at St Albans* [2018] UKSC 1, [2018] AC 236 at [15].

93 Serious Fraud Office.

94 City of London Police Economic Crime Academy; Dijen Basu QC; Kent County Council Trading Standards; Privacy International; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Magistrates Association; Birmingham Law Society; Southern Derbyshire Magistrates' Bench; Northumbria Law School Centre for Evidence and Criminal Justice Studies; Law Society.

95 Privacy International.

may appropriately serve to focus those conducting a search of the devices on what it is really necessary to seize.[96]

15.103 Some consultees acknowledged shortcomings of device warrants, but considered that there were no preferable alternatives.[97] Other interesting observations raised by consultees were that warrants may be drafted in hybrid form,[98] referring to both devices and information stored therein, and that some issuing authorities may require the warrant to be drafted in a particular form, requiring applications to be amended and resubmitted.[99]

Analysis

15.104 After carefully considering the arguments on both sides, we have concluded that the most desirable policy position is for search warrants to contain two parts when electronic devices are sought for the purpose of obtaining electronic data. By way of summary, those two parts should be as follows:

(1) **Part 1: the electronic device(s) to be searched for and seized** – we conclude at paragraph 15.27 above that electronic devices should continue to be capable of being the target material of a search warrant. This is provided that the information sought on the devices satisfies the statutory conditions for the grant of a search warrant. Accordingly, we conclude here that search warrants should continue to permit investigators to specify on the face of the warrant, in as much detail as is practicable, electronic devices as the material to be searched for and seized.

(2) **Part 2: the information on the electronic device(s) that is sought** – search warrants should now include a second part: an itemisation or description of the nature of the information sought on electronic devices.

15.105 In our view, this position would occupy a middle ground and strike an appropriate balance between the competing interests of the investigation of crime and the privacy rights of individuals. The division of a search warrant into two parts would also reflect the distinction that we have continued to emphasise: the search of premises *for* electronic devices (with which the first part of the warrant would be concerned) and the potential on-site or off-site search *of* electronic devices for information (which would be addressed in the second part of the warrant).

15.106 As we see it, there is clear value in search warrants specifying on their face the underlying information sought on devices, even if an investigator is still authorised to search for and seize entire devices. First, the warrant would make clear to an individual the extent of the intrusion into their private life that has been authorised. We accept that this information will be contained in the application form, of which an individual can formally request disclosure.[100] However, we consider that the information should also be contained on the warrant so that it is clear to those executing the warrant, who may be called upon to make

---

96 Crown Prosecution Service.

97 Senior District Judge (Chief Magistrate); Financial Conduct Authority.

98 Financial Conduct Authority.

99 National Crime Agency.

100 See paragraphs 9.11 to 9.14 above.

decisions on-site regarding seizure and extraction, and those who are the subject of a search.

15.107 Secondly, specifying the information sought also acts as a constraint on the level of intrusion, if not at the stage of seizure then during any subsequent examination, by making clear that which falls within and outside the scope of the warrant. The second part of the warrant would therefore be an important reference point and prevent the investigator from going on a fishing expedition.

15.108 Thirdly, specifying the underlying information sought would serve two additional functions, which we will explain in further detail in sections of the report that are to come. The first function is for the information be used as the basis to seek authorisation to search electronic devices on-site for that which is specified in the second part of the warrant.[101] This will strengthen an investigator's ability to make dynamic on the spot decisions when executing a search warrant and potentially lessen the interference with an individual's privacy rights by removing the need to seize entire devices. The second function is for the information to be used as a reference point for ascertaining which electronic data falls outside the scope of the warrant when examining electronic devices off-site.[102]

15.109 Fourthly, requiring warrants to be drafted in this way would not place undue burdens on investigators, or unreasonably constrain the execution of a search warrant. It is important to distinguish between the nature of information and the form it may take as electronic data. We accept the point made by consultees that the form information may take may not be known, however, the nature of the information must be known in order for the statutory conditions to be met. For example, the information sought may be "emails between Lyndon and Sebastian between 1 September 2019 and 31 August 2020". Therefore, the same latitude will be afforded to the investigator in specifying the information sought as is afforded when seeking to demonstrate how information stored on the device meets the statutory conditions.

15.110 The information specified in the second part of the warrant would also likely mirror the information already required to be included on the application form, which we recommend making explicit. For this reason, the inclusion of the information on the electronic device(s) that is sought will not impose an undue burden on an investigator, nor will cause additional delay. The level of specificity will of course depend on the nature of the investigation. The European Court of Human Rights has observed that there may be instances in which a search warrant couched in very broad terms is permissible, taking into account the urgency and complexity of the case.[103] The warrant should still have to identify, so far as is practicable, the information sought.[104]

15.111 Crucially, the first part of the warrant would still be able to specify the electronic device to be searched for and seized, with the appropriate level of specificity, thereby ensuring that unreasonable constraints are not placed on investigators. A search warrant would still be

---

101 We discuss this in relation to locally stored material at paragraphs 15.174 to 15.194 below and in relation to remotely stored material at paragraph 16.159 below.

102 We discuss this at paragraph 17.120 below.

103 *Sher and Others v the United Kingdom* (2015) App No 5201/11 at [174].

104 Police and Criminal Evidence Act 1984, s 15(6)(b).

capable of simple and practical execution.[105] Nor do we consider that a warrant presented in the way in which we have described would be prone to misunderstandings when executed.[106] While we expressed concern regarding the consequences that specifying entire electronic devices may have for the application of the CJPA regime, we recommend a new set of safeguards which would apply to the seizure of electronic material in Chapter 17. We also discuss further safeguards relating to the seizure of electronic devices in the next section.

15.112 The remaining issue for us to consider is that helpfully raised by Dijen Basu QC, who argues that specifying the information of interest would reveal an investigator's knowledge of the criminality in question and potentially tip-off co-conspirators. One way to meet this concern would be by redacting the information. We therefore consider the appropriateness of redacting the second part of the warrant first.

15.113 On one view, the information contained in the second part of the warrant should be disclosed without exception. The statutory safeguards,[107] and case law,[108] indicate that the copy of the warrant provided to the occupier must identify the material sought. The only information on the warrant that it seems permissible to redact is, if multiple premises are to be searched, the addresses of those other premises.[109] Accordingly, the second part of the warrant, which specifies the information ultimately sought on devices, ought to be disclosed in all cases.

15.114 One counterargument would be to distinguish the purpose of our proposed second part of the warrant. Strictly speaking, the information contained in the second part would not be the target of the warrant: the electronic device, specified in the first part, would be the material for which the warrant authorises entry onto premises to search and seize. However, our favoured view is that the information contained in the second part of the warrant still discloses the information sought and provides evidence establishing the extent of the investigator's authority to interfere with an individual's privacy rights. This view holds particular weight if the second part of the warrant is used as a reference point to search electronic devices on-site, which we recommend ought to be the case in recommendation 48 at paragraph 15.194 below. Further, if redaction were permissible, we foresee such redaction becoming commonplace, which would undermine the purpose of the second part of the warrant. For these reasons, we are of the view that it should not be permissible to redact the information in the second part of the warrant.

15.115 As we have ruled out the possibility of redaction, we are left to consider whether the potential prejudice to an investigation that might be caused by requiring a search warrant to disclose the information on devices sought is a reason not to make the recommendation. There are a number of reasons why we are not persuaded that the risk of prejudice is a sufficient reason not to require the information sought on electronic devices to be disclosed.

---

105 *R (Energy Financing Team Ltd) v Bow Street Magistrates' Court (Practice Note)* [2005] EWHC 1626, [2006] 1 WLR 1316 at para 24(5); *McGrath v Chief Constable of the Royal Ulster Constabulary* [2001] UKHL 39, [2001] 2 AC 731 at 738g.

106 *R (A) v Central Criminal Court and another* [2017] EWHC 70 (Admin) at [85], [2017] 1 WLR 3567 at [47].

107 Police and Criminal Evidence Act 1984, s 15(6)(b), 15(7) and 15(8).

108 *R v Chief Constable of Lancashire Constabulary, ex parte Parker* [1993] 2 All ER 56.

109 *R (Redknapp) v Commissioner of the City of London Police* [2008] EWHC 1177 (Admin), [2009] 1 WLR 2091 at [21]; *R (Bhatti) v Croydon Magistrates' Court* [2010] EWHC 522 (Admin), [2011] 1 WLR 948 at [22].

The risk of tipping-off will be present when hard copy documents are sought, which will require specificity. We see no reason for an investigator to enjoy a level of secrecy when electronic devices are the target material that is not possible when the target material includes hard copy documents.

15.116 Further, even if only electronic devices are specified and not the information sought thereon, the investigator's knowledge of the criminality in question is to a large extent revealed by the very execution of a warrant, which may still lead to co-conspirators being tipped-off. Finally, there are operational methods that can be, and frequently are, deployed in order to reduce the risk of prejudice. Search warrants can be executed on a number of locations simultaneously. Once lawful entry is effected, electronic devices can be searched for and secured promptly to decrease the risk of data deletion.

15.117 For these reasons, we make a recommendation accordingly.

Recommendation 48

15.118 We recommend that search warrants be required to contain two parts when electronic devices are sought for the purpose of obtaining information in the form of electronic data:

(1) the first part should specify the electronic device(s) to be searched for and seized; and

(2) the second part should specify the information on the electronic device(s) that is sought.

THE SEIZURE OF ELECTRONIC DEVICES

The current law

15.119 As set out in the relevant legal regime section at paragraph 14.43 above, the conceptualisation of an electronic device and the data stored thereon as a single item means that, where an investigator seeks specific electronic data, the whole electronic device on which it is stored may be the target of a search warrant and seized. Accordingly, an entire electronic device may be seized notwithstanding that there is only a small fraction of relevant material stored on it. Even if a search warrant is drafted in such a way that it does not permit the seizure of entire devices, section 50 of the CJPA permits an entire electronic device to be seized to sift out electronic data that is not covered by the warrant off-site.

15.120 In practice, the electronic device itself might not be physically seized. Instead, digital forensics specialists may "image" the electronic device, by extracting or copying the data stored on and/or accessible from the electronic device.

The consultation paper

15.121 In the consultation paper, we identified several arguments in favour of investigators being permitted to seize entire electronic devices instead of being required to copy relevant electronic data on-site. The first was that, in the majority of cases, seizure will be a practical necessity as extracting relevant data will not be possible. We have summarised the reasons why this is the case at paragraph 14.102 above. The second was that the seizure and retention of an entire device may assist with proving provenance, the continuity of evidence and pursuing reasonable lines of enquiry that may point away from the suspect or accused.

15.122 Conversely, we raised a concern that the seizure of entire electronic devices involves a significant privacy intrusion that may not be necessary or proportionate where only a fraction of the material on the device is target material that is sought, which may also be obtainable by other means. In particular, the seizure of whole devices may lead to the seizure of irrelevant, highly personal and protected material. Coupled with the ability to specify entire electronic devices on the face of the warrant, electronic devices may be seized without the protections under part 2 of the CJPA applying because the device itself is not mixed with, or contained in, something which the investigator is not entitled to seize.

15.123 These were all reasons for which we invited views[110] on the single item theory, asking whether it works effectively and fairly in practice.

Consultation responses

Advantages of being permitted to seize entire electronic devices

15.124 Several advantages were advanced in support of investigators being permitted to seizure entire electronic devices when executing a search warrant.

15.125 The SFO and Financial Conduct Authority told us that it is almost always impracticable to separate relevant electronic material from a device during a search. The following analogy was given: you can very effectively separate the salt from seawater in a desalination plant under controlled conditions, but it is a futile exercise to try and do so with your fingers on a beach. This applies irrespective of cyber forensic resources as there would still be insufficient time to perform a forensic extraction of relevant data. It would also involve in many instances being on premises for days or potentially weeks to complete searches. Other obstacles include where there are a significant number of devices or where devices are locked and encrypted. Therefore, as a practical matter, there are distinct advantages to permitting law enforcement to remove electronic devices for later analysis.

15.126 Other consultees pointed out that the seizure of entire devices can be less intrusive than searching for particular files on the premises.[111] It can be distressing to family members to watch while law enforcement officers search for particular files or types of files for prolonged periods while on the premises. Further, it was suggested that search warrants which specify electronic data as the target material may increase the likelihood of mistakes being made.[112]

15.127 The CPS explained that the seizure of an entire electronic device allows investigators to fulfil their disclosure responsibilities by following all reasonable lines of enquiry. It was suggested that, even if relevant electronic data could be extracted from a device, the response from the suspect will be likely to be that no attempt has been made to look for or to seize any other communications which cast a different light on those inculpatory statements, or indeed other communications which are exculpatory in nature.

15.128 Relatedly, a number of consultees pointed out that the seizure of an entire device ensures that all relevant evidence is captured.[113] There was said to be a risk of missing relevant evidence if seizure is limited to relevant material stored on the device. HMRC explained that

---

110 Consultation Question 51.

111 Justices' Clerks' Society; Metropolitan Police Service.

112 Justices' Clerks' Society.

113 Crown Prosecution Service; Competition and Markets Authority; Serious Fraud Office.

target searching electronic devices using search terms may identify some user created files, however, not all relevant evidence may respond to search terms. Further, there may be a need to obtain supporting data in the form of artefacts on the device which indicate dates, times and user creation (provenance). These artefacts would not be obtained if the entire electronic device was not imaged, meaning that consequently proving context and relevance of user files would be impossible.

15.129 Consultees also pointed out that specifying electronic devices reduces the risk of ambiguity arising over whether an investigator was entitled to seize evidence where the scope of the investigation widens shortly after the material is seized.

15.130 The Insolvency Service described how it is still possible to minimise intrusion where entire devices are seized. This can be achieved by applying search terms to identify relevant material sought. They suggested that this procedure has been carefully developed and that they engage with defence teams to ensure that there is no intrusion beyond the investigation being conducted.

15.131 The FCA agreed, noting that even where entire devices are seized, provision can be made to reduce the inconvenience caused.[114] For example, the investigator may allow important documents which are required for business continuity or children's exams to be made available to the subjects affected.

Disadvantages of being permitted to seize entire electronic devices

15.132 Several consultees described issues with the seizure of entire electronic devices and the single item theory more generally.[115]

15.133 A number of consultees considered that the seizure of entire devices which contain irrelevant material raises issues regarding individual privacy, necessity and proportionality.[116] Some consultees argued that the seizure of an entire device may be disproportionate and therefore constitute an infringement of article 8 of the ECHR.[117] For example, the seizure of a device containing large volumes of sensitive information might be regarded as disproportionate.[118]

15.134 The potentially serious consequences for the owner being denied access to their device were highlighted by a number of consultees.[119] One consultee illustrated the importance of access to electronic devices by referring us to a number of authorities in the context of restrictions placed pursuant to Sexual Harm Prevention Orders.[120] In one case, a blanket prohibition on computer use or internet access was described by the Court of Appeal as

---

114 Financial Conduct Authority.

115 City of London Police Economic Crime Academy; Dijen Basu QC; Kent County Council Trading Standards; Privacy International; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Magistrates Association; Birmingham Law Society; Southern Derbyshire Magistrates' Bench; Northumbria Law School Centre for Evidence and Criminal Justice Studies; Law Society.

116 Magistrates Association; Southern Derbyshire Magistrates' Bench; Northumbria Law School Centre for Evidence and Criminal Justice Studies; Law Society; Privacy International.

117 Law Society; Northumbria Law School Centre for Evidence and Criminal Justice Studies.

118 Privacy International; Magistrates Association.

119 Magistrates Association; Northumbria Law School Centre for Evidence and Criminal Justice Studies.

120 Northumbria Law School Centre for Evidence and Criminal Justice Studies.

disproportionate because it restricted the defendant in the use of what was described as an essential part of everyday living.[121] Affirming the decision, the Court of Appeal has recently observed that, since then "the importance of the Internet for everyday living has increased considerably".[122]

15.135 Northumbria Law School Centre for Evidence and Criminal Justice Studies also noted that it may be disproportionate to seize a device where it is used as a means to access stored data, if such data could be accessed by law enforcement using other means.[123]

15.136 The seizure of entire electronic devices also raises issues in respect of the protection afforded to legally privileged material and other forms of protected material.[124] It was acknowledged by one consultee that conceptualising devices as a single item means that the plain words of section 50 of the CJPA exclude its operation.[125] Another consultee said that the use of the CJPA is poorly understood across policing, in part because of the interpretation of digital containers being regarded as a single item.

15.137 A number of consultees who raised issues with the seizure of devices observed that ancillary issues then arise regarding how information is sifted, removed and stored.[126]

15.138 Some consultees observed that the single item theory is applied inconsistently across police powers.[127] For example, it was said that the single item theory will not apply in the case of the seizure of either paper documents (such as a lever arch file) or electronic devices where premises is searched without a warrant under sections 18 and 32 of PACE. This is because, in their view, it is only in respect of electronic devices, and when sought under a warrant, that law enforcement agencies are entitled to treat electronic devices as a single storage entity. As a consequence, where relevance cannot be ascertained the seize and sift provisions under the CJPA must be used.[128]

Analysis

The seizure of entire electronic devices

15.139 We have little hesitation in concluding that investigators should be able to seize entire electronic devices. It will often be impractical to separate relevant electronic material from a device during a search for the reasons set out at paragraph 14.102 above. If an electronic device could not be seized, and it was not possible to examine the device at the scene, vital evidence would be irrecoverable. The inevitability of over-collecting data is a reality that is recognised in other jurisdictions which permit the seizure of entire devices.[129] Even if it is possible to image electronic devices at the scene, it may be preferable to do so in a forensic

---

121 *R v Smith* [2011] EWCA Crim 1772, [2012] 1 WLR 1316 at [20].

122 *R v Parsons* [2017] EWCA Crim 2163, [2018] 1 WLR 2409 at [9].

123 Northumbria Law School Centre for Evidence and Criminal Justice Studies.

124 HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Magistrates Association; Birmingham Law Society; Privacy International.

125 Dijen Basu QC.

126 Law Society; Northumbria Law School Centre for Evidence and Criminal Justice Studies.

127 City of London Police Economic Crime Academy; Dijen Basu QC.

128 City of London Police Economic Crime Academy.

129 Federal Rules of Criminal Procedure (United States), r 41(e)(2)(B).

laboratory in certain circumstances. For example, it may take an inordinate amount of time to image devices on premises.

15.140 The main problem arising from the seizure of entire electronic devices is that huge quantities of irrelevant, sensitive and protected material may be taken into the investigator's possession. Further, individuals, including those who are not suspected of any criminality, may be left without their devices, with negative consequences for their professional, educational and personal lives. We accept that, at a practical level, there is an operational necessity for law enforcement agencies to limit the amount of data that their investigative teams reviews. Investigators are therefore unlikely, if ever, to inspect every last byte of personal data. Be that as it may, the intrusion of privacy that occurs when large volumes of data are seized or copied cannot be ignored, still less downplayed.

15.141 The question therefore becomes what safeguards should there be to prevent unnecessary interference with an individual's privacy rights and minimise the volume of electronic data acquired by law enforcement agencies to that which is necessary. Taking into account those recommendations already made, and those we are yet to make, we regard the following matters as tempering the power of the state to seize an individual's electronic device.

15.142 First, the entry onto premises, search for and seizure of an electronic device must be authorised by a judicial officeholder. At Recommendation 45,[130] we recommend that statutory conditions be amended to clarify that electronic devices can only be the target of a search warrant if the data sought satisfies the statutory conditions relating to the target material. We also recommend that search warrant application forms be amended to require an investigator to explain what information on devices is sought (Recommendation 46[131]) and why they believe that the information is on the device and why the information would satisfy the statutory conditions (Recommendation 47[132]). This should lead to greater scrutiny of whether the search for and seizure of an electronic device is necessary.

15.143 Secondly, in Chapter 17, we recommend a Code of Practice, which would provide a set of overarching principles and regulate the acquisition and treatment of electronic material. One of the principles ought to be minimising, where possible, the volume of data that investigators seize from premises in the first instance. The Code should also emphasise the importance of considering whether data can be obtained through alternative, less intrusive means.[133] A Code would also be flexible enough to apply to a range of scenarios. For example, with the cooperation of an occupier, relevant electronic data could potentially be extracted without the need for a device to be seized.

15.144 We would also point out that in many cases there will be an incentive for law enforcement agencies to extract as little data as is necessary given that investigators will have to process

---

130 See paragraph 15.34 above.

131 See paragraph 15.62 above.

132 See paragraph 15.66 above.

133 See *R v Bater-James* [2020] EWCA Crim 790 at [78] in which Fulford LJ, giving guidance on the approach to obtaining and examining witness's electronic devices, stated that investigators need to consider whether it is possible to obtain relevant electronic data by other means. See also *R (Energy Financing Team Ltd) v Bow Street Magistrates' Court* [2005] EWHC 1626 (Admin), [2006] 1 WLR 1316 at [24(1)] in which Kennedy LJ stated that, before seeking or issuing a warrant, it is always necessary to consider whether some lesser measure to obtain the material will suffice.

all of the material that they seize or copy. The processing of data becomes more time and resource intensive the more material that is seized or copied.

15.145 Thirdly, in the next section, we recommend that investigators should be able to apply for authorisation to search electronic devices while on premises. One of the advantages of such a power would be that it would, in appropriate cases, alleviate the need to seize electronic devices.

15.146 Fourthly, in Chapter 17, we recommend a new statutory regime governing the treatment of electronic material seized pursuant to a search warrant. This regime would require investigators to be more transparent in how they intend to examine electronic data. The statutory regime would also provide avenues for investigators to be held accountable for their treatment of electronic data.

15.147 For these reasons, we conclude that investigators should remain empowered to seize entire electronic devices, subject to the safeguards above.

The copying of electronic devices

15.148 A separate yet related issue concerns the copying, rather than seizing, of an electronic device. This conduct can also be described as the electronic device being imaged or the electronic data stored on the device being extracted. By this, we therefore mean the use of digital forensic tools to extract electronic data in order to produce a partial or whole forensically sound copy of the electronic device. We discuss this practice in our section on digital forensics at paragraphs 14.97 to 14.112 below. We are not concerned here with the *search* of an electronic device for relevant electronic data, which we discuss in the next section.

Can investigators copy electronic data instead of seizing an electronic device?

15.149 As indicated above, in practice, electronic devices are sometimes copied instead of seized. It seems to be understood in practice that this is permissible. However, we have considered whether search warrant provisions do in fact permit electronic devices to be copied as a matter of law. While it will depend on the proper construction of the statute concerned, we consider it likely that most search warrant provisions permit the partial or whole copying of electronic data from electronic devices in lieu of physically seizing and taking away the device.

15.150 The power to copy electronic data from devices is explicit under the CJPA, which states that to seize something includes to make a copy of it.[134] Under PACE, support for interpreting the phrase seizure in section 8(2) to include copying can be read from a number of provisions.[135] Other language may be used. For example, the Criminal Justice Act 1987 speaks of "tak[ing] possession",[136] which we regard as broad enough to cover the imaging of electronic devices.

15.151 Reliance could also be placed on the principle of statutory construction that a statute is "always speaking".[137] Accordingly, it could be argued that the underlying policy and purpose

---

134 Criminal Justice and Police Act 2001, s 63(1).

135 Police and Criminal Evidence Act 1984, ss 20(1) and 21(5).

136 Criminal Justice Act 1987, s 2(5)(b).

137 *R (Quintavalle) v Secretary of State for Health* [2003] UKHL 13, [2003] 2 AC 687 at [8].

of statutes which permit the seizure of material can only be fulfilled if an extension is made to include the copying of data. This is especially the case where there is no indication within a statute that terms such as seizure were meant to be given a restrictive meaning. While statutes permitting interference with the rights of citizens should be strictly construed,[138] an interpretation including copying within seizure may reduce interference with those rights. However, this is subject to our observation at paragraph 15.153 below regarding the extraction of volatile and remotely stored data.

Should investigators be permitted to copy electronic data instead of seizing an electronic device?

15.152 In our view, search warrant provisions should permit the copying of electronic data in lieu of the physical seizure of electronic devices. Although fact-dependent, the copying of electronic data, where possible, will generally be less disruptive than seizing an electronic device, which may leave an individual without access to their work and private life for extended periods of time.

15.153 That being said, the copying of an electronic device may result in *more* electronic data coming into the hands of an investigator than if the electronic device was seized. This is because, while a device is powered-on, it will have access to short term volatile memory.[139] Extraction tools may also copy that which is accessible from the device and therefore result in the copying of remotely stored data, which will likely be stored in another jurisdiction.[140] We discuss the implications of seizing overseas remotely stored data in the next chapter.

15.154 The possible copying of overseas remotely stored data does not lead us to the conclusion that the copying of electronic data from devices should be impermissible. This is especially so where the extraction of irrelevant or protected remotely stored data is inevitable and reasonable steps are taken to reduce the amount of data extracted. It is, however, something which should be dealt with in the Code of Practice we recommend.

Should search warrant provisions be amended to make clear that investigators may copy electronic data instead of seizing an electronic device?

15.155 A third and final question is whether search warrant provisions should be amended to make clear that they permit the copying of electronic data from electronic devices. Earlier in this chapter we made reference to the explanatory report to the Council of Europe Convention on Cybercrime, which discusses the use of appropriate terminology in search and seizure laws. It recognises that traditional terms, such as seizure, may require updating with more technologically-orientated computer terms, such as copy.[141]

15.156 As we have discussed, the majority of search warrants legislation was not drafted, nor has it been extensively amended, with electronic material in mind. This can be contrasted with search warrants legislation in other jurisdictions. A 2009 amendment to the United States Federal Rules of Criminal Procedure speaks of a search warrant authorising "the seizure or copying of electronically stored information".[142] The New Zealand Search and Surveillance Act 2012 distinguishes between seizure and the taking of "a forensic copy of a computer

---

138 D Bailey and L Norbury, *Bennion on Statutory Interpretation* (8th ed 2020) para 27.9.

139 We explain what volatile memory is at paragraphs 14.11 and 14.12 above.

140 We discuss cloud extraction software at paragraph 14.109 above.

141 Council of Europe, *Explanatory Report to the Convention on Cybercrime*, para 137.

142 Federal Rules of Criminal Procedure (United States), r 41(e)(2)(B).

hard drive".[143] The Australian Crimes Act 1914, as amended, also speaks of "copy[ing] … data".[144]

15.157 There are broader questions of whether a more substantial rewrite of law enforcement powers is desirable to take account of technological advancements. We discuss this in Chapter 18. For present purposes, we consider it desirable to update the language used in search warrant provisions so that it is made clear that the power to seize an electronic device includes the power to copy all or some of the electronic data stored on an electronic device while on premises. This would clarify the extent of the state's powers and remove any ambiguity. It may also encourage what in some cases will be a less intrusive interference with an individual's privacy rights.

15.158 As indicated at paragraph 15.148 above, we have been concerned in this section with the *copying* of electronic data from an electronic device rather than the *search* of an electronic device for relevant electronic data. From the perspective of a law enforcement agency, the cumulative effect of the recommendations and conclusions in this chapter would mean that, depending on how the warrant was worded, an investigator would have the power, amongst others, to:

(1) seize an electronic device by physically taking the hardware away;[145]

(2) copy an electronic device by extracting all or part of the data stored on the device;[146] and

(3) operate and carry out a targeted search of an electronic device while on premises in accordance with the information specified on a search warrant.[147]

Recommendation 49

15.159 We recommend that search warrant provisions be amended, where necessary, to make clear that the power to seize an electronic device includes the power to copy all or some of the electronic data stored on an electronic device while on premises.

THE SEARCH OF ELECTRONIC DEVICES ON PREMISES AND SUBSEQUENT SEIZURE OF ELECTRONIC DATA

The current law

15.160 At several points we have drawn a distinction between the search *for* an electronic device and the search *of* an electronic device. In our view, the current law is ambiguous as to the circumstances in which a search warrant permits the search *of* an electronic device on premises (also known as "in situ"), a point which we made in our consultation paper. However, in this section, we set out our interpretation of the current law.

---

143 Search and Surveillance Act 2012 (New Zealand), s 3.

144 Crimes Act 1914 (Australia), s 3L.

145 See paragraph 15.147 above.

146 See paragraph 15.149 above.

147 See Recommendation 50 (paragraphs 15.193 and 15.194 below).

15.161 When a search warrant is drafted in terms of electronic devices, the search warrant permits a search *for* an electronic device. When located, an electronic device can be seized or copied on-site, however, the wording of the warrant cannot be relied on as permitting the search of an electronic device on-site. This is also because, once the target device has been found, the search has been carried out to the extent required for the purpose for which the warrant was issued.[148] It is arguable that a search warrant that authorises a search of premises for electronic *data* authorises a search *of* an electronic device. If not, an investigator would either have to obtain consent to search a device or seize the device under the CJPA to sift the electronic data off-site.

15.162 While the search of an electronic device may not be supported by the wording of a search warrant, it can be by express statutory powers. To this end, there are statutory powers which go beyond the search *for* an electronic device and expressly authorise the operation *of* an electronic device. These powers may be exercised when executing a search warrant under particular regimes.

(1) Under schedule 15 to the Data Protection Act 2018, a search warrant authorises investigators, as well as to enter and search premises, to "inspect, examine, operate and test any equipment found on the premises".[149]

(2) Under the Consumer Rights Act 2015, an investigator who enters premises with or without a warrant[150] may, for the purpose amongst other things of seizing documents required as evidence, require a person with authority to access any electronic device and, if that is not complied with, the officer may "access the electronic device".[151]

15.163 There are some powers from which the power to search electronic devices can be inferred. For example, section 2(5)(b) of the Criminal Justice Act 1987 and section 176(5) of the Financial Services and Markets Act 2000 provide a power when executing a warrant to take any steps which may appear to be necessary for preserving relevant documents or information or preventing interference with them. Searching devices and seizing data, especially if volatile, is arguably a necessary step to preserve relevant material.

15.164 Sections 19(4) and 20(1) of PACE, which enable a constable to require the production of any information stored in electronic form, and similarly worded provisions in other statutes, are sometimes cited as permitting the search of an electronic device on premises. We discuss what we view as the correct interpretation of these sections in Chapter 18 and conclude that they do not permit an investigator to conduct a search of an electronic device.[152]

The consultation paper

15.165 In our consultation paper, we explained the ambiguity around whether the law permits those executing a warrant to conduct a search of electronic devices while on premises.[153]

---

148 Police and Criminal Evidence Act 1984, s 16(8).

149 Data Protection Act 2018, sch 15, para 5(1).

150 Consumer Rights Act 2015, sch 5, para 24.

151 Consumer Rights Act 2015, sch 5, para 31.

152 See paragraph 18.36 below.

153 Law Commission, *Search Warrants: Consultation Paper* (2018) CP No 235 paras 10.68 to 10.72.

We were informed by stakeholders that the searching of electronic devices on premises in the way described is likely to be deemed permissible by several law enforcement agencies when search warrants are executed. Although it clearly happens in practice, we were concerned that there was no clear legal basis for it. We considered that this position ought to be clarified.

15.166 Quite apart from ascertaining what the law is, some stakeholders indicated that the law should permit the search of devices. We were informed that searching electronic devices on premises has an operational benefit as it may allow law enforcement agencies to ascertain whether a device contains relevant evidence and therefore ought to be seized. Another advantage identified was that the search of devices may lead to fewer instances of seizure where it is decided that the device does not contain relevant evidence or what relevant data there is can be copied on-site.

Consultation responses

15.167 Although we did not ask a specific question on this point, consultation responses touched on it in the context of broader discussions on the shortcomings of search warrant regimes. Four[154] consultees made comments concerning the search of devices. Some comments related to using devices to search for remotely stored data, which we discuss in the next chapter, Chapter 16.

15.168 The Law Society endorsed[155] our interpretation in the consultation paper that sections 19(4) and 20(1) of PACE do not empower an investigator to conduct a search; therefore, if there is a legislative basis for searching devices on the premises, it is not through those provisions. More generally, the Law Society observed[156] that it would be beneficial to both the individual subject to a warrant and investigators to have clarity on the powers available and the extent of them.

15.169 The Whitehall Prosecutors' Group provided a general consultation response on the issue of electronic material. They argued that, in addition to seizing devices, it should also be possible for a warrant to permit the search of a device or digital storage media. The search should be for certain file types or all files responding to a certain search term specified on the warrant. This would provide investigators with the option, where appropriate, of examining the device in situ, searching for, and then taking away copies of files, thereby leaving the device behind.

15.170 The Whitehall Prosecutors' Group also explained the limits of powers to require the production of stored data by a person on the premises. They noted that there may be nobody on the premises, or at least, no person who can be trusted to access, copy and produce the data without seeking to alter or destroy it.

15.171 The National Crime Agency, as part of a general response on the issue of electronic material, discussed a "requirements-based approach" to the legal aspects of digital evidence. One of the key requirements identified for law enforcement was the capability to search through powered-on digital devices in the named premises.

---

154 Law Society; Whitehall Prosecutors' Group; National Crime Agency; Northumbria Law School Centre for Evidence and Criminal Justice Studies.

155 In response to Consultation Question 54.

156 In response to Consultation Question 56.

15.172 This requirement was also described as being "crime agnostic", and therefore relevant to the digital investigation of all crimes. However, the National Crime Agency stated that it would be particularly important for child sexual abuse and exploitation cases.

15.173 The Northumbria Law School Centre for Evidence and Criminal Justice Studies observed that there is a need for targeted search and seizure, particularly in the context of high volume data.

Analysis

15.174 We have already set out briefly a summary of the legal position. However, we have ultimately reached the view that it is ambiguous under the majority of search warrant regimes whether electronic devices can be searched on-site when executing a search warrant. This ambiguity means that the answer in respect of any given statute will likely depend on the principle of statutory construction utilised. For example, a purposive interpretation of legislation could be relied on to permit the search of electronic devices on-site.

15.175 There is also room for argument that the power to search electronic devices should be read in to certain statutory regimes by necessary implication so as to achieve the purpose of the statutory power.[157] Alternatively, the presumption against interference with a person's property or other economic interests may be invoked to favour a stricter reading of the statute.[158] A distinction may also arguably be drawn between a brief perusal of an electronic device to ascertain relevance as part of a cursory examination and a more detailed examination that occurs off-site.[159]

15.176 For present purposes, it is enough to conclude that the current law is unclear and that this ambiguity ought to be resolved. There are, in our view, three main reasons why the law should be amended to clarify whether, and if so when, electronic devices can be searched on-site.

15.177 The first reason accords with the observation made by the Law Society and which we have endorsed elsewhere: it would be beneficial to both the individual subject to a warrant and investigators to have clarity on the powers available and the extent of them. The second reason is that the limits on the use of the power could then be made explicit in its statutory formulation. A third and more specific reason is that without lawful authority, an investigator may be committing an offence under the Computer Misuse Act 1990 by searching an electronic device.[160]

15.178 We therefore proceed to consider whether investigators should have an express power to conduct a search of an electronic device while on premises and, if so, how the power should be framed.

---

157 J Auburn, J Moffett and A Sharland, *Judicial Review: Principles and Procedures* (2013) para 11.21.

158 See D Bailey and L Norbury, *Bennion on Statutory Interpretation* (8th ed 2020) para 27.9; *R v Secretary of State for the Home Department ex parte Simms* [1999] UKHL 33, [2000] 2 AC 115 at 131 by Lord Hoffman.

159 United States Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009) p 88.

160 We discuss this at paragraphs 14.65 to 14.66 above.

Should investigators have express powers to conduct a search of electronic devices while on premises?

15.179 We agree with the weight of consultees that investigators should have express powers to conduct a search of electronic devices while on premises. A number of considerations have led us to this conclusion, including the fact that there is a general consensus regarding the desirability of such a power amongst law enforcement agencies and the those who defend and represent the interests of individuals affected by a warrant.

15.180 From a law enforcement perspective, a power to search electronic devices when executing a search warrant would have a clear benefit by enabling investigators to identify there and then relevant electronic data stored on a device. Crucially, a search of an electronic device on premises may lead to securing highly relevant evidence of criminality that might not otherwise be obtainable.

15.181 Notably, Big Brother Watch has also encouraged the targeted search of electronic devices in the context of the search of complainants' devices.[161] In our view, one of the rationales they give will likely hold true for suspects' devices: the less data that law enforcement agencies seize or copy, the less of a delay to investigations and the criminal justice system more generally.

15.182 Parliament has provided law enforcement agencies with the power to obtain information stored in electronic form by specifically requiring the production of information, pursuant to sections 19(4) and 20(1) of PACE, and similar provisions. However, this does not alter our conclusion that the power to search electronic devices on premises will have value for two main reasons.

15.183 First, powers of production will have limited or no utility where there is either no occupier, an uncooperative occupier or simply too much data to expect an occupier to produce. Notably, the courts have been unimpressed by suggestions that occupiers should print off large volumes of relevant files in lieu of investigators seizing devices.[162] Secondly, there is an important distinction to be made between the production of data in native and non-native form,[163] which will have implications for the value of the electronic data: powers of production do not necessarily require information to be produced in its native form.[164]

15.184 We recognise that in some cases conducting a search of a device on premises may be difficult or impossible owing to technological barriers such as encryption. However, we do not consider that this would render toothless a power to search electronic devices on premises. For one, technical capabilities to access even protected devices vary and could improve.[165] We also discuss the related issue of compelling passwords in the next chapter.

15.185 Flexibility is undoubtedly important in this context. From a privacy perspective, a power to search electronic devices when executing a search warrant, subject to appropriate safeguards which we discuss below, *may* result in a more proportionate search and less

---

161 Big Brother Watch, *Digital strip searches: The police's investigations of victims* (July 2019) p 19.

162 *R (Paul Da Costa) v Thames Magistrates' Court* [2002] EWHC 40 (Admin), [2002] Crim LR 504 at [19]; *R* (*Cabot Global Ltd) v Barkingside Magistrates' Court* [2015] EWHC 1458 (Admin), [2015] 2 Cr App R 26 at [41] to [42].

163 We discuss these terms at paragraph 14.22 above.

164 We discuss this issue at paragraphs 16.147 and 18.40 below.

165 We discuss forensic capabilities at paragraphs 14.107 and 14.111 above.

collateral intrusion of an individual's privacy rights. In contrast, in some cases, the swift removal, copying and return of electronic devices may also be the most proportionate course of action.

15.186 The search of an electronic device on premises may reveal that it contains no relevant data, resulting in the device being neither copied nor seized. Where electronic devices do contain relevant electronic data, that data may be copied without the need to seize the device, provided investigators have the technical capability to do so and there is otherwise no good reason to seize the device. The power may therefore lead to investigators collecting less data than might otherwise be acquired. This point was also raised by Anand Doobay, a partner at Boutique Law, during our preliminary discussions with stakeholders. He suggested that the power to target search devices may remove the need to seize devices in some cases, ameliorating the effects of the seizure on the device owner.

15.187 One legitimate concern may be the risk of altering data and the contamination of evidence when electronic devices are searched on-site. Digital forensic tools include features to preserve the integrity and chain of custody of evidence. This is an issue to which law enforcement agencies will be alive, as they will be to the associated risk of evidence being excluded at trial under section 78 of PACE. These are also matters which should be addressed in any new Code of Practice. We discuss separately the desirability of a power to alter data on-site in the next chapter.[166]

15.188 For these reasons, we conclude that formalising the power to conduct a search of electronic devices on premises pursuant to a search warrant would have benefits for both investigators and those who are the subject of a search.

How should an express power to conduct a search of electronic devices while on premises be framed?

15.189 There are three key features that a power to conduct a search of electronic devices while on premises ought to have.

15.190 First, the authority to conduct a search of electronic devices should stem from the warrant and require separate authorisation. Investigators should not be able to search electronic devices on premises as a matter of course. Some jurisdictions provide for the power to operate electronic devices to access data if the investigator has reasonable grounds to believe that it contains evidential material.[167] In our view, however, a similar approach should be taken to all premises and multiple entry warrants: that a warrant may authorise the search of an electronic device on premises if the issuing authority is satisfied that it is necessary to do so in order to achieve the purpose of the warrant. The warrant should also permit the seizure or copying of any electronic data identified.

15.191 Secondly, the power to search electronic devices should be limited to the information specified in the second part of the warrant, namely the information on the devices that is sought, as recommended at Recommendation 48 above.[168] This would mean that an investigator is only entitled to search for information which an issuing authority has been satisfied meets the statutory criteria for the issue of a warrant. In our view, this would

---

166 See paragraphs 16.223 to 16.238.

167 For example see Crimes Act 1914 (Australia), s 3L(1).

168 See paragraph 15.118 above.

appropriately constrain the limits of the search and prevent the power being used to conduct a fishing expedition into a potentially limitless pool of data. It would also allow an individual to see from the warrant the extent to which their electronic devices may be searched on-site. We also recommend at Recommendation 56 that investigators should be required, if requested, to provide an audit of all actions taken in respect of electronic devices on premises.[169] This, too, would decrease the likelihood of fishing expeditions.

15.192 Thirdly, if authorisation is given to search an electronic device on premises, it should remain an operational decision of the investigator whether to exercise it, taking into account any principles or duties contained in a relevant Code of Practice. As discussed, it may not be technically possible to target search an electronic device on-site for a host of reasons. For example, there may be technological barriers such as encryption. A credible claim of legally privileged material present on the device would also rule out target searching.[170] It may also be more proportionate to seize the entire device without conducting a search of the device.

Recommendation 50

15.193 We recommend that search warrant provisions be amended to permit an investigator to apply for authority to conduct a search of electronic devices found during the course of a search where it is necessary to do so for the purpose for which the warrant is issued.

15.194 If granted, the search warrant should authorise the search for and copying of any electronic data stored on the device that corresponds to the information specified in the second part of the warrant.

169 See paragraph 17.95 below.

170 An investigator should not have sight of or access to legally privileged material. See Attorney General's Guidelines on Disclosure: Supplementary Guidelines on Digitally Stored Material (2011) at [A31]; *R (A) v Central Criminal Court and another* [2017] EWHC 70 (Admin) at [84], [2017] 1 WLR 3567 at [46].

Chapter 16: Search for and seizure of remotely stored electronic data

INTRODUCTION

16.1 In this chapter we discuss the powers that law enforcement agencies ought to have to search for and seize (ie copy) remotely stored electronic data under a search warrant. As we explained in Chapter 14, an increasing amount of data is now stored remotely and predominantly overseas. A number of consultees have said that remote storage presents one of the biggest issues for the law of search warrants. In practice, law enforcement agencies do search for and seize remotely stored data under a warrant, sometimes inevitably when imaging devices on-site.[1] However, what is clear from consultation responses is that clarity on the scope of powers to search for and seize remotely stored data is desperately needed.

16.2 The question of how search warrants should treat remotely stored data has been one of the most difficult aspects of this project. The recommendations that we make in this chapter are provisional in nature owing to the highly technical nature of the subject-matter, the overlap with other investigatory powers and the need for further cross-sectional input to refine any model adopted.

The issues in outline

16.3 Evidence of criminality may be stored in such a way that it is not stored on an electronic device but accessible from it. Electronic data may be accessible from an electronic device yet remotely stored by virtue of it being (1) on an electronic device's local area network; (2) not on a local area network but elsewhere in the jurisdiction; (3) outside the jurisdiction in a known or knowable location; or (4) in an unknown or unknowable location.

16.4 Law enforcement agencies in England and Wales need to obtain remotely stored data in order to be able effectively to prosecute crime. As a basic proposition, this is an uncontroversial statement that enjoys agreement across the spectrum of stakeholders and consultees. The prevailing view amongst consultees is also that the law governing access to remotely stored data is unclear and in need of reform.

16.5 Search warrant provisions involve the search of physical premises for evidence. Remotely stored data may theoretically be accessible from *any* electronic device on *any* premises with the right tools and access details to an online account. For example, if relevant evidence is stored in a Dropbox account, subject to any two-factor authentication that is enabled,[2] with the correct username and password, the online account could be accessed, and relevant data copied, from any internet enabled electronic device. The premises into which entry is

---

1 Consultation Question 50 in our consultation paper invited consultees to share examples of the types of electronic material that investigators seek under a search warrant. Consultees shared with us a wide range of examples of electronic data which may form the target of a search warrant, which we set out at paragraph 15.11 above. In theory, all of the electronic data set out at paragraph 15.11 above be stored remotely, including outside the jurisdiction. Consultees also confirmed that data stored in the cloud may be sought under a search warrant.

2 We explain what two-factor authentication is at paragraph 14.23(2) above.

authorised, and the electronic device through which data is accessed, may therefore be regarded as arbitrary features of a search when remotely stored data is concerned.

16.6 This raises a host of questions: are search warrants in fact the most appropriate investigative power to reform for the purpose of enabling law enforcement agencies to access and copy remotely stored data?[3] If so, what link must there be between the remotely stored data, the online service that stores the data, the electronic device from which the online service is accessible and the premises to be entered and searched in which the electronic device is found? Does the existence of remotely stored data call for new law enforcement powers drafted in terms of electronic devices instead of physical premises, or authorising the remote execution of a search warrant without entry into physical premises or the conducting of a search through another person's device?

16.7 Any reform of search warrants legislation therefore requires the identification of a coherent and rational thread, which ties relevant data that is stored remotely by an online service to a particular electronic device which is found in particular premises. Where this thread exists, a search warrant can be deemed an appropriate investigative power, subject to appropriate conditions.

16.8 In considering the circumstances in which search warrants should permit the search for and seizure of remotely stored data – or more accurately (1) the search of premises for an electronic device; (2) the search of an electronic device for an accessible online account or cloud connection; and (3) the search of an accessible online account or cloud connection for remotely stored data – our task has been further complicated by a number of matters.

16.9 The distinction between electronic data stored on a device and electronic data stored remotely but accessible from a device can seem itself an arbitrary distinction. Data can be stored remotely by a suspect both easily and unknowingly. It is also in one sense meaningless to describe data as having a location at all given that it may be fragmented, transitory and/or in an unknown and unknowable location. As a result, law enforcement agencies may not know, and, in some cases, could not be expected to know, where remotely stored data is physically located in advance of a search of premises.

16.10 At the same time, the location of electronic data is treated as significant under international law, with enforcement powers in respect of overseas data engaging issues of jurisdiction and territoriality. As a consequence, there is a risk of the exercise of search warrants impinging on international relations where overseas data is accessed and copied. This means that any recommendations for reform must be formulated in a way that is alive to international law principles and current state practice. However, the circumstances in which the search for and seizure of overseas data is deemed permissible under international law is unclear as other states grapple with these very same questions.

16.11 Privacy concerns are also intensified where law enforcement agencies are empowered to enter individuals' online lives which hold an almost limitless amount of information. A carefully crafted regime is therefore necessary that takes into account all of these matters, paying sufficient regard to:

(1) the importance of ensuring law enforcement agencies are equipped to investigate and prosecute crime;

[3] The Investigatory Powers Act 2016 and Regulation of Investigatory Powers Act 2000 are not within our terms of reference: see paragraph 1.9 above.

(2) the practical realities and challenges that are posed to investigators from cloud computing;

(3) the nature of remotely stored electronic data;

(4) the international law implications of accessing and copying such data; and

(5) the heightened privacy considerations that are now engaged by remotely stored data.

The structure of this chapter

16.12 In the consultation paper, our consultation questions concerning electronic material were presented in a single chapter dealing with both remotely and locally stored data. In respect of remotely stored data, we asked the following general questions:

(1) whether law enforcement require powers of extraterritorial search, seizure and production;[4] and

(2) whether the powers of production under the Police and Criminal Evidence Act 1984 ("PACE") require reform.[5]

16.13 Consultation responses covered wide ground, providing us with experiences and concerns about numerous related legal issues within the broad context that we had set out. In light of the consultation responses, we discuss the following five issues:

(1) the extent to which the search for, seizure and production of remotely stored material involves an extraterritorial use of investigative powers;

(2) the current international law position regarding the search for, seizure and production of remotely stored material;

(3) the framing of a power to enter premises, search devices for and copy remotely stored material;

(4) amending the laws governing the compulsion of passwords and other access information for electronic devices and online accounts; and

(5) introducing a power to modify or alter remotely stored data in order to preserve it and prevent interference.

16.14 While we discuss the extraterritoriality and international law implications of production powers in issues (1) and (2) above, we do not discuss production powers in great detail in the remaining issues. This is because production powers are exercisable not only when executing a search warrant. We do, however, recommend considering the operation of production powers as part of a wider review of law governing electronic material in Chapter 18 below. In that section, we specifically discuss the application of sections 19(4) and 20(1) of PACE to remotely stored data and conclude that the powers can compel the production of data stored remotely overseas.

---

4 Consultation Question 55.

5 Consultation Question 54.

Summary of our conclusions and recommendations concerning remotely stored electronic data

The extraterritorial application of search, seizure and production powers

16.15 We begin the chapter by discussing the extraterritoriality of powers of search, seizure and production. We conclude that it is unclear whether powers of search, seizure and production exercised within this jurisdiction in relation to remotely stored data should be classified as extraterritorial: while the powers are exercised within this jurisdiction, the location of data still holds particular significance. However, even if such powers were to be deemed extraterritorial, we consider it unlikely that the presumption against a statute having extraterritorial effect would operate so as to prevent the powers being exercisable in respect of remotely stored data.

The circumstances in which the search, seizure and production of remotely stored data is permissible under international law

16.16 We then turn to consider the circumstances in which the search, seizure and production of remotely stored data is permissible under international law. Any reform must be alive to recent state practice and international law principles to prevent risks to international relations and offending the sovereignty of other states. We conclude that the answer, too, is unclear: state practice indicates certain instances in which the conduct might be deemed acceptable, however, concerns clearly remain in the international community with no clear international consensus.

16.17 Remotely stored data must be accessed and copied by law enforcement agencies, in limited and regulated circumstances, when executing a search warrant for the legitimate aim of detecting, investigating and prosecuting crime. Given the lack of clarity surrounding the application of international law principles, the question best asked is whether the particular exercise of powers of search and copying is likely to offend state sovereignty and international comity. We consider that there will be circumstances in which the search, seizure or production of remotely stored data pursuant to a warrant is unlikely to cause a grievance from another state and that any infringement on the sovereignty of another state would be *de minimis*.

The search of premises for and copying of remotely stored data

16.18 The remainder of the chapter discusses reform to search warrant provisions. We conclude that law enforcement agencies should be given the powers to enter premises, search for and copy remotely stored data when executing a search warrant. Such powers are necessary to protect the public and effectively investigate and prosecute crime. There will be circumstances where it is not practicable to obtain evidence by means other than executing a search warrant.

16.19 It is unclear under the current law in what circumstances the search for and copying of remotely stored data is permitted. Irrespective of whether law enforcement agencies can search and copy remotely stored data under any given regime, such acts should be governed by a clearer framework. The law should therefore be amended.

16.20 Any amended laws must not unreasonably constrain the ability of law enforcement agencies to obtain remotely stored data. At the same time, amended laws must be drafted in such a way that there is an appropriate link between the remotely stored data and premises to be searched and so that jurisdictional problems will not arise. The search and copying of remotely stored data must have identifiable boundaries that ensure that authorisation is

given only where necessary to do so and the search is carried out in a proportionate manner subject to stringent safeguards.

16.21 It is not possible for us to reach a definitive conclusion on the appropriate model to be adopted for the search and seizure of remotely stored data in respect of the many search warrant regimes without further technical and cross-sectional input. There are a host of highly technical issues that must be resolved and on which we did not receive sufficient evidence to reach a considered conclusion. Any reform must also consider the interplay with powers under IPA, the Regulation of Investigatory Powers Act 2000 ("RIPA") and other Acts which fall outside of our terms of reference.

16.22 We recommend that the Government considers the desirability of amending the law to permit law enforcement agencies to obtain authorisation to search for and copy remotely stored data when executing a search warrant.

Compelling access to protected information

16.23 We then turn to consider amending the law governing the power to compel the production of passwords and other access information. While this is an issue that also arises in the context of locally stored material, it is particularly acute in relation to remotely stored material and so we discuss the matter in this chapter.

16.24 We accept that without a power to require passwords, any power to search for and copy remotely stored material will be rendered ineffective in certain circumstances given that virtually all electronic data is protected by either a password, encryption or two-factor authentication.[6] We set out the various arguments in favour of reforming the law. For a number of reasons, we do not make a firm recommendation. That said, based on the consultation responses that we did receive, and the analysis that we have undertaken, we consider that it is a matter that would merit further consideration.

16.25 We recommend that the Government considers the desirability of amending the law governing the power to compel the production of passwords and other access information with the aim of making the law clearer and more effective. This should include consideration of an integrated power to form part of search warrant regimes.

Preventing interference with remotely stored data

16.26 We turn finally to consider introducing a power to modify or alter remotely stored data in order to preserve it and prevent interference. There are few, if any, statutory powers that could be relied on as a lawful basis to modify or alter remotely stored data. Seeking preservation from service providers or other states is not an effective means of preventing the modification or alteration of remotely stored data to prevent interference. We therefore discuss whether law enforcement agencies should have the power to modify or alter remotely stored data to prevent interference with it. We recognise the rationale of a power to modify or alter data to prevent interference, as well as the valid concerns that would be raised by such an intrusive power. Again, for a number of reasons, we do not make a firm recommendation.

16.27 We recommend that the Government considers the desirability of introducing a power to modify or alter remotely stored data exercisable pursuant to a search warrant.

---

6 We explain what these security features are at paragraph 14.23 above.

THE EXTRATERRITORIAL APPLICATION OF SEARCH, SEIZURE AND PRODUCTION POWERS

Electronic data and extraterritoriality

16.28 In the consultation paper, we describe powers exercised within England and Wales to search for, seize or require the production of data stored remotely overseas as being "extraterritorial". We use the term extraterritorial to denote the enforcement of laws by a state in relation to matters (ie electronic data) outside of its own territory. Most frequently extraterritorial electronic data will be located in the territory of another sovereign state. However, as we discuss at paragraph 14.28 above, electronic data could also conceivably be stored in data centres on the high seas or in space.

16.29 The precise circumstances in which we regard the exercise of enforcement powers as being extraterritorial in this context are:

(1) an investigator, executing a search warrant on premises in England and Wales, searches an electronic device for, and/or seizes, data stored remotely overseas; or

(2) an investigator, executing a search warrant on premises in England and Wales, requires an individual to produce data stored remotely overseas that is accessible to the individual from the premises.

The consultation paper

16.30 We invited consultees' views on whether law enforcement agencies require powers of extraterritorial search, seizure and production under warrant.[7] Four consultees queried the underlying premise of this consultation question that powers of search and production exercised within the jurisdiction involved an extraterritorial application of enforcement powers.[8]

16.31 In this section, we consider whether we were in fact right to describe the exercise of powers of search, seizure and production in the circumstances set out at paragraph 16.28 as being extraterritorial. The answer is relevant to construing the application of the current law. This is because there is a presumption that, unless the contrary intention appears, a power conferred by a statute does not apply extraterritorially to people or matters outside its territory.[9] Our conclusions will also be relevant to our analysis of what is permissible under international law.

Consultation responses

16.32 Consultees put forward a number of arguments in support of the view that powers of search, seizure and production exercised within the jurisdiction but involving the interaction with material located abroad do not constitute extraterritorial action. These arguments fell under two headings. The first set of arguments sought to emphasise particular connections that the exercise of the power or the electronic data has with the state's own jurisdiction which meant

---

7 Consultation Question 55.

8 Crown Prosecution Service; Competition and Markets Authority; Whitehall Prosecutors' Group; Financial Conduct Authority.

9 D Bailey and L Norbury, *Bennion on Statutory Interpretation* (8th ed 2020) para 4.8.

that powers were not exercised extraterritorially. The second set of arguments sought to challenge the meaningfulness of treating electronic data as being located somewhere.

The jurisdictional connection

16.33 The Crown Prosecution Service ("CPS") argued that the enforcement action undertaken by law enforcement occurs within the jurisdiction, notwithstanding that the material is located in another jurisdiction. Accordingly, the exercise of enforcement powers could not be described as extraterritorial. It was likened to using a camera with a telescopic lens from English waters to observe and take pictures of a vessel by the French coast which may be about to import prohibited items into England.

16.34 In a similar vein, the Competition and Markets Authority considered that the fact that material stored overseas is accessible from premises within England and Wales means that powers of search and production were not "extraterritorial".

16.35 The CPS also argued that no issue of jurisdiction arises where the material has been created and/or accessed from the premises but the occupier has chosen from within the jurisdiction to store it overseas where it remains otherwise accessible.

The meaningless of describing data as having a location

16.36 The Whitehall Prosecutors' Group argued that it was "not meaningful" to describe data as existing in any physical location, and as such it was not meaningful to describe the search of a remote data storage facility, or requirement to produce cloud data, as an extraterritorial use of the power.

16.37 The Whitehall Prosecutors' Group observed that if documents do have a physical presence then it is virtually impossible to divine where it might be. It *might* be possible to locate, in any one moment of time, the location(s) of the various bytes of data that collectively comprise the file that is the document of interest. However, locating the various bytes of data is not the same as identifying, in any real sense, the location of the document itself. It was pointed out that those bytes of data may move to another server, potentially in another jurisdiction, moments later. As a result, there is never any guarantee that all bytes of data that comprise a file of interest will be stored on the same physical server, nor on servers in the same jurisdiction.

Analysis

Does the search, seizure and production of overseas data involve an extraterritorial exercise of power?

16.38 In our view, the arguments for and against the search, seizure and production of overseas data being classed as extraterritorial are finely balanced. The question is not one that we are compelled to answer for the purpose of recommending reform to the law of search warrants. This is because of further conclusions that we make in this section concerning the presumption against extraterritoriality and in our section discussing international law below, which means that nothing will significantly turn on the answer either way. That said, we discuss the possible arguments here as it is a matter on which we received several consultation responses.

The jurisdictional connection

16.39 We agree that the location of electronic data can seem arbitrary. A British national, situated in England, can create or access electronic data that is stored on a server located in another

country by using an electronic device with minimal effort involved. Data could be stored overseas either unintentionally, given the ubiquity of cloud computing, or purposefully to frustrate a criminal investigation. An investigator, conducting a domestic investigation, may then exercise powers of search, seizure or production within the jurisdiction, with any obligations placed on the individual to perform acts that are again within the jurisdiction. At all relevant times, the actual location of the data may be unknowable to both the British national and the investigator.

16.40 We consider that the most powerful factor in favour of construing these acts as territorial is that they are exercised from *within* the jurisdiction. On one view, it therefore seems overly technical to argue that a law enforcement agency is acting extraterritorially if overseas data is being copied from an electronic device, or required from an individual, located in England and Wales, particularly in the circumstances described in the paragraph above. In our view, it is nonetheless inescapable that, even if the data is unintentionally stored overseas by a British national in an unknowable yet accessible location, the electronic data *is* stored abroad, most likely within the jurisdiction of a foreign sovereign.

16.41 The answer to the question is therefore likely to depend on how much weight is given to the location of the data, for the data being situated abroad is the only feature that could classify the exercise of the power as extraterritorial in these circumstances. Accordingly, a finding of extraterritoriality rests on the premise that the location of data is a determinative factor in whether the power is exercised extraterritorially.

16.42 One judgment that may be relied on for the proposition that the location of electronic data is determinative is the decision of the United States Court of Appeals for the Second Circuit in *Microsoft v US*. In that case, the court regarded a warrant requiring Microsoft to produce data as an extraterritorial exercise of power as the data was stored in Dublin and would involve Microsoft interacting with its Dublin datacentre.[10]

16.43 In our view, this judgment should be treated with caution, as it involves a completely different legal system and different factual matrix to the scenarios that we have considered. In particular, Microsoft was compelled to disclose the electronic communications of a customer, a suspect whose citizenship and location were unknown. Judge Lynch, in a concurring opinion, also considered that it would be "remarkably formalistic" to classify action as extraterritorial where the US Government was demanding the data of a US citizen resident in the US and the data was located abroad as a result of the US customer misrepresenting their residence.[11]

16.44 It is also to be borne in mind that the magistrate at first instance disagreed that the proposed execution of the warrant was extraterritorial.[12] The matter was due to be heard before the Supreme Court of the Unites States until Congress enacted an amendment to the relevant statute making the appeal unnecessary.[13] The reasoning of the Court of Appeals for the

---

10 *Microsoft v United States* 829 F 3d 197 (2d Cir. 2016), pp 39 to 40.

11 *Microsoft v United States* 829 F 3d 197 (2d Cir. 2016), p 15 by Judge Lynch.

12 *In re Warrant*, 15 F Supp 3d at 475–76.

13 *United States v. Microsoft Corp.*, 584 US ___, 138 S Ct 1186 (2018).

Second Circuit on the point of extraterritoriality has also been the subject of academic criticism.[14]

16.45 The decision of the Divisional Court in *R (KBR) v Director of the Serious Fraud Office*[15] is perhaps more instructive. The case concerned the question of whether the Serious Fraud Office's ("SFO") power to issue a notice under section 2(3) of the Criminal Justice Act 1987 requiring the production of documents extended to a foreign company in respect of documents held outside the jurisdiction of the UK. In construing the statute, Gross LJ stated:

> Turning to section 2(3) itself, in my judgment and as a matter of first importance, it must have an element of extraterritorial application. It is scarcely credible that a UK company could resist an otherwise lawful section 2(3) notice on the ground that the documents in question were held on a server out of the jurisdiction.[16]

16.46 It could be said that implicit in this statement is the premise that the service of a section 2(3) notice on a UK company in the UK jurisdiction requiring the production of overseas data would involve "extraterritorial application". If so, the location of the data would be determinative of the question of whether the power is exercised extraterritorially. This is because, on those facts, extraterritoriality could not be founded on the nationality of the recipient or the location at which the power is exercised. However, the Divisional Court did not engage fully with this point and so it relies heavily on inference.

16.47 As regards powers of search and seizure, support for the argument that the location of data is determinative may be drawn from the Council of Europe Cybercrime Convention. The Cybercrime Convention is a multilateral treaty regulating, amongst matters, law enforcement investigations involving cyberspace. The UK has ratified the Cybercrime Convention and it has been in force since 1 September 2011.[17] The Cybercrime Convention addresses both "the search and seizure of stored computer data"[18] and "trans-border access to stored computer data".[19] In respect of the later, article 32 provides that:

> A Party may, without the authorisation of another Party:
>
> a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
>
> b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

16.48 In our view the Cybercrime Convention and its explanatory notes suggest that the exercise of powers of search and seizure in this jurisdiction which involve the interaction with data stored abroad is an extraterritorial exercise of such powers. Even if law enforcement officers do not leave the physical territory of England and Wales when exercising enforcement

---

14 Jennifer Daskal, "The Un-Territoriality of Data" (2015) 125 *Yale Law Journal* 326.

15 *R (KBR) v Director of the Serious Fraud Office* [2018] EWHC 2368 (Admin), [2019] QB 675.

16 *R (KBR) v Director of the Serious Fraud Office* [2018] EWHC 2368 (Admin), [2019] QB 675 at [64].

17 See https://www.gov.uk/government/publications/convention-on-cybercrime--2.

18 Convention on Cybercrime (Budapest, 23 November 2001) ETS No 185, art 19.

19 Convention on Cybercrime (Budapest, 23 November 2001) ETS No 185, art 32.

powers, they may be regarded as venturing into another state's cyber-territory and therefore acting extraterritorially.

16.49 The location of data may also be regarded as a determinative factor in cases of search, seizure and production where the data on overseas servers are altered or modified when data is accessed, copied or produced. Therefore, while acknowledging the attractiveness of the CPS's telescope analogy, the telescope would not involve a physical interference with anything on French soil. The search for and seizure of data could, depending on what was done, involve altering data stored on French servers.[20] A state may, in certain circumstances, regard effects produced on their territory by digital means as a breach of sovereignty.[21]

The un-territorial nature of electronic data

16.50 We acknowledge the argument that electronic data is inherently "un-territorial" and that describing data as being located somewhere is misleading.[22] Jennifer Daskal captures the essence of the argument in the following way:

> Modern technology challenges basic assumptions about what is "here" and "there." It challenges the centrality of territoriality within the relevant statutory and constitutional provisions governing the search and seizure of digitized information. After all, territorial-based dividing lines are premised on two key assumptions: that objects have an identifiable and stable location, either within the territory or without; and that location matters—that it is, and should be, determinative of the statutory and constitutional rules that apply. Data challenges both of these premises. First, the ease, speed, and unpredictability with which data flows across borders make its location an unstable and often arbitrary determinant of the rules that apply. Second, the physical disconnect between the location of data and the location of its user—with the user often having no idea where his or her data is stored at any given moment—undercuts the normative significance of data's location.[23]

16.51 The strength of this argument turns on how the nature of electronic data is perceived. We remain of the view that we adopted in our consultation paper:[24] data, even if fragmented and unknown, exists somewhere. Additionally, from an international relations perspective, to treat all electronic data as inherently non-territorial would likely have wider ramifications for international comity.[25]

Conclusion

16.52 Looking at the matter in the round, it is arguable either way whether the search for, seizure of or requiring the production of overseas data involves an extraterritorial exercise of power.

---

20 Jonathan Hall, "Restraint orders: R v Teresko (Case Comment)" [2018] *Criminal Law Review* 81 at 83 to 84.

21 Ministère des Armées, *International Law Applied to Operations in Cyberspace* (October 2019) p 7.

22 Jennifer Daskal, "The Un-Territoriality of Data" (2015) 125 *Yale Law Journal* 326 at 329; B Schafer and S Mason, in S Mason and D Seng, *The Characteristics of Electronic Evidence* (4th ed 2017) para 2.10; David Harvey, "Here's the thing: the cyber search provisions of the Search and Surveillance Act 2012" (2013) 10 *Digital Evidence and Electronic Signature Law* 39.

23 Jennifer Daskal, "The Un-Territoriality of Data" (2015) 125 *Yale Law Journal* 326 at 329.

24 Search Warrants (2018) Law Commission Consultation Paper 235, para 10.74.

25 Alex Davidson, "Extraterritoriality and statutory interpretation: the increasing reach of investigative powers" (2020) 1 *Public Law* 1 at 5.

The question of whether data is held abroad extraterritorially is one about which technologists and others may disagree. While the location of data may be arbitrary, it is still legally significant. With so many variables, including who created the data and where, the facts of individual cases may point to different conclusions. A different answer may also be arrived at based on the power being exercised: as powers of production are exercised *in personam* (against the person), a claim of extraterritoriality may be regarded as more tenuous.

16.53 All of this is not to say that the comments made by consultees and within the academic literature have no bearing on what is permissible under the current law or how reformed laws should be framed. It is our view that the considerations discussed are relevant to the operation of the presumption against extraterritoriality and whether the exercise of such powers would offend the sovereignty of other states.

Would the presumption against extraterritoriality operate to prevent the search and seizure of data stored outside the jurisdiction?

16.54 There is a presumption that, unless the contrary intention appears, a statute is taken not to apply extraterritorially to people and matters outside the territory to which it extends.[26] Whether this presumption is rebutted, and therefore whether a provision does have extraterritorial application, is a question of statutory construction,[27] having regard to the wording of the provision in question, the statutory purpose and the relevant context.[28]

16.55 While the question of extraterritorial application depends on a construction of the statutory provision concerned, as a general observation, even if the search for and seizure of remotely stored data was deemed an extraterritorial exercise of power, it is our view that the presumption against extraterritoriality is unlikely to operate so as to prevent such action.

16.56 It has been argued that a trend has emerged of the courts construing investigative powers so as to give them extraterritorial effect.[29] In the context of search warrants, we consider that there are a number of matters that would likely support the contention that Parliament did intend search warrant provisions to permit the search and seizure of remotely stored data.

16.57 First, it is necessary for search warrant provisions to apply in relation to remotely stored material in order for the provisions to deal comprehensively with the obtaining of relevant evidence.[30]

16.58 Secondly, it is necessary for search warrant provisions to apply to remotely stored data in order to give effect to the purpose of the statutory regimes.[31] To this end, there is a notable

---

26 D Bailey and L Norbury, *Bennion on Statutory Interpretation* (8th ed 2020) para 4.8.

27 *Masri v Consolidated Contractors Internation (UK) Ltd* [2009] UKHL 43, [2010] 1 AC 90 at [10]; *Bilta (UK) Ltd v Nazir (No 2)* [2015] UKSC 23, [2016] AC 1 at [212].

28 *R (KBR) v Director of the Serious Fraud Office* [2018] EWHC 2368 (Admin), [2019] QB 675 at [29].

29 Alex Davidson, "Extraterritoriality and statutory interpretation: the increasing reach of investigative powers" (2020) 1 *Public Law* 1.

30 D Bailey and L Norbury, *Bennion on Statutory Interpretation* (8th ed 2020) para 4.8.

31 D Bailey and L Norbury, *Bennion on Statutory Interpretation* (8th ed 2020) para 4.8.

shift from the courts towards a more purposive construction when investigative powers are concerned.[32]

16.59 Thirdly, it is necessary for search warrants to apply to remotely stored data in order to be effective, given the ease with which data may be stored remotely.[33] As stated in the context of investigative powers:

> Turning next to the policy considerations underpinning a finding of extraterritoriality, a common theme is the risk of rendering the provisions ineffective. It is scarcely credible, so the argument goes, that Parliament would not have intended the powers to be effective. Therefore, a finding of extraterritoriality prevents the powers from becoming toothless. In an increasingly interdependent world in which borders are routinely transcended, this argument must surely apply across the landscape of investigative powers.[34]

16.60 In conclusion, we consider that the arguments in favour of construing search and seizure provisions extraterritorially, where they relate to data stored abroad are, to the extent that such arguments are necessary at all, compelling. To conclude that investigators did not have the power to search for and seize data stored remotely unless expressly authorised would frustrate the aims of the provision conferring the powers, as suspects could easily choose to locate their data abroad purely for the purposes of evasion. It could also produce arbitrary results in searches, depending on where data was stored, or whether investigators or suspects knew the location of stored data. In our view, it is inconceivable that Parliament would have intended such a result; indeed, it appears that in many situations, Parliament considered the question, and chose to address it by referring to information that is "accessible from the premises"[35] or using deeming provisions.[36]

THE CIRCUMSTANCES IN WHICH THE SEARCH, SEIZURE AND PRODUCTION OF REMOTELY STORED DATA IS PERMISSIBLE UNDER INTERNATIONAL LAW

The relevance of international law

16.61 As well as a presumption against extraterritoriality, there is a related presumption that Parliament would not have chosen to confer powers on law enforcement agencies that are inconsistent with the comity of nations[37] and established rules of international law.[38] Therefore, powers of search, seizure and production cannot be exercised in ways that are in breach of international law.

---

32 Alex Davidson, "Extraterritoriality and statutory interpretation: the increasing reach of investigative powers" (2020) 1 *Public Law* 1 at 10.

33 D Bailey and L Norbury, *Bennion on Statutory Interpretation* (8th ed 2020) para 4.8.

34 Alex Davidson, "Extraterritoriality and statutory interpretation: the increasing reach of investigative powers" (2020) 1 *Public Law* 1 at 5.

35 Police and Criminal Evidence Act 1984, ss 19(4) and 20(1).

36 Higher Education and Research Act 2017, sch 5, para 9(2): references to items found on premises include (a) documents stored on computers or electronic storage devices on the premises; and (b) documents stored elsewhere which can be accessed by computers on the premises.

37 International comity refers to the respect a state shows to the sovereignty of other states.

38 D Bailey and L Norbury, *Bennion on Statutory Interpretation* (8th ed 2020) para 4.6. *Maxwell on the Interpretation of Statutes* (12th ed 1969) p 183.

16.62 In this section, we seek to identify the circumstances in which extraterritorial search, seizure and production is permissible under international law, in order to inform our recommendations regarding the search for and seizure of overseas material and ensure that any remodelled powers are compliant with international law.

16.63 In their consultation response, the Bar Council and the Criminal Bar Association ("CBA") denounced what they considered to be a generally risk-averse approach to obtaining access to overseas material. They argued that the significance of international law may have been overstated in the past. Further, because the relevant principles of international law are not clear in this area, there are risks with approaching reform from this starting point. Instead, they argued that the "true scope of the current law" should be ascertained first and whether it permits access to overseas material.

16.64 We understand the concern of the Bar Council and the CBA. In our view, any reform must be considered in light of recent state practice and international law principles, however unclear their application to remotely stored data might be. International law is binding. To legislate with indifference to it poses possible risks to international relations and may offend the sovereignty of other states.

Enforcement jurisdiction

16.65 The principle of international law that is engaged in this context is the principle of state sovereignty and non-intervention. In particular, international law prohibits the impermissible exercise of enforcement jurisdiction within the territory of another sovereign state. The Permanent Court of International Justice in the *Lotus* case described enforcement jurisdiction as follows:

> Now the first and foremost restriction imposed by international law upon a state is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another state. In this sense jurisdiction is certainly territorial; it cannot be exercised by a state outside its territory except by virtue of a permissive rule derived from international custom or from a convention.[39]

16.66 The editor of *Brownlie's Principles of Public International Law* summarises enforcement jurisdiction in this way:

> The governing principle of enforcement jurisdiction is that a state cannot take measures on the territory of another state by way of enforcement of its laws without the consent of the latter. Persons may not be arrested, a summons may not be served, police or tax investigations may not be mounted, orders for production of documents may not be executed, on the territory of another state, except under the terms of a treaty or other consent given.[40]

The circumstances in which the search, seizure and production of overseas electronic data is a permissible exercise of enforcement jurisdiction

16.67 We have concluded at paragraph 16.52 above that the use of powers of search, seizure and compulsory production exercised within a state's jurisdiction in respect of overseas

---

39 SS Lotus (France v Turkey), [1927] PCIL Reports, Series A No 10 at [45].

40 James Crawford, *Brownlie's Principles of Public International Law* (2019, 9th ed) p 462.

electronic data may arguably be classified as extraterritorial. We also concluded at paragraph 16.60 above that the presumption against a statute operating extraterritorially would in any event likely be rebutted even if such action were to be classified as extraterritorial. There remains a question-mark, however, over when such an exercise of enforcement jurisdiction is permissible under international law. As Cedric Ryngaert writes:

> The question has notably arisen whether, and under what circumstances, States can carry out remote searches with respect to information held on websites, computers, or servers *outside* their territory.[41]

16.68 This lack of clarity stems in part from the difficulty reconciling the *Lotus*-based principle of enforcement jurisdiction, which remains the cornerstone of the international law of jurisdiction, with the borderless nature of cyberspace.

16.69 In this section, we examine state practice and seek to set out the circumstances in which the search, seizure and production of overseas data has been deemed permissible under international law.

Mutual legal assistance

16.70 Law enforcement agencies may rely on mutual legal assistance (MLA) whereby the requested state will exercise powers in respect of the data in their territory.[42] This option will not be feasible where the location of data is unknowable. The Financial Conduct Authority ("FCA") also observed that, in the future, the location of service providers may be spread by competition, and new types of storage service providers will create new challenges that accelerate the ineffectiveness of traditional MLA processes and modern-day protocols.

Bilateral treaties

16.71 States may enter into bilateral treaties that permit the exercise of investigative powers in each other's jurisdictions. For example, on 7 October 2019 the UK and United States entered into an agreement that permits the UK to acquire, or obtain access to, electronic communications held or transmitted by US companies and permits the United States to acquire, or obtain access to, the content of communications held or transmitted by UK companies.[43]

16.72 The Crime (Overseas Production Orders) Act 2019 ("COPOA") grants law enforcement agencies and prosecuting authorities the power to apply for and obtain electronic communications content data directly from service providers (those who create, process, communicate or store electronic communications data) for the purposes of criminal investigations and prosecutions. Such orders may only be used when permitted under a designated international co-operation arrangement, that is, a relevant treaty between the UK and the country whose jurisdiction the data concerned is located.

16.73 The COPOA created a new overseas production order to obtain this type of electronic communications data which has extraterritorial effect, meaning that these orders are granted

---

41 Cedric Ryngaert, *Jurisdiction in International Law* (2nd ed 2015) p 81.

42 We discuss mutual legal assistance at paragraph 14.53 above.

43 The agreement ("Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime") was laid before Parliament under section 20(1)(a) of the Constitutional Reform and Governance Act 2010.

by UK courts exerting jurisdiction over evidence and persons outside the UK. This jurisdiction may only be asserted where a relevant treaty to which the UK is a party permits this to happen and which has been designated for the purposes of the COPOA. The UK-USA agreement mentioned in paragraph 16.71 above has been designated as a relevant treaty under the COPOA.[44] This means that overseas production orders can be made in respect of data governed by the laws of the United States.

16.74 In its consultation responses, the Magistrates Association stated that it appeared that new provisions may be necessary to cover extra-territorial searches, beyond existing search warrants. Due to the complex issues involved, it was said to be likely that any new provisions would involve cooperation with other countries, and therefore may require international agreements.

Consent

16.75 The search and seizure of remotely stored data is permissible where the state in whose territory the data is held allows the search or the information holder gives its consent.[45] This of course assumes that it is known where electronic data is stored. However, as we have explained, the location of electronic data may be unknowable.

Publicly accessible data

16.76 The search and seizure of remotely stored data will not be contested where the information is publicly accessible.[46] In such cases, however, an investigator would not need to obtain a search warrant as the evidence would be obtainable by other means.

Unknowable location

16.77 Where the location of overseas data is unknowable, state practice suggests that the search of and seizure of such data would not offend against the territorial sovereignty of another state. In December 2016, the United States amended Rule 41 of the Federal Rules of Criminal Procedure to permit the search (from anywhere) of remotely stored data, wherever situated, where either (1) the physical location of the data is concealed through technological means; or (2) protected computers in five or more districts are damaged.[47] The Government must make "reasonable efforts" to notify the person whose remotely stored data has been searched.[48] The US Department of Justice advised that such warrants would have "no extraterritorial effect".[49]

16.78 The New Zealand Law Commission and Ministry of Justice in their joint review of the country's Search and Surveillance Act 2012 also adopted the view that the search and

---

44 The Overseas Production Orders and Requests for Interception (Designation of Agreement) Regulations 2020 (SI 2000 No 38), art 2(a).

45 Convention on Cybercrime (Budapest, 23 November 2001) ETS No 185, art 32(b); Cedric Ryngaert, *Jurisdiction in International Law* (2nd ed 2015) p 81.

46 Convention on Cybercrime (Budapest, 23 November 2001) ETS No 185, art 32(a).

47 Federal Rules of Criminal Procedure (United States), r 41(b)(6).

48 Federal Rules of Criminal Procedure (United States), r 41(f)(1)(C).

49 United States Department of Justice "Mythili Raman Letter to Advisory Committee on the Criminal Rules" (18 September 2013) at 5, available at <https://www.justsecurity.org/wp-content/uploads/2014/09/Raman-letter-to-committee-.pdf>.

seizure of remotely stored data in an unknowable location is permissible under international law:

> If an enforcement agency cannot determine where the data is located, it is legitimate for it to conclude that the location is unknowable. In those circumstances, we consider that the Act should enable enforcement officers to access the data pursuant to a search warrant. In this respect, we endorse the Law Commission's conclusion in 2007 that, while principles of territorial sovereignty should be recognised to the maximum extent possible, those principles are impossible to observe where the identity of the relevant jurisdiction is unknown. This is the rationale that underlies the current remote access provisions in the Act and we are not convinced that there is a need to reverse that policy. From an international perspective, that rationale is the most prevalent justification for transborder access to data. New Zealand therefore is unlikely to raise any international relations concerns by continuing to adopt this stance.[50]

Sufficient or substantial jurisdictional connection

16.79 Another circumstance in which states may consider it permissible to search, seize or require the production of overseas data is where there is, in some form or another, a sufficient or substantial connection between certain subject-matter (persons or property) and their own jurisdiction.

The adoption of the test in this jurisdiction

16.80 In *R (KBR)*, the Divisional Court held that the extraterritorial ambit of section 2(3) of the Criminal Justice Act 1987 extended to a foreign company in respect of documents held outside the jurisdiction of the United Kingdom, provided that there was a sufficient connection between the company and the jurisdiction.[51] The Court also provided a non-exhaustive list of factors as to when a sufficient connection may or may not exist.[52] In reaching the above conclusion, the Divisional Court utilised the touchstone described by Lord Mance in *Masri*[53] of whether "eyebrows might be raised" at the notion that Parliament had conferred the extraterritorial jurisdiction in issue, holding that they would not.[54] The Divisional Court also regarded mutual legal assistance procedures as an additional power and not one of which law enforcement agencies were obliged to avail themselves.[55] It was pointed out that mutual legal assistance channels carry the risk of delay and of requests being ignored.[56]

16.81 A sufficient connection test has been adopted in other circumstances. In the Supreme Court case of *Perry v SOCA*, Hughes LJ, as he then was, stated that, if it were possible as a matter of construction, he would have wished to construe Part 5 of the Proceeds of Crime

---

50 New Zealand Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012 / Ko te Arotake i te Search and Surveillance Act 2012*, NZLC R141 (2017) paras 12.97 to 12.98.

51 *R (KBR) v Director of the Serious Fraud Office* [2018] EWHC 2368 (Admin), [2019] QB 675 at [71].

52 *R (KBR) v Director of the Serious Fraud Office* [2018] EWHC 2368 (Admin), [2019] QB 675 at [80] to [81].

53 *Masri v Consolidated Contractors International (UK) Ltd* [2009] UKHL 43, [2010] 1 AC 90 at [24].

54 *R (KBR) v Director of the Serious Fraud Office* [2018] EWHC 2368 (Admin), [2019] QB 675 at [72]. The same test was utilised by the Court of Appeal in *R (on the application of Jimenez) v First Tier Tribunal (Tax Chamber)* [2019] EWCA Civ 51, [2019] 1 WLR 2956 at [49].

55 *R (KBR) v Director of the Serious Fraud Office* [2018] EWHC 2368 (Admin), [2019] QB 675 at [93].

56 *R (KBR) v Director of the Serious Fraud Office* [2018] EWHC 2368 (Admin), [2019] QB 675 at [94].

Act 2002 ("POCA") to admit of limited extraterritorial effect where there was a "sufficient jurisdictional connection" between a part of the UK and the criminal proceeds.[57] He considered that such jurisdictional links contemplated by the then in force section 286 of POCA in respect of civil recovery orders would not be exorbitant, nor would it offend the sovereignty of other states.[58] The links envisaged included the crime being committed within the jurisdiction and the offender or holder of the property being domiciled, resident or present in the jurisdiction.[59]

16.82 In *In re Paramount Airways Ltd*, Sir Donald Nicholls V-C formulated a "sufficient connection" test for the purpose of determining whether an originating application under section 238 of the Insolvency Act 1986, claiming payment of moneys transferred, could be served on a foreign entity.[60] Accordingly, the court had jurisdiction under section 238 to make an order against a person resident abroad with no business in the jurisdiction provided that it was satisfied that the defendant had a sufficient connection with England for it to be just and proper to make the order despite the foreign element.[61]

16.83 A flexible approach to jurisdiction in the context of the commission of offences has also been adopted by the Court of Appeal of England and Wales. In *Smith (No 4)*, the Court of Appeal held that a crime may be regarded as committed within the jurisdiction if "a substantial part of the offence" was committed in England and Wales, even if the last act of the offence was not committed in England and Wales.[62] This approach has been consistently endorsed or applied by the Court of Appeal.[63] The Whitehall Prosecutors' Group submitted in its consultation response that the broad approach taken to jurisdiction and international comity adopted in respect of offences also needs to be adopted in respect of the powers used to investigate such offences.

16.84 The Investigatory Powers Act 2016 ("IPA"), provides the ability for law enforcement agencies to compel any service provider offering telecommunications services in the UK, including overseas service providers, to provide certain electronic communications sought by warrant, even if the data is stored or controlled abroad. The IPA covers any telecommunications operator which provides services to persons within the UK,[64] thereby establishing a necessary jurisdictional connection. A telecommunications operator can be required to disclose electronic communications without regard to where the communications are stored or processed, so long as it is reasonably practicable for the operator to provide assistance in obtaining the required communication.[65] The UK has therefore enacted powers for obtaining electronic communications from service providers providing services within the UK, irrespective of the location at which the data is stored.

---

57 *Serious Organised Crime Agency v Perry* [2012] UKSC 35, [2013] 1 AC 182 at [156].

58 *Serious Organised Crime Agency v Perry* [2012] UKSC 35, [2013] 1 AC 182 at [157].

59 *Serious Organised Crime Agency v Perry* [2012] UKSC 35, [2013] 1 AC 182 at [157]. Proceeds of Crime Act 2002, s 286(3). See also Crime and Courts Act 2013, s 48.

60 *In re Paramount Airways Ltd* [1993] Ch 223, 239 to 240.

61 *In re Paramount Airways Ltd* [1993] Ch 223, 239 to 240.

62 *R v Smith (No 4)* [2004] EWCA Crim 631; [2004] 3 WLR 229 at [55].

63 See *R v Sheppard* [2010] EWCA Crim 65; [2010] 1 WLR 2779; *R v Rogers* [2014] EWCA Crim 1680; [2015] 1 WLR 1017 at [54]; *R v AIL* [2016] EWCA Crim 2, [2016] QB 763; and *Burns* [2017] EWCA Crim 1466.

64 Investigatory Powers Act 2016, s 261(10).

65 Investigatory Powers Act 2016, ss 41 to 43.

The adoption of the test at a supranational and international level

16.85 There are examples of jurisdictional tests that centre on the connection that overseas data has to the jurisdiction and not its location at a supranational and international level. The European Production Order would permit a judicial authority in a Member State to request the production or preservation of electronic evidence directly from a service provider offering services in the European Union and established or represented in another Member State.[66] The order would apply to service providers that have a "substantial connection" to the Member States concerned.[67] Cedric Ryngaert has observed that:

> With this proposal, the European Commission moves away from territoriality as the determinative factor for enforcement jurisdiction in cyberspace. Thereby it could possibly set an international precedent to modernize international law in the area of transborder access to e-evidence.[68]

16.86 In a similar vein, the Cybercrime Convention Committee's Transborder Group has proposed extending the circumstances in which it is permissible to search for and seize overseas data under the Cybercrime Convention by using the "power of disposal" or the "person in possession or control" as a connecting legal factor:

> In "loss of (knowledge) of location" situations … it is problematic to rely on the principle of territoriality (defined by the location of the data or computer system) to determine the jurisdiction to enforce a search or seizure of electronic evidence. It has been argued, therefore, that an approach beyond territoriality was required. A connecting legal factor that provides an alternative to territoriality could be the "power of disposal" or "the person in possession or control". Even if the location of data cannot be clearly determined, data can be connected to a person having the power to "alter, delete, suppress or to render unusable as well as the right to exclude others from access and any usage whatsoever". Specific conditions and safeguards would need to be established.[69]

Our observations

16.87 What emerges from these developments is an acknowledgement that the location of electronic data cannot be determinative for the purposes of setting the permissible boundaries of enforcement jurisdiction. Strict adherence to the *Lotus*-based principle of enforcement jurisdiction is neither possible nor desirable when electronic data is sought.

16.88 States have therefore developed new incarnations of the territoriality principle based on sufficient or substantial connections with their jurisdiction. On the one hand, it may be said that such approaches to enforcement jurisdiction represent a legitimate modernisation of international law principles. On the other hand, it may be said that such approaches involve

---

66 European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, COM (2018) 225.

67 European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, COM (2018) 225, art 3.

68 Cedric Ryngaert, "The European Production Order – Tackling the Problem of Enforcement Jurisdiction and Extraterritoriality in Cyberspace" (18 July 2018) Renforce Blog < http://blog.renforce.eu/index.php/nl/2018/07/18/the-european-production-order-tackling-the-problem-of-enforcement-jurisdiction-and-extraterritoriality-in-cyberspace/>.

69 Cybercrime Convention Committee, *Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for consideration by the T-CY* (September 2016) para 144.

a tenuous assertion of territorial connection, which leads to exorbitant jurisdiction and offends the sovereignty of other states.

16.89 Consultation responses from law enforcement agencies regarded the search and seizure of remotely stored data as unlikely to offend the concept of international comity owing to the jurisdictional connection involved. The Whitehall Prosecutors' Group argued that the presence of the account holder, another person with control of the account, a person with the right to access the account, or a data owner within the jurisdiction gives sufficient standing for the state to be justified in authorising its agents to conduct the search.

16.90 Along similar lines, HMRC considered that, insofar as such a search is extraterritorial, the power to search for remotely stored data is a minimal, if not *de minimis*, form of extraterritorial search and not sufficient to offend against international comity when the cloud account holder or data owner is physically present within the jurisdiction.

Other circumstances in which the search, seizure and production of overseas data is permissible

16.91 In 2016, the Cybercrime Convention Committee's cloud evidence group made a series of recommendations for consideration by the Cybercrime Convention Committee when negotiating a protocol to the Cybercrime Convention to address the issues raised by cloud computing.[70] These included the consideration of the following proposals made by the Cybercrime Convention Committee's transborder group that would extend the circumstances in which it would be permissible to search for and seize overseas data:[71]

(1) Permitting transborder access to electronic data without consent but with lawfully obtained credentials. The report states that the other country would need to be notified before, during or after the event.

(2) Permitting transborder access to electronic data without consent in good faith (for example where the transborder access occurs by mistake or by accident) or in exigent or other circumstance (for example where the access is necessary to prevent imminent danger, physical harm, the escape of a suspect or the destruction of evidence). The report explains that, again, the other country would need to be notified.

(3) As discussed at paragraph 16.86 above, in loss of data cases, using the "power of disposal" or the "person in possession or control" as the connecting legal factor.

Notification requirement

16.92 As explained at paragraph 14.31 above, there are three potential relevant parties when remotely stored electronic data is concerned: (1) the individual or user who generates the electronic data; (2) the service provider who manages, processes or stores the electronic data; and (3) the state on whose territory the storage facility that stores the electronic data is located.

---

70 Cybercrime Convention Committee, *Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for consideration by the T-CY* (September 2016).

71 Cybercrime Convention Committee, *Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for consideration by the T-CY* (September 2016) para 144.

16.93 It seems that there is no basis in international law for a specific obligation to notify a state that powers of search and seizure have been exercised in respect of data in their territory.[72] Notification to a state may be viewed as beneficial in terms of international relations. This again assumes that the location of the data is knowable. Notifying an individual may be considered an appropriate safeguard, particularly where a search warrant is executed remotely from a target premises. However, where a search warrant is executed on physical premises, the action taken will not be covert, and so in our view notification would serve little purpose. We also recommend in the next chapter that an investigator be required to provide, in as much detail as practicable, details of what action was taken in respect of electronic devices on premises within a reasonable time from a person with an interest in the electronic material making a request for it.

Concluding observations

16.94 The circumstances in which the search, seizure and production of overseas data is permissible under international law is unclear. The Cybercrime Convention, while setting out the limited circumstances in which such activity is permissible, provides that other situations are neither authorised nor precluded.[73] The door is, in effect, left open. Some domestic courts and legislators have approved of the search, seizure and production of overseas data in other circumstances, holding that it is in keeping with international law.[74] At the same time, concerns clearly remain in the international community. The debate has been summarised by one academic as follows:

> Despite there being views on transborder access that argue the activity to be generally in line with territorial sovereignty, neither States nor international organisations have univocally approved such access without any additional legal grounds such as the consent of the other State, nor is the legality of transborder access widely supported by scholars. In fact, according to a recent UN study, around two-thirds of countries in all regions of the world perceived foreign law enforcement's access to other State's computer systems or data as impermissible, even if it may occur in practice either with or without the knowledge of investigators.[75]

16.95 The lack of international consensus has led to a concern expressed over states unilaterally asserting enforcement jurisdiction:

> In the absence of an agreed upon international framework with safeguards, more and more countries will take unilateral action and extend law enforcement powers to remote

---

72 Anna-Maria Osula and Mark Zoetekouw, "The Notification Requirement in Transborder Remote Search and Seizure: Domestic and International Law Perspectives" (2017) 11(1) *Masaryk University Journal of Law and Technology* 103 at 108 to 109. See also Council of Europe, *Explanatory Report to the Convention on Cybercrime*, para 204.

73 Convention on Cybercrime (Budapest, 23 November 2001) ETS No 185, art 39(3).

74 Cedric Ryngaert, *Jurisdiction in International Law* (2nd ed 2015) pp 81 to 82. For example, *R (KBR) v Director of the Serious Fraud Office* [2018] EWHC 2368 (Admin), [2019] QB 675.

75 Anna-Maria Osula, "Transborder access and territorial sovereignty" (2015) 31 *The Computer Law and Security Report* 719 at 725.

trans-border searches either formally or informally with unclear safeguards. Such unilateral or rogue assertions of jurisdiction will not be a satisfactory solution.[76]

16.96 Access to overseas data is an international issue which clearly requires a long-term solution. At the time of writing, the second protocol to the Cybercrime Convention is still under negotiation, which aims to address issues of jurisdiction.[77] Given the need for a state to protect its citizens by investigating, detecting and prosecuting crime, we consider that so-called unilateral assertions of jurisdiction are inevitable and required.

16.97 Remotely stored data is accessed by law enforcement agencies in England and Wales when executing a search warrant where necessary for the legitimate aim of detecting, investigating and prosecuting crime. Strict adherence to the *Lotus*-based principle of enforcement jurisdiction in the context of cyberspace does not produce rational results, a conclusion widely supported by developments at the national, supranational and international levels. As has been stated:

> It is submitted that the sui generis nature of electronic data, the location of which may be unstable or unknown, justifies a more nuanced approach to traditional international law concepts of jurisdiction and territoriality. … This suggests a need to recalibrate focus from the location of the data to matters such as who owns or controls the data, where it has been created or accessed and the extent to which it is accessible from within the jurisdiction.[78]

16.98 The reasoning behind these conclusions also appears in those consultation responses which discussed the extraterritoriality of search, seizure and production powers. These responses highlighted the meaninglessness of describing data as having a location and the otherwise strong jurisdictional connection that may exist. We therefore endorse the UK Government's view that:

> The global nature of the modern communications environment renders laws basing access to data purely on location ineffective and likely to lead to unintended and perverse outcomes. Further, for a nation's law enforcement functions to operate effectively, it requires access in limited and regulated circumstances to the electronic communications relating to those in its jurisdiction, wherever those communications are stored.[79]

16.99 The key question for us in this chapter is what those "limited and regulated" circumstances ought to be in the context of search warrants. To this end, given the nebulous state of

---

76 See Cybercrime Convention Committee, *Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for consideration by the T-CY* (September 2016) at [143].

77 Cybercrime Convention Committee, *Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime* (June 2017); and Cybercrime Convention Committee, *Preparation of the 2nd Additional Protocol to the Budapest Convention on Cybercrime State of play* (June 2019). Only some draft provisions of the second additional protocol have been published, and not those relating to the issues that we have been discussing.

78 Alex Davidson, "Extraterritoriality and statutory interpretation: the increasing reach of investigative powers" (2020) 1 *Public Law* 1 at 5.

79 United States v Microsoft Corporation, *Brief of the Government of the United Kingdom of Great Britain and Northern Ireland*. Available at:

https://www.supremecourt.gov/DocketPDF/17/17-2/23693/20171213140104710_17-2%20-%20Government%20of%20the%20United%20Kingdom%20of%20Great%20Britain%20and%20Northern%20Ireland.pdf

international law in this area, the question best asked is not what conduct is permissible under international law, to which there is no clear answer, but whether the desired policy (for example, a sufficient connection test) is likely to offend state sovereignty and international comity.

16.100 Drawing the threads from our discussion together, we cannot see that another state would have a grievance where law enforcement agencies, executing a search warrant in England and Wales, searched for and seized data intentionally or evasively stored in their territory by reason of a suspect using remote storage services whose storage facilities are located in the territory of the state concerned. In such circumstances, we consider that any infringement on the sovereignty of another state would be *de minimis* and unlikely to offend state sovereignty and international comity.

THE SEARCH OF PREMISES FOR AND COPYING OF REMOTELY STORED DATA

The current law

16.101 The circumstances in which law enforcement agencies can search for and copy remotely stored data from an electronic device on premises is unclear. We set out the current law as best we can here.

Satisfying the statutory access conditions

16.102 There are a host of variables that may be in play when relevant data is not stored on an electronic device on premises but remotely stored and accessible from an electronic device on premises. Depending on what intelligence a law enforcement agency has, there may be differing states of knowledge as to what data is on, or accessible from, specific premises. An investigator may suspect, believe or know that relevant data is:

(1) both stored on an electronic device and accessible from an electronic device on premises;

(2) either stored exclusively on an electronic device or accessible from an electronic device on premises; or

(3) exclusively accessible from, and not stored on, an electronic device on premises.

16.103 The requirement under section 8 of and schedule 1 to PACE that there are reasonable grounds for believing that relevant material is “on” premises is unlikely to be met where an investigator seeks relevant evidence that is likely to be stored remotely. This is because remotely stored material is not “on” premises but rather accessible from premises, whether it is stored overseas or not.

16.104 In our view, this problem cannot be overcome by relying on the single item theory as the theory is predicated on the relevant electronic data being stored *on* the electronic device, which causes an electronic device to become relevant evidence. There is no case law on whether an entire electronic device can be treated as relevant where the data sought is not stored on an electronic device but accessible from it.

16.105 As a result, the statutory access conditions for the issue of a search warrant could only be met in scenarios (1) and (2) at paragraph 16.102 above. A search warrant could not be sought in scenario (3) as there is no relevant evidence “on” premises.

16.106 In practice, investigators do apply for search warrants in respect of remotely stored data. For example, we have seen a PACE warrant that authorised the investigator to search for:

> Any material recorded on servers accessible from the subject premises.

Searching for and copying remotely stored data when on premises

16.107 At paragraph 15.174 above, we reach the view that it is ambiguous under the majority of search warrant regimes whether electronic devices can be searched on-site when executing a search warrant under the authority of a warrant.

16.108 It follows that it is equally, if not more, ambiguous whether investigators can conduct a search of an electronic device on premises for remotely stored data. More specifically it is ambiguous whether, when executing a search warrant, an investigator can conduct a search of an electronic device on premises in order to identify an online account (eg a Dropbox or Gmail account), access or connect to the account, and copy relevant data to use as evidence. Again, we consider it more likely than not that a search warrant does not permit an investigator to search an electronic device for remotely stored data.

16.109 In scenario (1) at paragraph 16.102 above, only the relevant data stored "on" an electronic device would meet the statutory access conditions. A warrant could therefore specify either an electronic device on which the data is stored or the locally stored data. If the warrant was drafted in terms of an electronic device, the device itself could be seized or locally stored data copied. If the warrant was drafted in terms of information, the electronic device would have to be seized under the CJPA provisions, unless consent was given to search the device. In neither style of drafting could remotely stored data be copied.

16.110 In scenario (2) at paragraph 16.102 above, so long as reasonable grounds for believing that the relevant electronic data is "on" a device on the premises, a warrant could again specify the whole electronic device or the information sought on the device. If it then transpired that the relevant electronic data was stored exclusively remotely, the electronic device could not be seized either under the authority of the warrant or under the CJPA provisions, as there would be no electronic data that the investigator was entitled to seize.

16.111 Where an investigator is on premises under the authority of a search warrant and relevant electronic data is held remotely, the investigator still has a host of options. First, the investigator could seek the consent of the occupier to search electronic devices for and copy remotely stored electronic data. We were informed by one agency that consent to access remotely stored data is granted in less than half of the cases in which it is requested.

16.112 Secondly, the investigator can require the production of the remotely stored data from an occupier. In Chapter 18, we explain our conclusions that sections 19(4) and 20(1) of PACE can be used in this way.

16.113 Thirdly, if the investigator manages to identify where relevant electronic data is remotely stored, they may request mutual legal assistance, typically in the form of production and preservation orders. If the remotely stored electronic data is managed, processed or stored by a person or company located in the United States, an investigator may apply for an overseas production order.[80]

---

[80] See paragraphs 16.71 to 16.73 above.

The consultation paper

16.114 As discussed in the sections above, we invited consultees' views on whether law enforcement agencies require powers of extraterritorial search, seizure and production under warrant.[81] We also invited consultees' views on whether reform to PACE is required to permit any such investigative measures.[82]

16.115 We pointed out at paragraph 10.75 of our consultation paper that the requirement under section 8 of and schedule 1 to PACE that material be "on" premises is unlikely to be met in respect of remotely stored data. At paragraph 10.76 of our consultation paper, we then set out two reasons why this problem may not be an acute one in practice.

16.116 The first reason was that sections 19 and 20 of PACE may allow access to remotely stored data when an investigator is on premises. We set out the reasons for this at paragraphs 18.46 to 18.56 below. However, this avenue would still require a lawful power to enter premises in the first place.

16.117 The second reason is that relevant remotely stored evidence may be *on* the premises by virtue of the presence of "trace data".[83] However, there may only be a small amount of trace data stored on an electronic device. There may also be circumstances in which there are no reasonable grounds for believing that there is trace data stored on an electronic device on premises. Further, it would be undesirable for the ability for law enforcement agencies to obtain relevant remotely stored data to turn on whether there are reasonable grounds for believing that there is trace data stored on an electronic device on premises.

Consultation responses

16.118 Sixteen consultees[84] made comments regarding the search of devices for and copying of remotely stored material.

The current law

16.119 Interestingly, Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate stated that, following consultation with the Investigatory Powers Commissioner's Office, they already had sufficient powers under the current law to acquire data stored remotely by a third-party service provider. They considered that section 19 of PACE, read alongside section 6(1)(c)(ii) of IPA, permitted them to:

(1) conduct a live examination of a seized device while on premises, or at a police station, for data stored remotely in the cloud;

(2) use subterfuge to access cloud accounts from a seized device; or

---

81 Consultation Question 55.

82 Consultation Question 55.

83 See paragraph 14.23 above.

84 National Crime Agency; Metropolitan Police Service; Dijen Basu QC; Financial Conduct Authority; Competition and Markets Authority; Bar Council and the Criminal Bar Association; Whitehall Prosecutors' Group; Staffordshire Police; Guardian News and Media; HM Revenue and Customs; Professor Richard Stone; Magistrates Association; The Law Society; Serious Fraud Office; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate.

(3) modify the data of a cloud storage account (such as resetting the password). Separately, Dijen Basu QC also considered that interrogating servers using seized devices could potentially be authorised (without the need for a warrant) pursuant to property interference authorisation under section 93 of the Police Act 1997.

Problems with the current law

The restrictive nature of the statutory access conditions

16.120 Consultees agreed that the restrictive nature of the statutory access condition, that material be "on" premises, meant that criminal investigations might be inhibited and crucial evidence lost.[85] For example, we were informed by one law enforcement agency that it would be difficult if not impossible to obtain a search warrant where a person makes indecent images of children while they are physically out of the country, uploads those images to an unknown remote storage facility and then re-enters this jurisdiction. In such a case, the indecent images would be accessible from an internet enabled electronic device, but the images would not be "on" premises in this jurisdiction.

16.121 The point was also made during our pre-consultation discussions that there are devices, such as a Google Chromebook, where virtually all data is stored remotely on the company's servers and none is saved on the device itself.[86] It was also said that, as time goes by, sophisticated criminals will see the benefit of forms of remote storage which enable instant remote destruction if necessary.[87] These issues all pose challenges to the way in which the statutory access condition for the grant of a search warrant is currently drafted.

The need for powers to search for and copy remotely stored data

16.122 Several law enforcement agencies highlighted their need to have clear powers to obtain data stored remotely in order to investigate criminality effectively.[88] Staffordshire Police explained that the way in which digital forensics operates means that electronic devices will provide more evidence while on the premises. We were informed that not having the ability to access remotely stored data pursuant to a search warrant would have disastrous consequences in child abuse investigations in particular, given that evidence regarding such offences is typically stored remotely.

16.123 A shared view emerged from consultation responses of the need to ensure that the law keeps up with technological developments.[89] At a law enforcement agency roundtable, we were informed that law enforcement agencies are encountering more and more data stored in the cloud. In their consultation response, HMRC stated that the law requires greater detail so that investigators can be more confident in the actions they can take to gain access to remotely stored data. The SFO noted the uncertainty as to whether remotely held material may be seized under warrant. They argued that it should be put beyond doubt precisely when remotely stored material may be seized.

---

85 National Crime Agency; Metropolitan Police Service; Dijen Basu QC.

86 Jonathan Hall QC.

87 Dijen Basu QC.

88 Financial Conduct Authority; Competition and Markets Authority; National Crime Agency; HM Revenue and Customs; Serious Fraud Office; Whitehall Prosecutors' Group; Staffordshire Police.

89 Metropolitan Police Service; Financial Conduct Authority; HM Revenue and Customs.

16.124 It was not only law enforcement agencies that held this view. The collective view expressed at a roundtable organised with the senior judiciary was also that investigative powers must be fit for the 21st century. Professor Richard Stone stated that it would be advisable for law enforcement agencies to be given specific powers relating to material held outside the jurisdiction. The Magistrates Association supported proposals to ensure agencies have the flexibility to investigate crime in the digital age while ensuring individuals' rights are protected. The Law Society expressed the view that it was perverse that information, accessible through a device controlled by a suspect, cannot be looked at by law enforcement where it has been purposefully stored abroad to frustrate action against the suspect.

16.125 Concern was also raised by the National Crime Agency and SFO regarding potential liability under the Computer Misuse Act 1990 ("CMA 1990"). It was said to be unclear whether section 10 of the CMA 1990 provides sufficient protection in this respect. Dijen Basu QC also observed that, potentially, interrogating servers using seized devices would amount to interception for the purposes of IPA.

16.126 Law enforcement agencies indicated that the following statutes required amendment to make clear that they permitted the access and copying of remotely stored data: section 8 of and schedule 1 to PACE; section 352 of POCA; section 2(4) of the CJA; and part 2 of the Criminal Justice and Police Act 2001 ("CJPA"). The SFO stated that they would want such powers to be exercisable by SFO staff and digital forensics specialists, not simply constables who execute their warrants.

The practicability of other methods to obtain remotely stored data

16.127 Consultees also considered the practicability of other methods of accessing remotely stored data. A point made that we have already explained at paragraph 14.30 above is that law enforcement agencies may not know ahead of executing a search warrant whether electronic data is stored remotely and, if so, the precise location of the data. This makes mutual legal assistance and production orders of limited use. For example, the point was made that the recently enacted COPOA will not be a solution for the routine access that investigators will need.[90]

16.128 Concern was also raised that the data which is provided by a third-party provider will not, strictly speaking, be the same data that is stored on the actual device on premises.[91] This is problematic for reasons of provenance, continuity and forensic integrity. [92] Therefore, powers of production are no substitute for imaging by digital forensics specialists.

16.129 As for letters of request and mutual legal assistance, it was argued that it was unacceptable to have to resort to these avenues where data is stored by a person within the jurisdiction.[93] It was pointed out that certain communication service providers may take six months to respond or delete the data, thereby losing evidence.[94] Further, such requests may be impossible to draft as the data comprising the file sought could be scattered across multiple

---

90 Bar Council and the Criminal Bar Association.

91 Metropolitan Police Service.

92 Serious Fraud Office.

93 Whitehall Prosecutors' Group.

94 Staffordshire Police.

jurisdictions and move jurisdictions many times a day.[95] The point was also made at a roundtable that we held with law enforcement agencies that investigators cannot rely solely on mutual legal assistance as smart criminals will store their data on servers in hostile countries.

Suggestions for reform

16.130 We set out here the suggestions made by consultees for reform. Two specific suggestions were made by consultees which would involve the creation of new search and seizure powers that are not linked to the search of premises. The first suggestion was the introduction of a warrant to conduct a search of electronic devices not connected to premises. The second suggestion was a warrant to search online accounts remotely without entering another person's premises. We regarded these two suggestions as falling outside of our terms of reference. We therefore discuss them in Chapter 18, which assesses the desirability of a wider review of the acquisition and treatment of electronic material in criminal investigations.

16.131 The suggestions discussed in this section are those which focus on the search of premises for remotely stored data. We discuss suggestions made regarding ancillary powers (the compelling of passwords and modification of data) in the sections of this chapter that follow.

16.132 The Metropolitan Police Service suggested that one way to remedy this problem would be to widen the statutory access conditions to cover electronic material that is accessible from a device kept on the premises. Dijen Basu QC also suggested that the simplest method would be to permit warrants to cover electronic data accessible from the premises, including by means of equipment to be found on those premises, wherever in the world that information was stored. He argued that, done this way, the warrant would remain, conceptually, a search warrant, but one which recognised the reality of increasing cloud-based storage without local backup.

16.133 The CPS acknowledged the potentially tenuous link between remotely stored data and the premises to be searched, given that the data can theoretically be accessed from any internet enabled electronic device irrespective or where it is located. Therefore, the CPS suggested an amendment to the access conditions of section 8 and schedule 1 PACE designed to extend existing powers and founded on a link between the remotely stored data and the premises:

(1) the starting point is that a warrant confirms the judicial determination that there are reasonable grounds to believe that an indictable offence has been committed, that there is evidence which is of substantial value to the investigation, and that a search may take place in the jurisdiction for that evidence;

(2) where material is stored remotely, it may be the equivalent of material which would be found in the course of that search but for the fact that it has been stored off the premises; or

(3) alternatively, the search may discover a device on the premises which on analysis indicates that the person using the device accessed material stored off the premises.

---

[95] Whitehall Prosecutors' Group; Financial Conduct Authority.

16.134 With the above in mind, the CPS suggested that references to “material on premises” in section 8(1)(b) and schedule 1 paragraph 2(a)(ii) of PACE should include electronic data which a constable has reasonable grounds for believing:

(1) would have been found on a device found on the premises but has been stored remotely from the premises; or

(2) has been placed in a remote electronic location by a person within the premises, or accessed from the premises.

The first condition would seem to require consideration of a hypothetical: but for the availability of remote storage, would the data have been stored locally on a device found on the premises? Electronic data would then be deemed to be stored within England or Wales notwithstanding any claim that it is or might be outside England or Wales.

16.135 The National Crime Agency advocated a ‘requirements-based approach’ to reform. Accordingly, the NCA identified as a key legal requirement, once premises were entered and devices were located, the power to:

(1) electronically search through powered-on digital devices in the named premises including identifying any cloud computing connections; and

(2) connect from the premises to an identified cloud profile (the data of which could be located anywhere in the world) to download the connected data for evidential purposes (using digital forensic best practices), including during the course of an investigation if a cloud account is identified.

16.136 The Whitehall Prosecutors’ Group argued that the age of remote storage of data, and cloud computing, required revision of the scope of a domestic search warrant to authorise an officer to access data belonging to the occupier of the premises (and the suspects if not members of this class of person) when stored remotely. It was suggested that a search warrant should be capable of authorising an officer executing the warrant to access a remote storage account and seize (ie copy) data where:

(1) a remote storage account has been identified as belonging to an occupier or suspect, or as containing the occupier or suspect’s data; and

(2) the occupier or suspect is present in the jurisdiction.

16.137 It was suggested that the warrant should be able to specify:

(1) both known cloud accounts and cloud accounts which cannot be identified in advance of the search; and

(2) particular file types, or all files responding to a certain search term.

16.138 Therefore, a search warrant might authorise the search of a particular remote storage account (say the cloud account in the name of jane.smith@address.com) for all invoices, contracts dated between 1 January 2018 and 31 December 2019 or any other file responding to a certain search term.

16.139 HMRC indicated that they wanted the ability to seek an e-warrant to search for and seize remotely stored data belonging to the occupier of the premises using search terms applied

to the cloud. In short, an “e-warrant” should be available that treats cloud accounts and other online storage facilities as “e-premises” which can be specified on the warrant (unless it is an “all e-premises” warrant).

16.140 The CPS expressed some caution about an e-premises regime that would treat remote storage accounts as premises which are capable of entry and search. First, entry onto premises outside of the jurisdiction would connote extraterritorial activity. Secondly, it was said that premises are a physical location which a human being should enjoy peacefully, unless a judicially-authorised exception to this is made. Accordingly, the place where electronic data is stored is not a premises. The Whitehall Prosecutors’ Group also preferred to treat a remote storage account as an “entity” rather than a premises, as premises may connote a physical place which a human ought peacefully to enjoy.

16.141 The Whitehall Prosecutors’ Group also considered that the drafting of the CJPA should also be updated to put beyond doubt the application of the seize and sift provisions in cases of cloud-based computing where there is remotely stored data.

Analysis

16.142 We begin by considering whether remotely stored material can be accessed lawfully through section 19 of PACE. This matter can be dealt with fairly swiftly. Section 19 of PACE is not a power of search. Therefore, the provision cannot be relied on as providing a freestanding power to permit the live examination of remotely stored data on premises. On this reading, a person does not have “lawful authority” to carry out an interception under section 6(1)(c)(ii) of IPA as it will not be in the exercise of a statutory power. Whether section 19 of PACE permits access to remotely stored data when blended with other statutory powers is of course another matter. We discuss sections 19 and 20 of PACE in more detail in Chapter 18.

16.143 Notwithstanding that issue, we are firmly of the view that law enforcement agencies require the power to enter premises where electronic data is held remotely, search electronic devices for, and copy, remotely stored data for the following cumulative reasons.

16.144 First, we are satisfied that, without such powers, criminal investigations would be easily frustrated owing to the ubiquity of cloud computing and the ease with which electronic data can be stored remotely. The investigation and prosecution of some of the most serious crimes – including terrorism, fraud and child abuse – will rely on the capability of law enforcement agencies to acquire remotely stored data. But it is not just these crimes that require law enforcement agencies to be able to obtain remotely stored data: evidence of the commission of the entire spectrum of criminal offences may exist in electronic form and be stored remotely.

16.145 Secondly, it may not be known, and unknowable before the execution of a search warrant, whether electronic data is in fact stored remotely. Even if it is known that material is stored remotely, the country in which the data is located or the service provider who controls the data may be both unknown and unknowable. In such cases, it may be impossible to obtain remotely stored data by means other than executing a search warrant.

16.146 Thirdly, even where it is known where remotely stored data is located, or who controls the data, there will be circumstances in which it is not practicable to obtain remotely stored data by means other than a search warrant. Mutual legal assistance is a slow and cumbersome

procedure, a point acknowledged by courts[96] and legislatures.[97] Assuming that a request is acceded to and data is not deleted or modified in the interim, it may take months to obtain the data.

16.147 As for powers of production, these rely on a person who can access the data being both present on premises and cooperative. There may also be simply too much data to expect an occupier to produce.[98] Any electronic data produced may also not be in its native form, a risk that is present when production orders are served directly on service providers. Nor do we regard recourse to targeted equipment interference warrants or similar investigatory powers as an appropriate or viable route for the routine acquisition of remotely stored data: from a simple practical point of view, the Judicial Commissioners of the Investigatory Powers Commissioner's Office, who are responsible for approving such warrants, are unlikely to be able to cope with the growing demand. Accordingly, a search warrant may be the best and indeed only investigative power to obtain evidence of criminality.

16.148 We are also firmly of the view that the current law lacks clarity and search warrant provisions should be amended. The current position is highly unsatisfactory: it is not clear what powers law enforcement agencies have to search for and copy remotely stored material when executing a search warrant. This means that law enforcement agencies cannot be confident that the action that they take is legally permissible. As a result, offences may be committed and there is a greater risk of evidence being ruled inadmissible. Those agencies currently taking a cautious approach may not be acquiring highly relevant evidence of substantial value. From the perspective of the individual, it is unclear the extent to which their property and privacy rights can be infringed and whether in any given case the state has exceeded its powers and redress could be sought.

16.149 The difficult question is which statutory provisions require amendment and, for each statutory regime, in what circumstances should the power to search for and copy remotely stored data be exercisable, and under what conditions. Specifically, the following matters must be addressed.

(1) What statutory conditions should be met to be issued a search warrant, granted judicial authorisation, or permitted to exercise a statutory power, where electronic data is stored remotely?

(2) How should warrants which authorise the search for and copying of remotely stored material be drafted?

(3) What particular powers should be exercisable – either under the authority of a search warrant or by virtue of a statutory provision – when conducting a search of an electronic device on premises for remotely stored electronic data and subject to what conditions?

---

96 See *R (KBR) v Director of the Serious Fraud Office* [2018] EWHC 2368 (Admin), [2019] QB 675 at [94].

97 See the explanatory notes to the Crime (Overseas Production Orders) Act 2019.

98 The courts have been unimpressed by suggestions that occupiers should print off relevant files in lieu of investigators seizing devices. See *R (Paul Da Costa) v Thames Magistrates' Court* [2002] EWHC 40 (Admin), [2002] Crim LR 504 at [19]; *R* (*Cabot Global Ltd) v Barkingside Magistrates' Court* [2015] EWHC 1458 (Admin), [2015] 2 Cr App R 26 at [41] to [42].

16.150 There are several different ways in which a power to search for and seize remotely stored data could be drafted. It could involve applying for a warrant to search specifically for the remotely stored data. It could be an ancillary power exercisable on premises that requires separate judicial authorisation. It could be an ancillary power that switches on automatically whenever an investigator enters premises under the authority of a warrant.[99] It could be a distinct power exercisable whenever an investigator is lawfully on premises, whether under the authority of a warrant or not.[100] How the power should be framed may depend on which search warrant provisions is being considered, given that each provision differs in its structure and purpose.

16.151 In this section we consider a number of ways in which a power to search for and copy remotely stored data under the authority of a search warrant could be framed. We do this in order to highlight the various considerations that must be taken into account when constructing a model in addition to the various advantages and disadvantages of each drafting approach. The models are not intended to form rigid and exhaustive regimes: elements from each model could be traded or adjusted.

16.152 The structure, conditions and exceptions of any model adopted in respect of a particular statutory regime will depend on a multitude of factors and considerations. We therefore consider that further discussion, input and consultation will be required, likely from law enforcement agencies, digital forensics specialists, online service providers, privacy groups and others who defend and represent the interests of individuals affected by warrants to ensure that the powers under any given regime are workable in practice and proportionate.

16.153 We accept that there remains a wider question of whether revising search warrants legislation is the appropriate mechanism through which to solve the issues posed by cloud computing and remotely stored data. Search warrants are, by their nature, about the entry and search of physical premises. Therefore, what makes a search warrant conceptually a search warrant is the link to physical premises. We accept that this link may be entirely artificial where data is accessible anywhere with an electronic storage device. We discuss this in Chapter 18, which makes the case for a wider review of the acquisition and treatment of electronic material. For present purposes, we have concluded that amendments could at a minimum be made to search warrants legislation which would involve a logical and proportionate extension of the powers in a way which would go towards solving the immediate issues facing law enforcement agencies.

Model 1: data is accessible from an electronic device on premises

The model in outline

16.154 The suggestion made by two consultees to widen the statutory access conditions to cover electronic material that is accessible from an electronic device on the premises would offer a quick fix to the problem of law enforcement agencies being unable to apply for a search warrant for remotely stored data. If this model was adopted, there would be a question of how far, if at all, the recommendations that we made in respect of locally stored data in Chapter 16 should apply to remotely stored data accessible from the premises.

---

99 For example, see the Crimes Act 1914 (Australia), s 3F(2B).

100 See Chapter 18 in which we discuss the desirability of clarifying whether, and if so in what circumstances, powers of production apply where data is stored overseas.

16.155 In terms of the statutory access conditions for the issue of a warrant, modifying Recommendation 45, remotely stored data would have to be accessible from an electronic device on the premises and satisfy the other statutory access conditions. For example, the remotely stored data would have to be relevant evidence and not consist of or include protected material. Further statutory access conditions could be included to ensure that the power is only used when necessary and proportionate. For example, it could be a condition that the issuing authority is satisfied that there are reasonable grounds for believing that it is not practicable to obtain the remotely stored data by other less intrusive means.

16.156 There would also be a question mark over whether the single item theory should carry through to remotely stored data so that an electronic device is capable of being the target of a search warrant if the remotely stored data accessible from the premises meets the statutory access conditions.

16.157 Modifying Recommendations 46 and 47, application forms would require an investigator, when they are seeking to obtain a warrant to search for and remotely stored data, to explain:

(1) in as much detail as practicable what information accessible from electronic devices on premises is sought;

(2) why they believe that the information is accessible from an electronic device on the premises; and

(3) why they believe that the information would itself satisfy the statutory conditions.

16.158 Modifying Recommendation 48, the second part of the warrant should specify the information accessible from the electronic device(s) that is sought. The first part of the warrant should perhaps specify, in as much detail as practicable, the electronic device(s) to be searched for and *examined* rather than seized.

16.159 Modifying Recommendation 50, an investigator could be permitted to apply for authority to conduct a search of electronic devices found during the course of a search where it is necessary to do so for the purpose for which the warrant is issued. If granted, the warrant could authorise the search for and copying of any electronic data accessible from the device that is responsive to the information specified in the second part of a search warrant.

Advantages of the model

16.160 The advantages of expanding the statutory access conditions to include material "accessible from premises" is that it would be a relatively straightforward statutory fix. In some cases, the issue of remotely stored material has been addressed in legislation in this way in the form of a "deeming provision".[101] For example, powers of entry and search under the Higher Education and Research Act 2017 provide that references to items found on premises include:

(1) documents stored on computers or electronic storage devices on the premises, and

[101] A section of a statute, regulation or other legal instrument that explicitly states how something is to be treated or regarded.

(2) documents stored elsewhere which can be accessed by computers on the premises.[102]

16.161 The matter of whether remotely stored data could be searched for and copied would be put beyond doubt. Another distinct advantage of using the term "accessible from premises" is that, by also capturing material "on" premises, the statutory access conditions would include material in any location and therefore not require an investigator to grapple with the way in which the material is stored. The location of data would therefore hold no significance when investigators sought evidence of criminality from premises.

Disadvantages of the model

16.162 There are, in our view, several disadvantages of amending the statutory access conditions to include material accessible from an electronic device on premises. The biggest challenge would be to the proportionality of the regime and the lack of a sufficient link between remotely stored data and the premises to be searched. As we explained in the introduction to this chapter, particular remotely stored data could be accessible from *any* device on *any* premises. On a literal reading of the statutory access conditions, law enforcement agencies would be able to obtain a warrant to search their own headquarters, or the premises of an electrical retailer, as remotely stored data could be accessed with the right tools from an electronic device on any premises. Formulated in this way, the power may also be troubling from an international perspective as the location of the target data would be rendered meaningless.

16.163 On one view, this concern may be regarded as an artificial one: a court is unlikely to grant a search warrant where there is such a tenuous link between the target data and premises which an investigator seeks authority to enter. Further, in some cases, a link may be established through the fact that a specific electronic device on premises will provide additional data or metadata, such as access and download dates.

16.164 In addition, there would be sufficient safeguards to prevent search warrants being obtained arbitrarily even without the access condition being narrowed beyond that which is accessible from the premises. The statutory access conditions of search warrant provisions, read as a whole, limit the instances in which a search warrant may be obtained. For example, under PACE, there would have to be reasonable grounds for believing that the remotely stored data relates to an indictable offence that had been committed. Arguably, the statutory access conditions themselves ensure that a sufficient jurisdictional link with the remotely stored data exists.

16.165 Equally, law enforcement agencies must exercise their powers rationally, proportionately and in good faith.[103] The Human Rights Act 1998 also requires powers to be exercised in a way which is human rights-complaint.[104] Crucially, these requirements may form the grounds of a judicial review. As observed by the Divisional Court in *KBR*:

> The exercise [of the investigative power] is plainly subject to judicial review on the usual grounds. Fishing expeditions would be unlikely to survive scrutiny. Moreover, insofar as

---

[102] Higher Education and Research Act 2017, sch 5, para 9(2).

[103] *R (Miranda) v Secretary of State for the Home Department* [2016] EWCA Civ 6, [2016] 1 WLR 1505 at [113].

[104] Human Rights Act 1998, s 6(1).

any notice can be seen as oppressive or unreasonable, Art. 8 of the ECHR may well be engaged.[105]

16.166 Finally, the decision whether to grant a warrant sits with a judge: individuals are therefore protected against excessive reach by independent judicial scrutiny.[106] Together, these safeguards would significantly limit the likelihood of unreasonable searches of premises that have no link to the target data that is remotely stored.

16.167 However, on another view, it could be said that reliance on public law requirements, backed up by judicial review, and the constitutional check of a judge would not suffice to prevent the arbitrary use of search warrant were the access conditions to include material accessible from a device on premises without more.

16.168 Another disadvantage is that the regime may be regarded as not sufficiently nuanced to account for the distinct nature of remotely stored data and the actions required to collect it. As noted by the NCA, they seek the power to identify online accounts that hold remotely stored data, access/connect to these accounts and copy/download the data. The search for remotely stored data involves a completely different enterprise to the search for locally stored material, which can be as simple as specifying an electronic device as the material to be searched for on the premises and seizing the entire device. The search for remotely stored data may require the identification of specific online accounts and the performance of certain acts to obtain access. It may therefore be said that a more tailored e-warrant regime is appropriate. The strength of this criticism would depend on how any provisions were drafted.

Model 2: storage on or access from premises

The model in outline

16.169 One way of narrowing down the statutory access conditions so as to form a greater link between the remotely stored data and target premises would be to adopt the formulation suggested by the CPS: references to "material on premises" in section 8(1)(b) and schedule 1 paragraph 2(a)(ii) of PACE should include electronic data which a constable has reasonable grounds for believing that the data:

(1) would have been found on a device found on the premises but has been stored remotely from the premises, or

(2) has been placed in a remote electronic location by a person within the premises, or has been accessed from the premises.

Therefore, such material would be deemed to be stored within England or Wales notwithstanding any claim that it is or might be outside England or Wales.

Advantages of the model

16.170 Reformulating the statutory access conditions along the lines proposed by the CPS could be said to create a coherent and rational link between the electronic data and the target premises. The formulation would therefore decrease the risk of an unreasonable search and

---

105 *R (KBR) v Director of the Serious Fraud Office* [2018] EWHC 2368 (Admin), [2019] QB 675 at [73].

106 *R (Rawlinson & Hunter Trustees & Others) v Central Criminal Court, the Director of the Serious Fraud Office* [2013] 1 WLR 1634 at [78].

arguably pose less of an affront to state sovereignty than simply requiring the remotely stored data to be accessible.

Disadvantages of the model

16.171 Although a seemingly small change – such as from data that is *accessible from* premises to data that *has been accessed from* premises – the formulation might lead to arbitrary results and lead to statutory access conditions that are too difficult for law enforcement agencies to satisfy. The arbitrariness that the statutory access conditions might have can be revealed by considering a series of examples.

16.172 We consider first the CPS's first limb, that the data would have been found on an electronic device on premises but has been stored remotely. If a person made indecent images of children while abroad and uploaded the images to an online remote storage account before disposing of the electronic device, it may be said that the indecent images would never have been on the premises in this jurisdiction upon their return. Therefore, the statutory access condition would not be met.

16.173 We consider next the requirement that the data has been placed in a remote location by a person within the premises. A number of individuals could use the same device to save files which evidence criminality, with the person who uploaded the data leaving the premises. In this case, a person within particular premises may not be the same person who placed the file in a remote location. A person could also place the file in a remote location and then keep their device stored at an associate's premises, such that any person within the premises will not have placed the data in a remote location.

16.174 Turning to the requirement that the data "has been accessed from the premises", there are several reasons why it may be difficult to prove this requirement, or it may simply not be met. Issues may stem from the requirement that the data has been accessed *from the premises*. A person could access remotely stored data from a device only while outside their premises. Were the requirement to be that the data has been accessed from *a device* on the premises, regularly replacing an electronic device would mean that electronic data may not yet have been accessed from a device on premises. Issues may also stem from the requirement that the data *has been accessed* in the past. A person may not have accessed a file in the past but be presently accessing the data. Given that data is modified when accessed, it could be said that the data being accessed is not, technically speaking, the same as data that has been accessed.

16.175 It must also be recalled that an investigator must satisfy an issuing authority that there are reasonable grounds for believing, or suspecting under some provisions, that the particular state of affairs exists. It may place unreasonable constraints on investigators to have to establish reasonable grounds for believing that remotely stored data has been placed in a remote electronic location by a person within the premises, or accessed from the premises. The requirements may also lead to disputes on premises regarding whether a particular device has in fact accessed the data or whether a person within the premises has in fact placed the data in a remote location.

Model 3: sufficient connection

The model in outline

16.176 One way to avoid the broad reach of statutory access conditions that are formulated in terms of data "accessible from premises" whilst also avoiding the arbitrary results and practical difficulties that may flow from conditions that centre on access and storage would

be to adopt a sufficient connection test. An issuing authority would therefore have to be satisfied that there were reasonable grounds for believing that the remotely stored data had a sufficient connection to the premises specified in the application.

16.177 Whether the remotely stored data had a sufficient connection to the specified premises would be a question of fact, capable of being satisfied in a number of ways. For example, a sufficient connection may exist where remotely stored data:

(1) has been created by, stored by, accessed by or is being accessed from an electronic device currently on the specified premises;

(2) has been created, stored or accessed by a person who is currently residing at, occupies or controls the specified premises;

(3) is stored in an online account owned or controlled by a person and an electronic device also owned or controlled by the same person is on the specified premises; or

(4) is stored in an online account owned or controlled by a person who is currently residing at, occupies or controls the specified premises.

Advantages of the model

16.178 The sufficient connection model would be flexible enough to permit an investigator to obtain a warrant to enter premises to search for and copy remotely stored data in a range of scenarios. As new forms of technology emerge, and methods of storing data remotely develop, a sufficient connection test may also be more future-proof than a test which focusses on the performance of particular acts.

16.179 A sufficient connection test is unlikely to lead to arbitrary results, nor unreasonably constrain an investigator who tries to establish that the conditions are met. The test should also prevent search warrant applications for remotely stored data where it would be unreasonable to do so owing to no link between the data and premises concerned.

16.180 A similar test also enjoys support in a number of other settings discussed at paragraphs 16.79 to 16.86 above. In addition, the test would be more desirable from international law perspective. As with the other tests, further statutory access conditions could be included to ensure that the power is only used when necessary and proportionate. For example, it could be a condition that the issuing authority is satisfied that there are reasonable grounds for believing that it is not practicable to obtain the remotely stored data by other less intrusive means.

Disadvantages of the model

16.181 A statutory access condition for the issue of a search warrant that required a sufficient connection may suffer from a lack of clarity and imprecision. It would be less certain whether an application for a search warrant will be granted and may lead to inconsistent practices. Further, the circumstances in which remotely stored data can be searched for and copied is arguably an area of law where the conditions should be more clearly defined. A sufficient connection test may also lead to a new line of attack for challenging the decision to issue a search warrant. These problems may be partially addressed as guidance and case law emerge.

Model 4: remote storage account warrant

The model in outline

16.182 This model centres on the accessing and copying of data from a remote storage entity which is accessible from a premises. There are two points to note from the outset with a remote storage account warrant model. First, we consider it unnecessary to decide whether remote storage accounts are best classified as e-premises or an entity. State intrusion into a person's remote storage account, much the same as a person's premises, is likely to engage the right to respect for private and family life and correspondence under article 8 of the ECHR. Whether classified as a premises or not, equally robust safeguards must exist.

16.183 The second point to note from the outset is that the remote storage account warrant regime advocated for by the Whitehall Prosecutors' Group did not address the statutory access conditions to be met to justify entry onto premises in the first place. The only conditions discussed by consultees were those which would justify a search for remotely stored data while on premises.

16.184 This of course causes no trouble where there are reasonable grounds for believing other data, or the data itself, is on premises as a normal warrant could be sought. However, for the reasons explained at paragraphs 16.103 and 16.104 above, certain warrants cannot be issued where there are no reasonable grounds for believing that data is on premises because it is stored remotely. As it stands, it is unclear how the conditions suggested by the Whitehall Prosecutors' Group would be transposed into statutory access conditions, as there is a seeming lack of connection to specified premises.

16.185 Putting the statutory access conditions to one side, based on the submission of the Whitehall Prosecutors' Group, the statutory conditions for authorisation would require reasonable grounds for believing/suspecting that:

(1) a remote storage account accessible from the premises either:

(a) belongs to an occupier or suspect; or

(b) contains the occupier or suspect's data; and

(2) the occupier or suspect is present in the jurisdiction.

16.186 The e-premises warrant would be required to specify:

(1) both known remote storage accounts and remote storage accounts which cannot be identified in advance of the search; and

(2) particular file types, or all files responding to a certain search term.

16.187 The e-premises warrant would authorise an investigator to search for remote storage accounts corresponding to the warrant, access the account and copy remotely stored data responsive to search terms also specified in the warrant.

Advantages of the model

16.188 A model that treats remote storage accounts as a separate entity or e-premises would provide for a more nuanced and focused regime that appreciates the distinction between locally and remotely stored data, and from where the latter is to be sought. It follows that the regime would be more proportionate by limiting the pool of remotely stored data obtainable

to that which corresponds to specific search terms and is stored in a pre-identified online account. In this regard, the regime would reflect our recommendation at Recommendation 48 for a two-part warrant (specifying the thing to be searched for and the information it holds that is sought). The regime would also achieve the NCA's requirements: authority to identify online accounts, connect to them and copy relevant data.

16.189 We regard the inclusion of online accounts that are not in the name of a suspect, but contain their data, within the statutory conditions as important for the workability of such a model: most remote storage accounts can be used with false or anonymised user details, which would not be known until the account was accessed. For similar reasons, it is understandable that an investigator would not be able to specify the remote storage accounts to be searched with the level of specificity suggested by the Whitehall Prosecutors' Group at paragraph 16.138 above. It would therefore seem sensible for the model to extend to attributable remote storage accounts that cannot be identified in advance of the search.

16.190 There would also be a strong jurisdictional connection where the data is remotely stored in the online account of a suspect present in the jurisdiction, or in an online account that contains that suspect's data. An investigator could only access and copy data that belongs to or concerns a person present within the jurisdiction. The regime would therefore be less likely to cause problems from an international law perspective.

Disadvantages of the model

16.191 As with the second model we discussed, depending on how the statutory conditions for authorisation to search remote storage accounts were worded, arbitrary results may be produced. For example, the suspect or occupier may frequently travel abroad meaning that they are not present in the jurisdiction. The model would also have to account for how an investigator would be authorised to enter specific premises in the first place and what connection the premises should have to justify entry onto it.

Amending the CJPA regime

16.192 We agree that it should be made clear how the seize and sift provisions under the CJPA apply to remotely stored data. We can envisage scenarios where, when searching an online account, it would not be possible to carry out a targeted search of the account or ascertain that which fell within the scope of the warrant. In such cases, the reasons justifying the principle under the CJPA regime that an investigator is permitted to seize more data than they are entitled to in order to sift the data off-site would, in our view, have equal application to remote storage accounts.

16.193 It is difficult to discuss reform of the CJPA in any meaningful way without a clear view of the model of search and copying to be adopted. There may also be a question of whether the CJPA itself should be amended or whether the power to seize and sift remotely stored data should be contained within each relevant search warrant regime. We also note that, on a strict reading of section 50(1)(c) of the CJPA, it is arguable that the CJPA would already permit the extraction of more remotely stored data than necessary for the purpose of sifting the data off-site, provided the power to copy data is specified in part 1 of schedule 1 to the CJPA.

Conclusion

16.194 When the New Zealand Law Commission published its report on search and surveillance powers in 2007, it described the search of remotely stored material as "one of the most difficult areas" dealt with in its report.[107] Ten years on, in their 2017 report, the New Zealand Law Commission and Ministry of Justice recommended that further consideration be given to whether an investigator should be required to obtain a search warrant with internet access authorisation before accessing the internet during a search.[108] In doing so, the report indicated that the recommendations were preliminary in nature, with firm recommendations regarded as inappropriate because further consultation with technical experts would be required to ensure that the recommendations were workable.[109]

16.195 We consider ourselves driven to a similar conclusion. It is not possible for us to reach a definitive conclusion of the appropriate model to be adopted in respect of the many search warrant regimes without further technical and cross-sectional input to refine any model adopted. There are a host of highly technical issues that must be resolved and on which we did not receive sufficient evidence to reach a concrete view.[110] Any reform must also consider the interplay with powers under IPA, RIPA and other Acts which fall outside of our terms of reference. We would also agree with the comment made by the Law Society that the topic of electronic material generally "seems to require separate, specialist consideration and consultation in its own right."

16.196 While we make no firm recommendations, we have reached the following conclusions:

(1) Law enforcement agencies should be given the powers to enter premises, search for and copy remotely stored data when executing a search warrant. Such powers are necessary to protect the public and effectively investigate and prosecute crime. There will be circumstances where it is not practicable to obtain evidence by means other than executing a search warrant.

(2) It is unclear under the current law in what circumstances the search for and copying of remotely stored data is permitted. Irrespective of whether law enforcement agencies can search and copy remotely stored data under any given regime, such acts should be governed by a clearer framework. The law should therefore be amended.

(3) Any amended laws must not unreasonably constrain the ability of law enforcement agencies to obtain remotely stored data. At the same time, amended laws must be drafted in such a way that there is an appropriate link between the remotely stored data and premises to be searched and so that jurisdictional problems will not arise from an international perspective. We have discussed the circumstances in which states have deemed there to be a suitable jurisdictional connection for the purpose of enforcement jurisdiction at paragraphs 16.79 to 16.90 above. The search and copying of remotely stored data must have identifiable boundaries that ensure that

---

107 Law Commission Search and Surveillance Powers (NZLC R97, 2007) para 7.116.

108 New Zealand Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012 / Ko te Arotake i te Search and Surveillance Act 2012*, NZLC R141 (2017) p 220 (Recommendation 45).

109 New Zealand Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012 / Ko te Arotake i te Search and Surveillance Act 2012*, NZLC R141 (2017) paras 12.19, 12.129, 12.133 and 12.144.

110 For example, in what state must an electronic device be to be searched? How far should an investigator be permitted to operate an electronic device? To what extent should an investigator be permitted to use their own electronic devices to conduct a search while on premises?

authorisation is given only where necessary to do so and the search is carried out in a proportionate manner subject to stringent safeguards.

Recommendation 51

16.197 We recommend that the Government considers the desirability of amending the law to permit law enforcement agencies to obtain authorisation to search for and copy remotely stored data when executing a search warrant.

COMPELLING ACCESS TO PROTECTED INFORMATION

The current law

16.198 A common problem for investigators is that electronic devices, and online accounts, are protected by passwords, encryption and two-factor authentication.[111] As we set out in our section on relevant legal regimes, there are statutory powers to assist in obtaining access to electronic devices.

16.199 Section 49 of RIPA provides a power to impose a disclosure requirement on a person believed to have a key, code, password, algorithm or other data which allows access to protected information. A person to whom a section 49 RIPA notice has been given is guilty of an offence if he knowingly fails, in accordance with the notice, to make the required disclosure.[112] A requirement of disclosure of knowledge of the means of access to protected data under compulsion of law will not engage the privilege against self-incrimination unless the electronic data itself, which exists independently of the person's will and to which the privilege does not apply, contains incriminating material.[113] In any event, any interference with the privilege against self-incrimination may be proportionate and permissible.[114] The existence of such privilege does not justify refusing an application for permission to give a section 49 notice.[115] An application for a direction pursuant to a court's case management powers to disclose a decryption key or password cannot be used to circumvent section 49 of RIPA.[116]

16.200 Section 49 of RIPA is not the only statutory provision which provides a power to compel the production of passwords. Under the Terrorism Act 2000, there is a power to request "any information",[117] which may include a password.[118]

---

111 See paragraph 14.23 above.

112 Regulation of Investigatory Powers Act 2000, s 53(1).

113 *R v S* [2008] EWCA Crim 2177, [2009] 1 WLR 1489 at [24].

114 *R v S* [2008] EWCA Crim 2177, [2009] 1 WLR 1489 at [25].

115 *Greater Manchester Police v Andrews* [2011] EWHC 1966 (Admin), [2011] ACD 18.

116 *Love v National Crime Agency* [2016] Lloyd's Rep FC 424.

117 Terrorism Act 2000, sch 7, para 5(a).

118 See *Rabbani v DPP* [2018] EWHC 1156 (Admin).

The consultation paper

16.201 We explained in our consultation paper that stakeholders told us that sections 19(4) and 20(1) of PACE, and section 2(3) of the Criminal Justice Act 1987, have on occasion been used to compel the production of passwords. It was said that most police forces, however, follow the route set out under part 3 of RIPA to obtain a decryption key where they do not have the technical capability to defeat an electronic device's security measures. One stakeholder described this "blurred and confusing" overlap as ripe for reform.[119]

16.202 In the consultation paper we argued that interpreting production powers as empowering investigators to compel the production of passwords would provide very far reaching powers, which apply whenever a constable is lawfully on premises whether in exercise of a warrant or otherwise. In particular, the powers may be exercised without judicial authorisation at any stage.

16.203 Stakeholders suggested the introduction of a power under warrant to compel passwords for electronic information. Two main arguments were put forward for introducing a power under warrant to compel passwords or encryption keys.

(1) If the court is persuaded to issue a warrant permitting entry to the premises to be forced, the premises searched, and a laptop removed, it seems that the warrant should also be capable of permitting access to cloud data accessible from the laptop, as this is arguably a less intrusive act.

(2) the use of electronic media, cloud storage and encryption is no longer the sole preserve of organised crime and has become commonplace. If would be burdensome if routine criminal investigations had to involve the special investigative methods in IPA and/or RIPA.

16.204 Whilst we saw some merit in these arguments, we considered that to propose this kind of power would fall outside the scope of the present project, as it would in essence be an extension of other statutory powers under RIPA that have not been the focus of the review. We concluded that, whether or not such a power is desirable, discussion of it formed no part of the present project.

Consultation responses

16.205 Five consultees made comments regarding the power to compel the production of passwords.[120] The Bar Council and the CBA did not agree that there was any objection in principle to section 19(4) of PACE power being used to compel the surrendering of passwords. They could see no reason why part 3 of RIPA, with its significant maximum sentence for non-compliance, should provide the only means by which passwords may be required.

16.206 Quite apart from whether section 19(4) allowed law enforcement agencies to compel the production of passwords, several consultees indicated the importance of the power. Dijen Basu QC observed that, if warrants were permitted to cover remotely stored data, the power would need to be supplemented by a power to issue a decryption notice to be complied with

---

119 David McCluskey, Consulting Partner at Taylor Wessing.

120 Bar Council and the Criminal Bar Association; Dijen Basu QC; Whitehall Prosecutors' Group; Financial Conduct Authority; HM Revenue and Customs.

immediately, on pain of similar penalties as in part 3 RIPA for failure to comply without reasonable excuse.

16.207 The Whitehall Prosecutors' Group suggested that any search warrant power to search remotely stored data should be capable of being supported by a power, granted by the issuing authority alongside the warrant, to require the account holder to provide the login details to a remote storage account or to give the officer executing the warrant immediate access to the same (on pain of punishment). It was said that any reform would need to consider section 49 of RIPA to ensure that officers can compel access to the data covered by the warrant immediately. The Whitehall Prosecutors' Group suggested that it may be better for the section 49 style power to sit alongside the power to apply for and execute an e-warrant.

16.208 The FCA argued that the power to compel the production of passwords should not be outside the scope of the present project because there is no point in having the power to seize data that cannot be accessed. In their view the two issues were self-evidently linked. Further, it was said that two-factor authentication renders seizure, and attempted access to remotely stored data, useless without related powers to compel the means to intercept authorising pin codes and decrypt and override security. They also argued that sanction for suspects or third parties failing to assist with these processes should be created and should be significant.

16.209 HMRC stated that it was vital that a search warrant under PACE and POCA be able to permit search of the cloud and copying of any data found there, as well as the issuing of a notice requiring the disclosure of passwords to enable such a search to be carried out. They stated that there may be merit in consolidating the power to issue a notice requiring provision of passwords or keys to access data under section 49 of RIPA.

Analysis

The necessity of powers to compel access to protected information

16.210 We accept that without a power to require passwords, any power to search for and copy remotely stored material will be rendered ineffective in certain circumstances. Virtually all electronic data is protected by either a password, encryption or two-factor authentication. As put by the New Zealand Law Commission and Ministry of Justice in their 2017 report:

> In recent years there has been a significant growth in encryption technologies that hinder law enforcement's access to devices and online accounts …
>
> Due to these developments, law enforcement agencies around the world are increasingly struggling to access data held on electronic devices and in online accounts, even when they have lawful authority to do so in the form of a warrant.
>
> We consider that, if an electronic device or online account is the subject of a search warrant, the Act should provide law enforcement officers with meaningful and appropriate tools to lawfully obtain the necessary passwords, encryption keys and other access information. Without such tools, these warrants would be redundant.[121]

[121] New Zealand Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012 / Ko te Arotake i te Search and Surveillance Act 2012*, NZLC R141 (2017) paras 12.155 to 12.157.

16.211 The Independent Reviewer of Terrorism Legislation, Jonathan Hall QC, recently spoke about the problems caused by the inaccessibility of devices in terrorism investigations.[122] The point was made that techniques such as end to end encryption, encrypted metadata and auto-destruction of communications are here to stay. Further, it was said that:

> Although advances in de-encryption are constantly being made, it is quite possible in the near future that terrorism investigations will be defeated by suspects withholding passwords meaning that police cannot obtain access to electronic evidence of attack planning or terrorist publications or the like… it is questionable whether the existing law provides an adequate framework for deterring individuals from refusing to allow access to information on their devices.

16.212 The compulsion of passwords has been the subject of recent judicial examination in other jurisdictions. In the case of *Shergill*,[123] the Ontario Court of Justice refused to order an accused to unlock his smartphone or to provide the Crown with the password for the device as it would engage the accused's right to silence and the protection against self-incrimination. The court did, however, acknowledge that the current digital landscape presented challenges to law enforcement and that legislative reform may be warranted.[124]

16.213 Where law enforcement cannot obtain a password, the only option is to try and break into the device with decryption tools. The level of success may vary depending on the software installed on the device and the tools which law enforcement have.

Whether the current law requires reform

16.214 The first argument for reforming the current law is that it is, at present, unclear what powers permit the compulsion of passwords. Accordingly, there is inconsistent practice across law enforcement agencies. We agree that it would be useful to put beyond doubt which provisions permit the compulsion of passwords and other information to access electronic material. We explain at paragraphs 18.59 to 18.62 below why we consider it is unlikely that section 19(4) of PACE permits a constable to require the production of a password. Even if provisions such as sections 19(4) and 20(1) of PACE and section 2(3) of the Criminal Justice Act 1987 could be used to compel the production of passwords, it is our view that these provisions do not provide a sufficiently robust framework to govern such activity.

16.215 The second argument for reforming the current law is that a power to compel passwords should sit alongside a search warrant regime. Arguably, it would make the powers self-contained, which would render the law clearer, and enable the power to be purpose-built. This is also the position in other jurisdictions.[125]

16.216 The third argument in favour of reforming the current law is that part 3 of RIPA is deficient. This is a point to which stakeholders and consultees alluded. RIPA notices are rarely served;

---

122 Jonathan Hall QC, "Scanning the Horizon: Technology and Risk" (22 January 2020), <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2020/01/200122-HJS-speech-.pdf>.

123 *R v Shergill* (2019) ONCJ 54.

124 *R v Shergill* (2019) ONCJ 54 at [51]. See also the decision of the Massachusetts Supreme Judicial Court for the County of Suffolk in *Commonwealth v Jones* 481 Mass 540, 117 NE 3d 720.

125 Crimes Act 1914 (Australia), s 3LA; Search and Surveillance Act 2012 (New Zealand), s 130.

106 notices were issued across the UK in 2017.[126] We understand that the process for obtaining a RIPA notice is regarded as too slow and onerous. We were also informed by one law enforcement agency that there is a reluctance to prosecute individuals for failing to comply with a notice that is served.

16.217 While written permission for the giving of a notice can only be authorised by a circuit judge or district judge (magistrates' courts),[127] this is subject to a number of exceptions. For example, a search warrant may empower a person to serve a notice requiring disclosure if the warrant gives explicit permission for the notice to be given.[128]

16.218 Where prosecutions are brought, and persons are convicted, the sentence of two years' imprisonment (or five years' in cases of child abuse or national security) may be regarded as incommensurate with the sentence for the suspected offence.

16.219 For example, a murder suspect was sentenced to 14 months' imprisonment for refusing to give his Facebook password to detectives investigating the death of a 13-year-old girl. Therefore, a person being investigated for murder, which carries a mandatory life sentence,[129] may on a cost-benefit analysis decide it is better to plead guilty to that offence at the first available opportunity to face a maximum 16 months' imprisonment.[130]

16.220 Even if it is accepted that the current law requires reform, there is then the question of what that reform should be. There are several issues regarding the operation of a power to compel the production of passwords. For example, does it follow from the warrant or does it require judicial approval. If so, should approval come from a magistrate or a Crown Court judge? In what circumstances, if any, should urgent authorisation be obtainable? Should the power compel an individual to disclose information or provide assistance?[131] What should the penalty for non-compliance be? How should it be linked, if at all, to the offence that is being investigated? What opportunity should a person have to resist a notice pending legal advice? What other safeguards should exist? These are all important matters on which there are a range of possible views and on which further consultation would be necessary before reaching a firm conclusion.

16.221 There are several cumulative reasons why we cannot make a firm recommendation on this matter. First, it is not a matter on which we directly consulted. Secondly, we did not receive sufficient evidence from consultees to reach a firm view. We also did not receive consultation responses from privacy organisations and others who defend and represent the interests of individuals affected by warrants. Thirdly, any reform would likely involve detailed consideration of, and amendment to, part 3 of RIPA, which is not within of our terms of reference. That said, based on the consultation responses that we did receive, and the

---

126 Investigatory Powers Commissioner's Office, *Annual Report of the Investigatory Powers Commissioner 2017* (HMSO, 2019), Cm 1780, para 6.7.

127 Regulation of Investigatory Powers Act 2000, sch 2, para 1(1).

128 Regulation of Investigatory Powers Act 2000, sch 2, para 2(2)(a).

129 Murder (Abolition of Death Penalty) Act 1965, s 1(1).

130 See also *Rabbani v DPP* [2018] EWHC 1156 (Admin) in which the appellant refused to provide the PIN and password for his mobile phone and laptop computer, which led to a conviction for an offence of wilfully obstructing or seeking to frustrate a search or examination contrary to the Terrorism Act 2000, sch 7, para 18(1)(c).

131 See Higher Education and Research Act 2017, sch 5, para 6(d). See also Crimes Act 1914 (Australia), s 3LA.

analysis that we have undertaken, we consider that it is a matter that would merit further consideration.

Recommendation 52

16.222 We recommend that the Government considers the desirability of amending the law governing the power to compel the production of passwords and other access information with the aim of making the law clearer and more effective. This should include consideration of an integrated power to form part of search warrant regimes.

PREVENTING INTERFERENCE WITH REMOTELY STORED DATA

The current law

16.223 When electronic material is stored locally on premises, an investigator can seize the entire device, which will prevent interference with the electronic data. In contrast, with remotely stored data, even if an electronic device is seized, data stored in an online account can still be accessed, and therefore modified or deleted, by using another device to connect to the online account.

16.224 There are no statutory powers that explicitly permit a law enforcement agency to modify or alter remotely stored data for the purpose of preventing interference with it. Section 2(5)(b) of the Criminal Justice Act 1987 and section 176(5) of the Financial Services and Markets Act 2000 provide a power when executing a search warrant to take any steps which may appear to be necessary for preserving relevant documents or information or preventing interference with them. On one interpretation, these provisions could permit the modification of remotely stored data to prevent interference. Property interference authorisation under the Police Act 1997 may also be regarded as a legal basis to modify the data of a remote storage account.

16.225 The only other option that law enforcement agencies will have to prevent interference with remotely stored data is to make a preservation order. This can be requested through mutual legal assistance channels or by making a request to a service provider.

The consultation paper

16.226 We did not discuss the availability of powers to prevent third-party interference with remotely stored material in the consultation paper, however, it was an issue raised with us in consultation responses.

Consultation responses

16.227 Two consultees[132] discussed this issue during the consultation period. DS Clayton Ford, a Detective Sergeant with Essex Police, wrote that in order to prove the making (ie downloading) of indecent images, surrounding evidence is required beyond the indecent images themselves. This evidence, along with the indecent images themselves, will often be located in email and cloud storage accounts. Therefore, online accounts contain relevant evidence beyond the indecent images themselves.

[132] DS Clayton Ford, Essex Police; Financial Conduct Authority.

16.228 He stated that, while the images themselves can be examined and recorded at the scene of the search warrant, what cannot be done is to take control of online accounts through for example, changing a password. As a result, evidence may be lost as data stored in online accounts can be modified through another device once investigators leave the premises. Examination of online accounts at the scene is an incredibly lengthy process, akin to sifting through thousands of sheets of paper.

16.229 As a solution, DS Ford proposed a power to "take control" of any data that is available during the execution of a search warrant, along similar lines to the "seize and sift" provisions under the CJPA, which permit the taking control of inextricably linked physical objects. The FCA also stated that they require, along with the power of extraterritorial search, data preservation authority.

Analysis

16.230 As indicated, there are few, if any, statutory powers that could be relied on as a lawful basis to modify or alter remotely stored data. The only options would therefore be to seek preservation of the data. As noted at paragraph 16.129 above, we were informed that certain communication service providers may take six months to respond or delete the data requested, thereby losing evidence.[133] Further, such requests may be impossible to draft as the data comprising the file sought could be scattered across multiple jurisdictions and move jurisdictions many times a day.[134] In our view, seeking preservation from service providers or states is therefore not an effective means of preventing the modification or alteration of remotely stored data to prevent interference.

16.231 This poses the question of whether law enforcement agencies should have an explicit power to modify or alter remotely stored data to prevent interference. The underlying rationale on which the power to modify remotely stored data is premised is shared with several powers already on the statute book. At its heart is the need to prevent evidence of criminality being lost, altered or destroyed.

(1) Section 19(4) of PACE requires, as a condition precedent, reasonable grounds for believing that it is necessary to require information to be produced in order to prevent it being concealed, lost, tampered with or destroyed.

(2) Section 56(1) of the CJPA provides that, where a constable has been involved in the seizure of material under section 50 or 51 CJPA, it is possible to retain evidence of any offence or property obtained in consequence of the commission of an offence if it is necessary to do so to stop it being "concealed, lost, damaged, altered or destroyed" even if this is not material which was being searched for.

(3) As set out at paragraph 16.224 above, section 2(5)(b) of the Criminal Justice Act 1987 and section 176(5) of the Financial Services and Markets Act 2000 provide a power when executing a search warrant to take any steps which may appear to be necessary for preserving relevant documents or information or preventing interference with them.

---

133 Staffordshire Police.

134 Whitehall Prosecutors' Group; Financial Conduct Authority.

16.232 An explicit power to alter data pursuant to a search warrant is found in Australian federal law. Under section 3F(2A)(b) of the Crimes Act 1914, a warrant that is in force authorises the executing officer or a constable assisting to add, copy, delete or alter other data in the computer or device found in the course of a search authorised under the warrant. This can only take place where necessary to obtain access to data in order to determine whether the relevant data is evidential material of a kind specified in the warrant. The provisions do not explicitly state that the alteration of remotely stored data can take place to prevent the data being modified.

16.233 Section 3F(2C)(a) provides that activities undertaken to access data do not authorise the addition, deletion or alteration of data when those actions are likely to interfere with communications in transit or the lawful use by other persons of a computer, unless specified in the warrant. Section 3F(2C)(b) further provides that activities do not authorise the material loss or damage to other persons lawfully using a computer.

16.234 We can see the rationale of a power to modify or alter data to prevent interference. At the same time, we recognise that valid concerns are raised by such intrusive powers. On 12 June 2019, a debate took place organised by University College London and Bindmans LLP on state security and freedom of the press. Jodie Ginsberg, Chief Executive of Index on Censorship, spoke about the search warrants executed by the Australian Federal Police on the headquarters of the Australian Broadcasting Corporation, which gave police the powers to "edit or delete material". This reference would have been to the power emanating from section 3F of the Australian Crime Act 1914 discussed above. It was said that the power "sounds like an invitation to plant evidence by the police."

16.235 This is a reason why the chain of custody is of vital importance and the forensic integrity of data must be maintained. By altering data, the continuity of evidence may be lost. This issue is dealt with to some degree by the ACPO Good Practice Guide for Digital Evidence. The ACPO Guidelines require that if an investigator performs an act that is likely to access data they must be competent to do so and be able to give evidence explaining why it was done.[135] We discuss the potential for updating and consolidating these guidelines in a new Code of Practice, which we recommend above.

16.236 On one view the "taking over" of an online account in the way in which we have described would not alter individual data files but only the metadata around access dates and times. Emails or text messages would also potentially need to be sent to overcome two-factor verification devices. DS Clayton Ford accepted that there may be a minor loss of data as a result of "taking over" an online account but that it would be justified against the aims of the investigation as per the ACPO Guidelines.

16.237 As with the other topics discussed in the chapter, a definite view on the desirability of a power to modify or alter remotely stored data, and the contours of any such power, would require further technical and cross-sectional input. Like the power to compel passwords, it is not a matter on which we directly consulted, nor have we received a sufficiently broad range of consultation responses to reach a firm view. That said, based on the consultation responses that we did receive, and the analysis that we have undertaken, we consider that it is a matter that would merit further consideration.

---

135 ACPO, *Good Practice Guide for Digital Evidence (Association of Chief Police Officers* (2012) para 2.1.2.

Recommendation 53

16.238 We recommend that the Government considers the desirability of introducing a power to modify or alter remotely stored data exercisable pursuant to a search warrant for the purposes of preventing interference with or preserving the data.

Chapter 17: The treatment of electronic material

INTRODUCTION

17.1 In Chapters 15 and 16 we make several recommendations regarding the search for and seizure or copying of electronic devices and electronic data (together, "electronic material") pursuant to a search warrant. In this chapter, we consider the law and procedure which governs the treatment of electronic material once it is in the possession of a law enforcement agency following the execution of a search warrant. We no longer maintain a distinction between locally and remotely stored data. This is because we consider that the framework governing the treatment of material should not differ based on whether electronic data now in possession of an investigator was previously stored on an electronic device on premises or remotely held.

17.2 We begin the chapter by providing a short summary of the current law. We then proceed to discuss the problems with the current law identified in our consultation paper and set out the consultation responses. Finally, we recommend in this chapter a new statutory regime to govern the treatment of electronic material seized or copied pursuant to a search warrant. We also recommend that the regime is supplemented by a new Code of Practice which would regulate the acquisition and treatment of electronic material in search warrant cases. Set out together, the recommendations that we make in this chapter are as follows.

(1) We recommend the introduction of a new statutory regime governing the treatment of electronic material. The regime ought to apply whenever a relevant power of seizure or production is exercised in respect of electronic material following the execution of a search warrant.

(2) We recommend that, under this new statutory regime, an investigator be required to provide the following information within a reasonable time from a person with an interest in the electronic material making a request for it:

(a) as specific a description of what was seized as is reasonably practicable;

(b) details of what action was taken in respect of electronic devices on premises in as much detail as practicable; and

(c) protocols setting out how electronic material is to be examined.

(3) We also recommend that an investigator be required to comply with the following statutory duties:

(a) to return electronic devices following seizure on premises as soon as reasonably practicable;

(b) to return and/or delete protected electronic material as soon as reasonably practicable; and

(c) to return and/or delete non-responsive electronic material so far as is reasonably practicable.

(4) We also recommend that a person with an interest in electronic material be able to apply to the Crown Court for:

(a) a judge to approve of, or adjudicate on disputes regarding, the way in which the investigator intends to examine electronic material; and

(b) the return or deletion of particular electronic data or return of an electronic device on the grounds that:

(i) the electronic material is reasonably required by the person with an interest in it; or

(ii) continued retention by an investigator of the electronic material is not necessary.

(5) Finally, we recommend the creation of a Code of Practice governing the acquisition and treatment of electronic material in criminal investigations involving search warrants.

17.3 Our recommendations would introduce strong and consistent safeguards to the treatment of electronic material. They would lead to greater transparency, accountability and limit the interference with property and privacy rights. At the same time, the recommendations would facilitate the expeditious examination of electronic material in a way which does not inhibit criminal investigations or impose unreasonable demands on law enforcement agencies. The recommendations would permit operational flexibility and practical justice to be achieved on a case by case basis.

SUMMARY OF THE CURRENT LAW

17.4 We have already set out an overview of the current law regarding the treatment of electronic material in Chapter 14. In this section, we repeat a number of observations relevant to the issues that we will be discussing.

17.5 There are no provisions specifically governing the treatment of *electronic* material seized pursuant to a search warrant. Instead, the way in which such material is handled is regulated by the provisions which govern the treatment of material generally. The legal obligations and powers which apply post-seizure or copying depend on the power under which seizure was made and the official who exercises the power of seizure.

17.6 Owing to the impracticability of searching through large volumes of material on-site, a detailed regime for the excess seizure of material and later sifting off-site was provided in part 2 of the Criminal Justice and Police Act 2001 ("CJPA"). The explanatory notes indicate that the drafters of the Act had electronic material in mind, albeit in 2001 when the digital landscape differed quite drastically. The CJPA provides a set of safeguards, which include serving a written notice containing information[1] and the duty of an investigator to sift out non-responsive material.[2] However, these safeguards only apply when material has been seized

---

1 Criminal Justice and Police Act 2001, s 52.

2 By this we mean material that does not fall within the scope of the warrant (see Criminal Justice and Police Act 2001, s 53).

under the CJPA[3] and not under the authority of the warrant or in response to a power of production.

17.7 There are a number of additional powers and duties that will apply under other legislative regimes. By way of brief summary, various overlapping statutory provisions govern the power to retain seized material. Additionally, the Code of Practice issued under the Criminal Procedure and Investigations Act 1996 creates a duty to retain relevant material and pursue all reasonable lines of enquiry. Data must also be processed lawfully under part 3 of the Data Protection Act 2018, and section 6 of the Human Rights Act 1998 makes it unlawful for a public authority to act in a way which is incompatible with the European Convention on Human Rights ("ECHR").

THE CONSULTATION PAPER

17.8 Our focus in our consultation paper was on the shortcomings of part 2 of the CJPA as it is this regime that governs the off-site sifting of voluminous and mixed material. We identified three issues with the regime when applied to electronic material. Those issues, which will now be discussed in turn, were:

(1) the inapplicability of the CJPA seizure powers where investigators are authorised to seize an entire electronic device;

(2) the fact that the CJPA safeguards only apply to relevant powers of seizure; and

(3) the difficulty in applying the CJPA regime in investigations involving large volumes of electronic material.

The inapplicability of Criminal Justice and Police Act 2001 seizure powers where authorised to seize an entire device

17.9 As discussed in our consultation paper, the single item theory conceptualises an electronic device as a single entity, which is capable of being the target of a search warrant and seized notwithstanding that it might also contain irrelevant material. In contrast, the CJPA regime envisages electronic devices being treated as a container when determining whether to exercise powers of seizure. This is apparent from the explanatory notes to the two powers of seizure contained in section 50 of the CJPA:

> Subsection (1) applies where a constable or other person exercising an existing power of search is unable to determine whether something may be or may contain something for which he is authorised to search, e.g. where there is a large bulk of material. Subsection (2) applies to the situation where the constable is unable to separate out the material he is able to seize from that which he is not e.g. *where the material is on a computer*. If it is not "reasonably practicable" to carry out the determination or separation required by subsections (1) and (2) the material can be seized to be examined elsewhere (emphasis added).

17.10 This disconnect means that, where a search warrant authorises the search for, and seizure of, an entire device, the warrant may preclude the application of the CJPA seizure powers under the 'plain meaning' or literal rule of statutory construction. This is because, where an investigator is entitled to seize an entire electronic device under the authority of a search

[3] Criminal Justice and Police Act 2001, s 50.

warrant, neither power of seizure applies: it *is* reasonably practicable for the investigator to determine what they are entitled to seize as they can seize the entire device. Further, any target data is contained in something which they *do* have power to seize: the entire device.

17.11 As a result, where the search and seizure of electronic devices is pursuant to a warrant – and the devices have been specified on the face of the warrant with no express exclusion of protected material – recourse to part 2 of the CJPA is a voluntary exercise, rather than one that is compelled by law. Where electronic devices are seized under the authority of a search warrant rather than the CJPA, the safeguards under sections 52 (written notice) and 53 (off-site sift) of the CJPA do not apply.

17.12 A number of stakeholders recognised this practical effect of treating a computer as a single relevant item for the purposes of warrant applications and voiced concern regarding the circumvention of the greater protections in part 2 of the CJPA. One stakeholder argued that the powers in section 50 of the CJPA are used in only a fraction of the cases where they ought to apply.

The limited reach of the Criminal Justice and Police Act 2001 statutory safeguards

17.13 In our consultation paper, we listed two further ways in which the statutory safeguards have limited reach. The first is that the safeguards under sections 52 and 53 of the CJPA are contingent on seizure being made under section 50 of the CJPA. However, seizure under section 50 can only be made where an investigator would otherwise be able to exercise a power of seizure specified in part 1 of schedule 1 to the CJPA. As a result, material which is produced in response to a power of production cannot be seized under the CJPA powers. Certain powers of production are treated as powers of seizure for the purpose of part 2 of the CJPA,[4] however, not for the purpose of sections 50 and 51.[5]

17.14 Secondly, the Law Society's Criminal Law Committee also drew our attention to the fact that if, after conducting a search, it becomes apparent that a seized item contains privileged or other protected material, there appears to be no mechanism to re-categorise the material so that it is retained under a different statutory provision. Therefore, if electronic devices are seized pursuant to a search warrant adopting the single item theory, and it later becomes apparent that the device contains privileged or other protected material, sections 52 and 53 of CJPA governing the sorting of material and the return of protected and irrelevant material do not apply.

The difficulty in applying the Criminal Justice and Police Act 2001 regime in investigations with large volumes of material

17.15 In the consultation paper,[6] we alluded to the case of *Business Energy Solutions Ltd*,[7] the judgment of which had not yet been handed down. We suggested that the need for litigation on such fundamental issues as the meaning of "seized property", "return" and "reasonably practicable" illustrates that the CJPA may be inadequate to deal with the realities of modern investigations.

---

4 Criminal Justice and Police Act 2001, s 63(2).

5 Criminal Justice and Police Act 2001, s 63(1)(c).

6 Search Warrants (2018) Law Commission Consultation Paper No 235 at para 10.100.

7 *Business Energy Solutions Ltd v Crown Court at Preston* [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887.

17.16 In *Business Energy Solutions Ltd*, the Divisional Court considered two matters of statutory construction concerning the CJPA. First, whether the duty to "return" seized property in section 53 of the CJPA applied to retained data which is copied from seized computer storage devices which are, following copying, restored to their owners. Secondly, whether the reasonable practicability of separation test, in sections 53 and/or 59 of the CJPA, was based upon physical/technical capability or a broader practical capability. The court relied on a purposive construction to answer the first question in the affirmative, although it accepted that the language of the CJPA did not naturally or easily embrace the destruction of electronic data.[8]

17.17 It has been suggested that the issues raised by the case illustrate that the language of the CJPA may be struggling to keep pace with modern digital forensics.[9] Another example given is the ambiguity over what is envisaged in cases involving large volumes of material by the duty under section 53 of the CJPA to conduct an "initial examination" following the seizure of devices.

The consultation questions

17.18 In response to the problems identified with the current law in respect of the CJPA regime, we invited consultees' views on:[10]

(1) the current operation of part 2 of the CJPA in relation to electronic material;

(2) whether the CJPA contains adequate safeguards where the case involves a search and seizure of electronic devices containing large volumes of data; and

(3) how, if the current safeguards are inadequate, consultees propose the scheme should be amended.

17.19 Separately, we considered that, if the practice of seizing entire electronic devices under powers other than the CJPA was to continue, the statutory safeguards in the CJPA ought to apply whenever an electronic device is seized.[11] In making a provisional proposal to this effect, we envisaged the statutory safeguards in the CJPA which would apply would be those remodelled in light of the consultation questions above. With that in mind, we provisionally proposed[12] that, in principle, the procedures and safeguards in the CJPA ought to apply whenever electronic devices are seized under powers exercised when executing a search warrant. If consultees agreed, we invited further views on which procedures and safeguards ought to apply.

---

8 *Business Energy Solutions Ltd v Crown Court at Preston* [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [83].

9 Alex Davidson, "Seizure of Electronic Data: Business Energy Solutions Ltd v Preston Crown Court (Case Comment)" [2018] *Criminal Law Review* 860 at 864.

10 Consultation Question 53.

11 Search Warrants (2018) Law Commission Consultation Paper No 235 at para 10.175.

12 Consultation Question 57.

CONSULTATION RESPONSES

17.20 Seventeen consultees[13] shared their views on the operation of the CJPA generally, and the adequacy of the safeguards. Seventeen consultees[14] also responded to our provisional proposal that the CJPA safeguards should apply to all device seizures: 13 agreed that they should;[15] and four disagreed.[16]

17.21 We consider, first, consultees' views on the operation of part 2 of the CJPA; secondly, the adequacy of the content of the safeguards in the CJPA; and, thirdly, the extent to which the safeguards ought to apply whenever electronic devices are seized pursuant to a search warrant.

The operation of the Criminal Justice and Police Act 2001

17.22 Some consultees took the view that there were no problems with part 2 of the CJPA,[17] although they did not provide reasons for this view. However, the majority of consultees did identify problems with the operation of the CJPA. For example, HMRC wrote that reform to part 2 of the CJPA would be welcomed. It was said that the statutory provisions in the Police and Criminal Evidence Act 1984 ("PACE"), the CJPA and other Acts have been overtaken by technological advances, especially the rise in cloud computing. Cases with such facts get shoe horned into statutory regimes that are not quite fit for purpose by citing the need for pragmatism.

17.23 Of those consultees who did raise issues with the CJPA regime, the criticism focused on two areas. The first related to the difficulty in ascertaining both when and how the regime applies. The City of London Police Economic Crime Academy argued that two problems stem from the single item theory. First, it can be difficult for investigators to know when the powers of seizure under the CJPA are engaged when devices are to be treated as a single item. Secondly, assuming that the seizure powers can be exercised, it can be difficult in practice to determine when recourse should be had to the CJPA powers of seizure in respect of digital devices.

---

13 Consultation Question 53. One member of the public; City of London Police Economic Crime Academy; Kent County Council Trading Standards; Birmingham Law Society; Northumbria Law School Centre for Evidence and Criminal Justice Studies; Independent Office for Police Conduct; The Law Society; Justices' Clerks' Society; Dijen Basu QC; Bar Council and the Criminal Bar Association; Metropolitan Police Service; National Crime Agency; Competition and Markets Authority; Whitehall Prosecutors' Group; Financial Conduct Authority; Serious Fraud Office; HM Revenue and Customs.

14 Consultation Question 57. Professor Richard Stone; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Birmingham Law Society; Northumbria Law School Centre for Evidence and Criminal Justice Studies; Independent Office for Police Conduct; The Law Society; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; Bar Council and the Criminal Bar Association; Metropolitan Police Service; National Crime Agency; Competition and Markets Authority; Financial Conduct Authority; Serious Fraud Office; HM Revenue and Customs.

15 Professor Richard Stone; Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; Kent County Council Trading Standards; Birmingham Law Society; Northumbria Law School Centre for Evidence and Criminal Justice Studies; Independent Office for Police Conduct; The Law Society; Magistrates Association; Dijen Basu QC; Bar Council and the Criminal Bar Association; Competition and Markets Authority; Metropolitan Police Service.

16 National Crime Agency; Financial Conduct Authority; The Serious Fraud Office; HM Revenue and Customs.

17 Kent County Council Trading Standards; Metropolitan Police Service.

17.24 The second criticism was that the CJPA regime placed an undue burden on the authorities in practice.[18] In particular, part 2 of the CJPA was described as onerous and restrictive, especially in cases with a high volume of material and where devices with relevant electronic data cannot be accessed. As a consequence, there was a clear aversion to the seizure of devices under the CJPA, except where necessary, due to the device containing, or being likely to contain, protected material.

17.25 The Whitehall Prosecutors' Group considered that the powers of seizure under the CJPA are necessary where an electronic storage device is known, or is credibly claimed, to contain material that the warrant cannot cover as a matter of law. This material will therefore consist of legally privileged material and other categories of material (such as excluded material) which may be exempt from seizure under the warrant.

17.26 The Serious Fraud Office ("SFO") explained that their preferred approach is to seize devices under the authority of the warrant and to rely on section 50 of the CJPA only if there is no other alternative. This will be most likely where a device contains, or may contain, legally privileged material.

17.27 Consultees acknowledged that robust procedures are required to ensure that legally privileged material is isolated from investigators and subject to review by independent counsel. However, outside protected material, the task envisaged in relation to the return of non-responsive data[19] was said to be too onerous.

17.28 The requirement to sift out and return non-responsive data after an "initial examination" under section 53 of the CJPA was said, in essence, to be an unduly rigid procedure adequately to interrogate data. Sifting on search terms as part of a single examination risks missing material which is not immediately responsive to search terms intended to identify relevant material. It was pointed out that the statutory caveat that property does not need to be returned if it is not reasonably practicable for it to be separated under section 53(3)(c) of the CJPA does not prevent the binary nature of the statutorily mandated single examination.

17.29 Instead, it was said that what is needed is the ability to conduct an iterative analysis of large volumes of data which accommodates further examination, such as the application of new search terms, in relation to fresh lines of enquiry or for disclosure purposes. The realities of the digital age were said to call, once protected material has been sifted out, for the rest of a pool of electronic material to remain available for further analysis, including for the purposes of disclosure.

17.30 The National Crime Agency also raised concern with the requirement of an "initial examination" where large volumes of data are contained on a device. They were particularly unclear about the proposed role to be played by the defendant's representatives in the initial examination under section 53(4) of the CJPA. They queried whether it is to participate actively in the sift or passively observe officers who carry out the sift. They pointed out that electronic material is often in large quantities – into the terabytes – and takes days to review.

17.31 The Whitehall Prosecutors' Group argued that the sifting process under the CJPA should be limited to those categories of material that cannot by law be covered by the warrant, rather

---

18 Whitehall Prosecutors' Group; Financial Conduct Authority; Serious Fraud Office; National Crime Agency.

19 This means electronic data that does not fall within the scope of the search warrant.

than identifying which files are not relevant. They noted that looking at every file is invariably impossible. Search terms and dip sampling will be needed.

17.32 The Whitehall Prosecutors' Group did accept that, outside the CJPA regime, investigators must devise a plan for examining electronic devices and considering their contents. Irrelevant material should be isolated or quarantined as a separate matter from the obligations arising under the CJPA.

17.33 The Financial Conduct Authority ("FCA") stated that there was no issue with the return of electronic storage devices containing discrete hard drives where there is no relevant material. However, they argued that once relevant material is found then the law should enable the entirety of the forensic image of the device to be retained or retention of the device itself should be authorised. Therefore, the CJPA should permit retention of the whole device, or a forensic image of the whole device, rather than having to justify the retention by referring to section 53(3) of the CJPA.

17.34 The justification for permitting the retention of entire devices with relevant evidence was that the development of forensic science means that methods which prevent access to relevant evidence may be circumventable in the future. Given the inaccessibility of the relevant evidence, it was said to rarely, if ever, be reasonably practicable to separate and return irrelevant or protected material from the relevant material.

The adequacy of the content of the safeguards relating to electronic material

17.35 Some consultees considered that the safeguards relating to the treatment of electronic devices once seized were adequate.[20] The majority of consultees, however, did not. Several consultees discussed the extent to which the safeguards apply in the context of the adequacy of the safeguards. We discuss this as a separate issue in the next section. At present we are concerned with the *content* of the safeguards and not their extent.

17.36 The Bar Council and the Criminal Bar Association ("CBA") observed that the law should address more clearly the *treatment* of information stored in digital devices once seized. Once a device is seized, a public authority will have access to large volumes of private, privileged and/or irrelevant information. Seizure is therefore only the first step in the exploitation of data. The next step is the sifting of data, and proper safeguards ought to apply to how that sifting is performed.

17.37 One possibility put forward by the Bar Council and the CBA, which we explained in at paragraph 15.53 above, was for a warrant to contain two parts: one part specifying the device that may be seized; the other part specifying the way in which the information contained on the device should be treated (on the assumption that the whole device will be seized). Investigators would therefore be encouraged to set out transparently how they intend to deal with the data, and the Crown Court should have the power to adjudicate on relevant disputes. It was further suggested that most disputes should be capable of agreement, especially if there were a clear and open Code of Practice which authorities were obliged to take into account. HM Revenue and Customs also suggested that a post-search protocol for the interrogation of seized or extraction data seizure and subject to judicial approval or scrutiny could be created. The Crown Court could then give directions in respect of the treatment of material.

---

[20] Kent County Council Trading Standards; Competition and Markets Authority; Independent Office for Police Conduct.

17.38 Other consultees discussed post-search protocols. The Whitehall Prosecutors' Group stated that, where a device has been seized, officers should devise a protocol for interrogating the device. It was said to often be prudent to share this protocol with the device owner and invite representations on the approach to be taken. It was suggested that, where there is dispute as to the correct approach then either the investigator, device owner, or other affected party should be able to apply to the Crown Court for directions as to how the electronic device and its contents, including copies, should be handled. Such directions should be capable of dealing with retention, return, deletion, copying, examination and the like. This way the correct approach could be divined and given judicial endorsement. HMRC also raised the possible role that could be played by a judicial authority in the treatment of electronic material. They saw merit in the Crown Court having the ability to give directions in respect of the handling or retention of data post-seizure or extraction.

17.39 As to the treatment of devices, it was pointed out by the Bar Council and the CBA that public bodies have a duty to devise and operate a system to isolate potential legally privileged material from bulk material lawfully in its possession.[21] They suggested that the same duty might be identified in relation to other protected material which the warrant cannot by law cover.

17.40 The Justices' Clerks' Society expressed the view that devices and data are removed from households for too long.[22] They proposed that devices should be interrogated *in situ* (ie copied on the premises) subject to strict rules where it is both practicable and will reduce inconvenience.[23] Although analysis in situ may not always be practicable, for example due to inaccessibility on the premises,[24] where it is possible it may be the least intrusive way of conducting the sift.[25]

17.41 Alternatively, where devices are seized, it was suggested that interrogation should take place within a tighter timescale.[26] One consultee argued that interrogation should take place within days rather than months given people's reliance on electronic devices.[27] Another consultee expressed the view that devices should only be seized where it is proportionate to do so and the sifting process is likely to be conducted within a reasonable time.[28]

17.42 A member of the public considered that greater emphasis should be placed on the return of electronic devices. In a similar vein, the Birmingham Law Society ("BLS") suggested a statutory framework to enable a person with an interest in seized property to request the provision of copies of particularised material with detailed information as to the storage location within a device. They gave the example of enabling the return of client lists, business to business data or accounting records required for taxation purposes. It was said that, at present, there is little onus on investigators to accept calls to provide copies of innocuous but important material seized in the course of a lawful search. The commonplace

---

21 *R (McKenzie) v Director of the Serious Fraud Office* [2016] EWHC 102 (Admin), [2016] 1 WLR 1308 at [34].

22 Justices' Clerks' Society.

23 Justices' Clerks' Society.

24 Senior District Judge (Chief Magistrate).

25 Justices' Clerks' Society.

26 Senior District Judge (Chief Magistrate).

27 Justices' Clerks' Society.

28 Northumbria Law School Centre for Evidence and Criminal Justice Studies.

seizure of items capable of holding any form of data may result in significant disruption to legitimate business interests and harm third parties not subject of the search or investigation.

17.43 The Law Society reiterated the two concerns regarding the limited applicability of the seize and sift regime above. They suggested that the CJPA should be amended to allow the reclassification of material if seized under a power other than section 50 of the CJPA when in fact it should have been as it contains protected material.

17.44 As mentioned above, the Bar Council and the CBA suggested that disputes concerning the treatment of devices would be assisted by a clear and open Code of Practice. Another consultee suggested a requirement to comply with a PACE electronic devices Code of Practice, which would be admissible in any proceedings in relation to which they are relevant.[29] HM Council of District Judges (Magistrates' Court) also made the suggestion of a Code of Practice in the context of formulating search protocols.

17.45 It was said that the Code of Practice could then be kept up to date with evolving technology, rather as the current Codes of Practice are kept up to date. In a similar vein, another consultee suggested that guidance could usefully discuss what is proportionate when seizing or extracting electronic material in specific circumstances.[30]

The extent to which safeguards ought to apply

17.46 The majority of consultees agreed with extending the procedures and safeguards in the CJPA to apply whenever electronic devices are seized pursuant to a search warrant. Most felt that ensuring the uniform treatment of electronic devices[31] would promote greater consistency and therefore simplicity.[32] It was accepted that the single item theory meant that the CJPA regime was being avoided in certain circumstances.[33] It was also said that there is a need for section 50 of the CJPA to expressly cover the seizure of electronic devices so that the protections under Part II of the CJPA are available to the owner of the device.[34]

17.47 It was also argued that to extend the CJPA safeguards would bring greater clarity to the process to protect legally privileged and excluded material.[35] Another consultee told us that extending the safeguards to the seizure of devices would dispense with the need for an artificial statement on the face of the warrant that it does not authorise seizure of items subject to legal privilege in order for the warrant to be lawful. BLS expressed the view that there were simply no good reasons for not making such an extension.[36]

---

29 Dijen Basu QC.

30 Northumbria Law School Centre for Evidence and Criminal Justice Studies.

31 Birmingham Law Society; Northumbria Law School Centre for Evidence and Criminal Justice Studies; Law Society.

32 Metropolitan Police Service.

33 Law Society.

34 Dijen Basu QC.

35 Independent Office for Police Conduct.

36 Birmingham Law Society.

17.48 Notwithstanding their agreement with the proposal, the Independent Office for Police Conduct made a series of additional observations.[37] They indicated that an extension of the safeguards should not affect the ability of investigators to challenge assertions of legally privileged material where appropriate.[38] They also noted the tension that an expansion of the CJPA regime might have with the disclosure regime, in particular in light of recent guidance from the Crown Prosecution Service ("CPS") in relation to investigative action and subsequent disclosure of electronic material.[39] Finally they told us that there is a need to ensure that the sift process does not preclude a search for evidence of criminality which may be stored in other parts of the device.[40]

17.49 Consultees also grappled with the exact powers which should trigger the CJPA regime. One consultee considered that the safeguards should apply where seizure is not only pursuant to the warrant itself but also powers exercised after the execution of the warrant.[41] Another suggested that the safeguards should also apply where material is produced under compulsion.[42]

17.50 The Bar Council and the CBA seemed to favour a more targeted extension. They suggested that the CJPA safeguards should be extended to cover (1) a seizure of an electronic device identified in a section 8 of PACE warrant which does not specify excluded material; and (2) electronic data or devices received in answer to a notice under section 2 of the Criminal Justice Act 1987.

17.51 Giving more detail on section 2 of the Criminal Justice Act 1987, the Bar Council and the CBA said that they were aware of a judicial review in which the claimant, a solicitor, challenged the seizure of an iPhone under a section 2 'here and now' notice. The basis of the challenge was that the device was bound to contain legally privileged material.[43] At present, the seizure powers under the CJPA would not apply in such a case.

17.52 Those who disagreed with extending the safeguards argued, essentially, that the CJPA, in its current form, is onerous and cumbersome. HMRC, for example, stated that applying the CJPA procedures to all seized devices could create logistical and cost issues which could hamper the ability of investigators to undertake their role effectively. The reasons why have been set out in the section above which details comments made by consultees on the operation of the CJPA regime.

---

37 Independent Office for Police Conduct.

38 Independent Office for Police Conduct.

39 Independent Office for Police Conduct. See https://www.cps.gov.uk/legal-guidance/disclosure-guidelines-communications-evidence.

40 Independent Office for Police Conduct.

41 Competition and Markets Authority.

42 Law Society.

43 The case was *Fisher v Serious Fraud Office*. The matter settled at court on the basis that the device would be considered by independent counsel, and no judgment was given.

A NEW LEGISLATIVE REGIME

Guiding principles

17.53 After considering consultees' responses, we are fortified in our view that a new legislative regime is required to govern the treatment of electronic material seized when executing a search warrant. The current law leads to an inconsistent application of safeguards under the CJPA. Even when the safeguards do apply, it is unclear how precisely they ought to operate in criminal investigations with large volumes of electronic material. This is partly owing to the provisions failing to appreciate the nature of modern electronic material, to the detriment of both investigators and those who are the subject of a search.

17.54 In redesigning and recalibrating the regime governing the treatment of electronic devices, we have been guided by a number of principles. These principles seek also to reflect the duties owed under human rights and data protection law in addition to law enforcement agencies' disclosure obligations under the Criminal Procedure and Investigations Act 1996. While an inherent tension exists between the principles we discuss, our recommendations seek to strike the right balance between the various competing interests.

17.55 The law governing the treatment of electronic material should place greater emphasis on the property and privacy rights of those whose devices and data are seized. State intrusion into an individual's privacy must be proportionate to the public interest in the investigation and prosecution of crime. A central component of this is minimising both the length of time that an individual spends without access to their electronic material and the amount of data that is viewed and retained by law enforcement agencies. The law should also require law enforcement agencies to be transparent in how they handle electronic material and provide suitable avenues for such agencies to be held accountable for the treatment of such material. The protections that apply should also do so as consistently as possible.

17.56 At the same time, this must be balanced with the realities of modern investigations involving electronic material. Any regime must not impose unrealistic or disproportionate demands on the investigator, inhibiting criminal investigations and causing unnecessary expense and delay. An appropriate degree of onus and control in carrying out the investigation must reside with the relevant law enforcement agency.

17.57 The law should also facilitate and permit the law enforcement agency to "press on" with the investigation and examine electronic material expeditiously. To this end, the regime should encourage the swift resolution of disputes, preferably outside of court, whilst discouraging unmeritorious challenges and delaying tactics. Accordingly, the regime must support the wider public interest in providing enforcement agencies with the tools to protect the public by detecting crime and prosecuting offending.

17.58 Another principle that we regard as crucial to achieving these aims is flexibility. There cannot be a one-size-fits-all approach to the treatment of electronic material. There is a multiplicity of factors all of which may require electronic material to be treated slightly differently when being examined. As technology and digital forensics continue to evolve, the framework should also be future-proofed as much as possible. In this regard, we consider that an important distinction is between the *method* of sifting electronic devices and the desired *result*.

17.59 This has informed our conclusion that, generally speaking, the most appropriate place for setting out the desired result of examining devices is in legislation, which should provide broad overarching and enduring duties. For example, the separation, return and/or deletion

of protected material, such as legally privileged material, should be a core duty of any such regime. Accordingly, the statutory regime ought to be prescriptive of the result, not the method.

17.60 On the other hand, we consider that the method by which this is achieved, such as by enlisting independent counsel and utilising search terms, is best set out in guidance and by law enforcement agencies supplying statutorily mandated post-search protocols. As new technology emerges, there is a need to have flexible guidance which is capable of being updated and for the approach adopted by law enforcement agencies to be tailored to the specific case. That a fact-specific approach is necessary is supported by observations made by the Supreme Court of New Zealand:

> The police will be entitled to search the computer in order to identify any relevant material, generally off-site. If relevant material is identified, downstream issues of some difficulty may arise, for example, as to how relevant material is to be preserved, what steps should be taken in relation to irrelevant material and how material is to be returned/made available to the suspect. We are not in a position to provide specific guidance on these matters in the abstract as much will depend on the circumstances of particular cases and the particular characteristics of the technology involved.[44]

17.61 We agree that the approach to be taken in respect of examining electronic devices will depend on the circumstances of the particular case, requiring flexibility in the means adopted. However, the end result to be achieved should be made clear in statute, but still subject to caveats of reasonableness where appropriate to prevent unreasonable constraints being placed on an investigator.

When the new regime should apply

The exercise of a relevant power

17.62 We conclude that the new regime should apply whenever electronic material is seized following the execution of a search warrant. This would mean that the regime is as broad as possible under our terms of reference. Uniform provisions in these circumstances would provide clarity, consistency of approach and greater protections to individuals who are subject to powers of seizure or compulsion. Given that article 8 of the ECHR will be engaged in all instances of device seizures or data extraction, safeguards which provide procedural protections to those with an interest in the property should apply consistently. Another practical benefit of uniform provisions is that it would obviate the need, noted by the Law Society above, to reclassify material where protected material is subsequently identified and procedural safeguards do not apply.

17.63 To ensure clarity and consistency, we consider that the regime should be triggered by an electronic device or electronic data being acquired through the exercise of a relevant power of seizure or production following the execution of a search warrant. We use the phrase "relevant power" because we consider that a definitive list of seizure and production powers to which the safeguards apply would bring about the maximum degree of clarity. The inclusion of powers of production would also address the anomaly raised by the Law Society, Bar Council and the CBA that such powers do not currently fall within the CJPA regime.

---

44 *Dotcom v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745 at [194].

17.64 Thought will also have to be given to the interplay that any new regime has with other regimes, with an awareness of their respective contours. Investigative powers regimes may have their own tailored suite of safeguards governing the treatment of material obtained in the exercise of specific powers. By way of example, all material obtained under the authority of an equipment interference warrant must be handled in accordance with safeguards imposed under the Investigatory Powers Act 2016, as supplemented by a code of practice,[45] and approved by an issuing authority. Electronic material may be acquired through exercising multiple powers, which may result in the application of safeguards from multiple regimes.

Issues caused by a new regime

17.65 Even by making a recommendation that the regime applies to relevant powers exercised in respect of electronic material following the execution of a search warrant, issues of incoherence and unfairness may potentially arise.

Limited to relevant powers exercised following the execution of a search warrant

17.66 The first issue is the risk of incoherence if a new regime only applies when a relevant power is exercised *following the execution of a search warrant*. Production powers and the CJPA regime apply in cases where an individual is on premises other than under the authority of a warrant. As a result, where a relevant power is exercised, but a law enforcement officer is not on premises under the authority of a warrant, the safeguards would not apply.

17.67 The difference between the application of safeguards based on whether an investigator is on premises under the authority of the warrant could be said to be arbitrary. Arguably, stronger safeguards should apply when an investigator is not on premises under the authority of a search warrant as there has been no independent judicial authorisation granting lawful entry.

17.68 Unfortunately, this is an inevitable effect of our terms of reference being limited to search warrants. We are unable to make recommendations that would substantially affect law enforcement powers more generally. That being said, we observe that it would be sensible for a clear regime to apply consistently across law enforcement powers. We discuss this issue in the next chapter, in which we recommend a wider review of the treatment of electronic material in criminal investigations.

17.69 Big Brother Watch has also questioned whether our proposals in respect of the treatment of electronic material would extend to complainants whose devices are examined.[46] Again, owing to our terms of reference, they would not. There are also strong arguments that bespoke safeguards should apply when complainants' devices are acquired by law enforcement and not simply a relevant power of seizure or production. This, too, is discussed in the next chapter which concerns a wider review of the treatment of electronic material in criminal investigations.

Limited to relevant powers exercised in respect of electronic material

17.70 The second issue is the risk of incoherence if a new regime only applies when a relevant power being exercised *in respect of electronic material*. The CJPA regime applies to "property", and therefore to hard copy material as well as electronic material. Arguably, our

---

45 Home Office, *Equipment Interference Code of Practice* (March 2018) paras 9.1 to 9.84.

46 Big Brother Watch, *Digital strip searches: The police's investigations of victims* (July 2019) p 14 to 15.

new regime should also extend to hard copy material. This is for the same reason as identified above: that arbitrary results may be produced by limiting the regime in this way.

17.71 This arbitrariness can be highlighted by considering that large volumes of hard copy documents may be seized and then scanned electronically into a database, therefore becoming intermixed with electronic data. There will also be crossovers between electronic and hard copy material: for example, a hard copy record of a private key may provide access to a digital wallet. An infringement of privacy and property rights also occurs irrespective of whether the material acquired by the state is in hard copy or electronic form. Further, the criticisms of the CJPA, such as the blunt nature of carrying out an initial sift and non-applicability of the safeguards where material is produced, also apply to hard copy material. From a practical point of view, some of the recommendations that we make could also apply equally to hard copy material with minimal, if any, modification.

17.72 Electronic material is unique in its nature. It is also heterogeneous: there are clear differences between a Word document and a cryptoasset. These characteristics call for a more nuanced framework. Accordingly, there will be some rules that will have to be tailored, and could only therefore apply, to electronic material. At the same time, an efficient regime should also be in place in respect of hard copy material. Consideration should therefore be given to expanding any new statutory regime to include:

(1) electronic material acquired during criminal investigations in instances other than following the execution of a search warrant; and

(2) material that is not an electronic device or stored in electronic form.

17.73 Finally, as a matter of drafting, in order to limit statutory amendment of the CJPA to search warrants in the way in which we described, either a new section or numerous exceptions would need to be added. Again, this partial amendment of the CJPA risks creating an unwieldy and unnavigable statute. As the rules that govern the treatment of electronic material are contained in a number of overlapping statutory regimes, partial amendment would likely occur in other regimes such as PACE. It is for this reason, among several others, that we recommend a wider review of the acquisition and treatment of electronic material in criminal investigations so that issues such as this will not occur.

Recommendation 54

17.74 We recommend the introduction of a new statutory regime governing the treatment of electronic material. The regime ought to apply whenever a relevant power of seizure or production is exercised in respect of electronic material following the execution of a search warrant.

The duty to provide details of what was seized

17.75 As discussed in our section on relevant legal regimes in Chapter 14,[47] when an investigator seizes material, depending on the power of seizure, there may be a duty to provide details of

[47] See paragraph 14.75 above.

what has been seized. This duty is automatic if seizure is made under the CJPA,[48] or only following a person's request if seizure is made under PACE.[49] The courts have held that, where electronic devices are seized, the duty under PACE does not extend to the provision of a composite item by item breakdown of the contents of an electronic device.[50] Similar reasoning would likely apply to the CJPA.

17.76 Where electronic material is obtained following the execution of a search warrant, we consider that there should be a single rule governing the provision of details of what was seized. It is our view that the duty should only be triggered when a request is made for details of what was seized and not automatically upon seizure. In some cases, details will not be sought and so an automatic duty to provide such details would lead to unnecessary expense. We also take the view that, adopting the wording of section 21(2) of PACE, the action must be performed within a reasonable time from the making of the request for it.

17.77 To counterbalance this, it should be made clear to a person affected by a search warrant that the right to request details exists. A suitable place for this would be in the notice of powers and rights, which we recommend placing on a statutory footing at Recommendation 32.[51]

17.78 On the topic of the notice of powers and rights, for convenience and to save time, we also consider that the notice of powers and rights could cover most of the points that are required to be in a written notice under section 52 of the CJPA when an investigator seizes property under sections 50 or 51 of the CJPA.

17.79 In terms of level of detail, we have concluded that the most desirable rule would be for law enforcement agencies to be required to provide as specific a description of what was seized as reasonably practicable. We have reached this conclusion for the following reasons. First, the starting point of the rule is that law enforcement agencies should be as transparent as possible regarding what has been seized.

17.80 Secondly, the inclusion of a test of reasonable practicability would prevent unreasonable demands being placed on investigators. We note that a similar approach is taken in the United States, where the Federal Rules of Criminal Procedure do not address the question of whether the inventory required under rule 41(f)(1) should include a description of the electronic data stored on seized devices. The commentary to the rule provides:

> Where it is impractical to record a description of the electronically stored information at the scene, the inventory may list the physical storage media seized. Recording a description of the electronically stored information at the scene is likely to be the exception, and not the rule, given the large amounts of information contained on electronic storage media and the impracticality for law enforcement to image and review all of the information during the execution of the warrant.

17.81 Thirdly, the proposed rule would be flexible. This is all the more important as technology evolves – both the capability of digital forensic tools and the volume and storage of data – which requires any statutory rule to be enduring. The Code of Practice could then expand on

---

48 Criminal Justice and Police Act 2001, s 52(1).

49 Police and Criminal Evidence Act 1984, s 21(1).

50 *Business Energy Solutions Ltd v Crown Court at Preston* [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887.

51 See paragraph 7.179 above.

the meaning of what may be reasonably practicable. The proposed rule would also be able to account for the factual differences between, say, seizing electronic devices with a very large storage capacity and targeted copying of a handful of files from an electronic device.

17.82 Fourthly, the inclusion of a test of reasonableness should protect law enforcement agencies from unmeritorious challenges or where the only purpose of making a request is to impede the investigation. For example, where law enforcement agencies have copied an entire device without physical seizure, it will be possible for individuals to see the details of what has been copied by viewing their devices.

17.83 Fifthly, we recommend further below a mechanism to request more specific details of the electronic material that has been seized or copied. This would provide an important failsafe mechanism to ensure accountability, which is particularly important given the degree of discretion that would be afforded to law enforcement agencies by our proposed rule.

17.84 By way of final observation, we note that the proposed rule could apply equally to hard copy documents. For example, in circumstances where filing cabinets or folders are seized, depending on the size of the objects concerned, it may or may not be reasonably practicable to list the contents of the container rather than to list the container itself.

Recommendation 55

17.85 We recommend that, under the new statutory regime in Recommendation 54 above, an investigator be required to provide as specific a description of what was seized as reasonably practicable to a person with an interest in the electronic material within a reasonable time from the making of the request for it.

The duty to provide details of action taken in respect of electronic devices on premises

17.86 The second statutory duty that we considered is a duty to provide details of action taken in respect of electronic devices on premises. At present, there is no legal requirement for investigators to document what procedures were adopted when examining an electronic device. Therefore, while an investigator may be required to provide details of what electronic devices were copied, there is no legal requirement to detail what steps were taken in copying the device.

17.87 The only statutory requirement with some similarity would be under section 73 of the Explosives Act 1875. This requires a report to be provided to the Secretary of State detailing actions taken on premises where written authority to enter premises is granted by a superintendent rather than judge.[52]

17.88 Code B of PACE, however, requires an officer in charge of the search to make or have made a search record,[53] to be kept at a police station,[54] which includes matters such as whether force was used and details of any damage caused.[55] Code B also provides that a

---

52 See also slightly less similarly the Terrorism Act 2000, sch 5, para 15(3).

53 Code B, para 8.1.

54 Code B, para 9.1.

55 Code B, para 8.1(viii) and (ix).

record of the action taken should be made on the premises search record, including the grounds for refusing an occupier's request for a person to witness the search.[56] The third principle of the ACPO guidelines also provides that an audit trail or other record of all processes applied to digital evidence should be created and preserved.[57]

17.89 The efficacy of a duty to provide details of action taken in respect of electronic devices on premises was considered by the New Zealand Law Commission and Ministry of Justice in their joint review of the Search and Surveillance Act 2012. In their issues paper, they wrote:

> One option for reducing the amount of irrelevant material that is seen during digital searches would be for the Act to require a person undertaking a search of a computer or other data storage device to produce a record of their search procedure. That record would then be available on request to the owner of the computer or device searched. This option has three advantages. First, it would ensure that the person conducting the search is accountable for each step taken in the process. Knowing that someone may check up on the procedure followed should help ensure that the search is conducted within lawful limits. Second, it would provide a defendant in subsequent criminal proceedings with the means of checking whether or not evidence from the search used against him or her was lawfully obtained. Third, even if criminal proceedings did not eventuate, it would enable the person who owned the computer or device to know the extent to which his or her privacy had been interfered with and make a complaint to the Privacy Commissioner, where appropriate.[58]

17.90 The New Zealand Law Commission and Ministry of Justice's final report, however, noted that the consultation responses were divided:

> Of particular note were the submissions from agencies that employ specialist digital forensic staff. Those agencies advised that these specialists are always mindful of the need to conduct targeted searches, for principled reasons and also as a result of time and resource constraints. They observed that specialists already make technical notes of the steps involved but argued that creating a more accessible detailed record in every case would be impractical. They suggested that such a requirement could significantly impede investigations given the large number of files that may need to be reviewed and the large number of keyword searches and other filters that may need to be used to find those files. In light of those observations, we consider that a record-keeping requirement is not appropriate in cases where the search is conducted pursuant to a search warrant or in an urgent situation. If there is a warrant, there is scope for case-specific conditions to be put in place. If the situation is urgent and is premised on responding to an emergency rather than collecting evidence, a recordkeeping requirement would be unduly onerous. We do, however, think that a record-keeping requirement should attach to warrantless Internet searches.[59]

17.91 We have reached the conclusion that a duty to provide details of action taken in respect of electronic devices on premises would be desirable in this jurisdiction. We agree with the New Zealand Law Commission and Ministry of Justice that such a duty would provide

---

56 Code B, para 6.11.

57 ACPO, *Good Practice Guide for Digital Evidence (Association of Chief Police Officers* (2012) para 2.1.3 and p 31.

58 New Zealand Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* / *Ko te Arotake i te Search and Surveillance Act 2012*, NZLC IP40 (2016) paras 6.42 and 6.43

59 New Zealand Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012* / *Ko te Arotake i te Search and Surveillance Act 2012*, NZLC R141 (2017) paras 12.68 and 12.69.

greater accountability and be of benefit to those affected by a search warrant, who may wish to complain of action taken on premises. From an international law perspective, we also consider that it would be an important safeguard where remote search and seizure has taken place.

17.92 We also regard the duty as justified on the basis of the heightened privacy considerations that are engaged when electronic devices with huge volumes of irrelevant and sensitive data are searched, copied and seized. The duty would also be of clear benefit where no occupier was present at the time of the search, as there would otherwise be no way of knowing what action has been taken in respect of electronic devices. We also regard the duty as having particular value given that we have recommended express powers to search electronic devices on premises.

17.93 The issue for us is therefore whether these benefits would be outweighed by the burden placed on law enforcement agencies by recommending such a duty. In our view, the benefits would not be outweighed. The duty would be placing on a statutory footing that which is already best practice, with a slight extension to provide the accessible record produced to a person with an interest in the electronic device.

17.94 We have also reached this conclusion having arrived at a formulation of the duty that would require details of action taken to be provided in as much detail as practicable and supplied only on request. This would afford an appropriate degree of latitude to investigators and would account for urgent cases where circumstances do not allow for detailed notes of the action taken. The right to make a request should be made clear in the notice of powers and rights, which we recommend placing on a statutory footing at Recommendation 32.[60] Once again, we regard the proper place for expansion of the duty to be in the Code of Practice recommended at the end of the chapter.

Recommendation 56

17.95 We recommend that, under the new statutory regime in Recommendation 54 above, an investigator be required to provide details of what action was taken in respect of electronic devices on premises, in as much detail as practicable, to a person with an interest in the electronic device within a reasonable time from the making of the request for it.

The duty to provide details of how electronic material will be examined

17.96 In Chapter 15, we considered whether there ought to be a statutory duty for investigators to devise pre-search protocols for approval by the issuing authority when applying for a search warrant in respect of electronic material.[61] We reached the view that a requirement to provide pre-search protocols would be undesirable. In summary, this was because of the number of unknown variables as to what electronic material investigators may face when executing a search warrant. As a result, investigators would have to produce vague protocols that would offer little protection for occupiers, may unreasonably constrain investigations and would probably require extensive revision post-seizure.

---

60 See paragraph 7.179 above.

61 See paragraphs 15.67 to 15.82 above.

17.97 Several consultees suggested a requirement to provide post-search protocols. On the whole, we see merit in a person having the right to request information from a law enforcement agency who has seized or copied electronic material on how their electronic device(s) or data is to be treated. First, post-search protocols would overcome the problems that we identified with pre-search protocols. Law enforcement agencies will be able to be specific in how the electronic material will be examined, which will lead to greater transparency and be of more use to occupiers.

17.98 Secondly, we do not consider that a requirement to produce post-search protocols on how electronic material is to be treated would be unduly burdensome. A tailored data examination strategy should already be devised by law enforcement agencies before electronic material is examined.[62] The Whitehall Prosecutors' Group also agreed that, where a device has been seized, officers should devise a protocol for interrogating the device. Additionally, we do not consider that the duty to provide post-search protocols should be engaged automatically upon seizure or copying. As with the other rights discussed above, we consider that the right to request post-search protocols should be made clear in the notice of powers and rights, which we recommend placing on a statutory footing at Recommendation 32.[63] To the extent that the duty to provide post-search protocols does place a burden on investigators, we regard this as justifiable and a fair trade-off for investigators being empowered to seize entire electronic devices.

17.99 Third, post-search protocols would have a practical benefit for both law enforcement agencies and those with an interest in the electronic material. We recommend below a mechanism by which law enforcement agencies and those with an interest in electronic material can apply to the Crown Court for a determination regarding the treatment of the material, a suggestion with which there is broad agreement amongst law enforcement agencies and those who defend and represent the interests of individuals affected by warrants. This means that investigators would be able to obtain judicial approval to examine electronic material in the terms set out in the post-search protocol and therefore press on with the investigation at hand. Similarly, a person with an interest in the electronic material would be able to challenge the proposed treatment of the material in the post-search protocol, with the Crown Court adjudicating on the dispute. Accordingly, the post-search protocol would be capable of judicial approval and scrutiny.

17.100 The Code of Practice recommended at the end of the chapter should contain a detailed discussion on formulating post-search protocols and the matters that should be included.[64]

---

62 ACPO, *Good Practice Guide for Digital Evidence (Association of Chief Police Officers* (2012) p 36.

63 See paragraph 7.179 above.

64 See *R v Bater-James* [2020] EWCA Crim 790 at [88] in which Fulford LJ gave guidance on how the review of a witness's electronic communications should be conducted, highlighting that a fact-specific approach is required.

Recommendation 57

17.101 We recommend that, under the new statutory regime in Recommendation 54 above, an investigator be required to provide protocols setting out how electronic material is to be examined to a person with an interest in the property within a reasonable time from the making of the request for it.

The duty to return electronic devices

17.102 In the light of consultation responses, we have concluded that a new statutory regime should include an explicit duty to return electronic devices that are seized. If electronic devices are seized, electronic data should therefore be copied off-site and dealt with in accordance with the duties discussed in the sections which follow.

17.103 The creation of a duty to return electronic devices is justified owing to the acute impact that the seizure of a device has. Electronic devices, particularly mobile phones and laptops, now contain an almost limitless amount of personal data concerning every aspect of our lives and other people's lives that will be irrelevant to a criminal investigation. They are used for performing activities that are integral to our social, academic and work lives. It is not difficult to envisage how even short periods of time without access to electronic devices can have a catastrophic impact on these three activities:[65] electronic devices are used to socialise and plan events with friends and family; for entertainment and gaming; for managing finances; to work and run businesses; and to prepare for important educational assessments.

17.104 While we have little hesitation in recommending a statutory duty to return electronic devices, the precise terms of the duty require more careful consideration. In particular, should a fixed period be laid down by which time electronic devices must be returned? If so, what should the period be? Should there be a mechanism for law enforcement agencies to retain electronic devices beyond the maximum period, or for individuals to request return of electronic devices sooner?

17.105 The 2009 amendment to the Unites States Federal Rules of Criminal Procedure did not include a fixed period by which time electronic devices were to be returned. The rationale behind this approach is contained in the committee notes, which provide:

> While consideration was given to a presumptive national or uniform time period within which any subsequent off-site copying or review of the media or electronically stored information would take place, the practical reality is that there is no basis for a "one size fits all" presumptive period. A substantial amount of time can be involved in the forensic imaging and review of information. This is due to the sheer size of the storage capacity of media, difficulties created by encryption and booby traps, and the workload of the computer labs. The rule does not prevent a judge from imposing a deadline for the return of the storage media or access to the electronically stored information at the time the

[65] See most recently *R v Bater-James* [2020] EWCA Crim 790 at [78] in which Fulford LJ wrote that "the loss of [an electronic] device for any period of time may itself be an intrusion into [a person's] private life, even apart from considerations of privacy with respect to the contents."

warrant is issued. However, to arbitrarily set a presumptive time period for the return could result in frequent petitions to the court for additional time.[66]

17.106 We are alive to the current practical realities that face law enforcement agencies. As we explained at paragraph 14.104 above, there is a significant backlog of electronic devices awaiting examination.[67] Waiting times have been reported as long as 9 months,[68] and even up to a year before electronic devices are imaged or analysed.[69] Although in some respects an inevitability owing to resources, we consider such lengthy delays to be unacceptable.

17.107 On careful reflection, we consider that the duty should be for electronic devices to be returned as soon as reasonably practicable, without laying down a maximum period of retention. Electronic devices should be retained only for such time as is strictly necessary. However, in our view, a fixed period would fail to account for the practical realities of digital investigations, operate arbitrarily and lead to frequent applications for continued retention.

17.108 We also accept the concerns raised by the FCA that electronic devices, and therefore relevant evidence contained therein, may be inaccessible at the present time, but capable of being accessed at a later date through technological advancement. That said we would stress that whether it is, in all the circumstances of the case, proportionate to retain an inaccessible device will be very much fact dependent.[70]

17.109 In reaching this conclusion there is of course a risk that electronic devices will remain retained for unacceptably long periods of time, which would seem to render the duty of little benefit. The principal safeguard in such instances is for an application to be made for the return of electronic devices, a mechanism that we recommend later in this chapter. Other safeguards include the power to search electronic devices on-site, which we recommended at Recommendation 50,[71] and for the Code of Practice (which we recommend at the end of this chapter) to encourage the copying of electronic data on-site rather than seizure.

Recommendation 58

17.110 We recommend that, under the new statutory regime in Recommendation 54 above, an investigator be required to return electronic devices following seizure on premises as soon as reasonably practicable.

The duty to return and/or delete protected electronic material

17.111 Where electronic devices are seized under the CJPA, section 53 of the CJPA mandates that an initial examination is carried out as soon as reasonably practicable after the seizure

---

66 Federal Rules of Criminal Procedure (Unites States), r 41 (Committee Notes on Rules—2009 Amendment).

67 https://www.thetimes.co.uk/edition/news/police-struggling-to-clear-evidence-backlog-of-12-000-devices-rpmhmfnpt.

68 Big Brother Watch, *Digital strip searches: The police's investigations of victims* (July 2019) p 18.

69 https://www.policeprofessional.com/news/forensic-delays-deeply-concerning-as-case-backlog-grows/ and HM Inspectorate of Constabulary, *Online and on the edge: Real risks in a virtual world* (2015) p 6.

70 See *Love v National Crime Agency* (19 February 2019) (unreported) for a case in which the magistrates' court was tasked with deciding whether electronic devices seized as part of an ongoing criminal investigation ought to be returned to the owner following an application for the return of property under the Police Property Act 1897, s 1.

71 See paragraphs 15.193 and 15.194 above.

to identify and return any material that the investigator was not entitled to seize. Sections 54 and 55 of the CJPA also mandate that legally privileged, excluded and special procedure material (ie protected material) must be returned as soon as reasonably practicable after seizure unless it is not reasonably practicable for the material to be separated without prejudicing the property.

17.112 In our new statutory regime, we have concluded that law enforcement agencies should be required to return and/or delete any protected material that a warrant cannot cover as a matter of law. This will always cover legally privileged material and, depending on the investigatory power, very likely excluded material and may include special procedure material. In our view, this duty should not have to be fully discharged before the remainder of the electronic data can be examined. The first duty of an investigator following the seizure or copying of electronic material should be, however, to isolate protected material, but not necessarily to have completed the process by which it will be returned and/or deleted. We have reached this conclusion because the process of seeking independent counsel's advice and determining which material attracts legal professional privilege in particular can take some period of time. Once potentially privileged material has been isolated and provided to independent counsel, the examination of non-privileged material should not have to be delayed pending the receipt of the advice of independent counsel on what material attracts legal privilege.

17.113 Beyond stating this overarching duty in statute, we do not consider it desirable to prescribe the method by which it is to be achieved: it will be a fact-sensitive matter that should be addressed in post-search protocols taking into account the Code of Practice recommended below. For example, we were informed that it is commonplace in investigations into serious and complex crime for the quantity of material gathered to number in the region of tens of millions of documents. Innovative solutions are required and must be permitted under any statutory regime. It is for this reason that there are two aspects of the current regime under section 53 of the CJPA that we consider should not be included in any new statutory regime.

17.114 First, we agree with investigative agencies that the vague statutorily mandated "initial sift" under section 53 of the CJPA should be removed. In our view, the duty does not accord with the reality and complexity of investigations with large volumes of electronic material. It also risks the inadvertent sifting out of relevant material. In the future, the use of technology to sift large volumes of material will increasingly feature artificial intelligence, including technology assisted review based on algorithms and machine-based learning. This will require an iterative process where search terms are honed and carried out alongside human review, meaning that there will be no single instance of review.

17.115 An initial sift may therefore be *one* method of achieving the desired result of sifting out protected and non-responsive[72] material, but it should not be mandated, as an iterative process may be more appropriate under certain circumstances.[73]

17.116 Secondly, we do not consider that the need to have due regard to the desirability of the presence of a person or their representative during the initial sift should be set out in statute.

---

[72] This means material that does not correspond with the terms of the warrant and so is not authorised to be searched for or seized under the authority of the warrant.

[73] This conclusion has also been influenced by our attendance at a section 59 CJPA hearing at Blackfriars Crown Court, in which there was a dispute regarding what conduct must be undertaken to satisfy the statutory initial sift requirement.

We note that it is not mandated by section 53(4) of the CJPA but instead only due regard need be had to its desirability: it is therefore an optional part of the procedure which we agree will be impracticable in cases with large volumes of electronic material. Moreover, we regard it as better expressed in a Code of Practice given that it concerns the method by which sifting occurs rather than what the result of the sift should be.

Recommendation 59

17.117 We recommend that, under the new statutory regime in Recommendation 54 above, an investigator be required to return and/or delete protected electronic material as soon as reasonably practicable.

The duty to return and/or delete non-responsive electronic material

17.118 The seizure or copying of electronic devices results in law enforcement agencies acquiring large volumes of material that is non-responsive to the warrant and irrelevant to a criminal investigation. Even where electronic devices are returned, investigators may have retained entire copies of the devices. We make several recommendations in this report which aim to reduce the volume of non-responsive and irrelevant data acquired by law enforcement agencies, however, the seizure or copying of large volumes of electronic data, and therefore non-responsive and irrelevant data, will be inevitable in many cases.

17.119 Under the CJPA, anything found after an initial examination which cannot lawfully be retained must be separated and returned. The duty to "return" non-responsive material not within the scope of the original warrant includes an obligation to delete copied electronic data.[74] The duty to return material applies to each individual copied file as it does to the original device.[75] Seized property can be retained under the CJPA if it is responsive to the warrant (section 53(3)(a)), evidence in relation to, or obtained in consequence of, an offence and may be destroyed (section 53(3)(b)) or property that it is not reasonably practicable to separate (section 53(3)(c)). This last exception means that an investigator need not necessarily undertake the Herculean task of segregating non-responsive electronic data, even if technically possible to do so.[76]

17.120 We conclude that the essence of this statutory duty should be replicated in a new regime. In particular, there should be a statutory duty to, so far as is reasonably practicable, return and/or delete non-responsive electronic material. The reference point for determining whether material is responsive would be the second part of the warrant specifying the information on the electronic device(s) that is sought, which we recommend at Recommendation 48 above.[77]

17.121 We agree with the Whitehall Prosecutors' Group that, once protected material has been isolated, the rest of the material should be unlocked and available for examination. Therefore, investigators will no longer be under a statutory duty to identify and isolate non-

---

74 *Business Energy Solutions Ltd v Crown Court at Preston* [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [83].

75 *Business Energy Solutions Ltd v Crown Court at Preston* [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [75].

76 *Business Energy Solutions Ltd v Crown Court at Preston* [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [98].

77 See paragraph 15.118 above.

responsive material as part of a single examination before being able to examine the remaining pool of material. The duty to return and/or delete non-responsive electronic material would of course remain engaged.

17.122 The duty should also recognise that non-responsive and irrelevant data cannot, and should not, be sifted out in one fell swoop. An investigator may need to retain electronic data so that provenance and continuity can be established if it is challenged.[78] In the event of a prosecution, further searches are also likely to be required to comply with the prosecutor's duties under the CPIA, particularly after service of defence statements when the true issues in the case are liable to crystallise. New lines of enquiry may emerge that point away from a suspect and require further analysis of retained electronic data. The duties on the prosecutor under the CPIA to keep disclosure under review therefore means that it may be necessary to carry out searches on more than one occasion.[79] For these reasons, a wide pool of electronic data may need to be retained.

17.123 We see several benefits in a new regime being recalibrated in this way. The duty would align with the CPIA regime discussed in Chapter 14 so that investigators will be able to advance the investigation by identifying relevant material. In line with our guiding principles, this would facilitate and permit law enforcement agencies to "press on" with the investigation and examine electronic material expeditiously. We therefore agree with the observations made by the Whitehall Prosecutors' Group and SFO that, once protected material has been sifted out, there ought to be scope for the rest of a pool of electronic material to remain available for further analysis, including for the purposes of disclosure.

17.124 The method by which non-responsive material is identified, segregated, returned and/or deleted should, as with protected material, be addressed in post-search protocols taking into account the Code of Practice recommended below.

Recommendation 60

17.125 We recommend that, under the new statutory regime in Recommendation 54 above, an investigator be required to return and/or delete non-responsive electronic material, so far as is reasonably practicable.

Application regarding the treatment of property

17.126 At Recommendation 57 above, we recommend that an investigator should be required to provide protocols setting out how electronic material is to be examined to a person with an interest in the property within a reasonable time from the making of the request for it. We point out at paragraph 17.99 above that post-search protocols would have a practical benefit for both law enforcement agencies and those with an interest in the electronic material in that it would be capable of judicial approval and scrutiny.

---

78 *Business Energy Solutions Ltd v Crown Court at Preston* [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [111].

79 *R v R* [2015] EWCA 1941 at [38], [50] and [59] by Sir Brian Leveson P. See also *R v Bater-James* [2020] EWCA Crim 790 at [88] in which Fulford LJ stated, on the question of how the review of the witness's electronic communications should be conducted, that investigators will need to adopt an incremental approach.

17.127 Under the current law, there is no mechanism to apply to the Crown Court to approve of, or adjudicate on disputes regarding, the proposed treatment of electronic material. The Crown Court has a power under section 59(5) of the CJPA to give directions in respect of property. However, at present this requires either an underlying application for the *return* of property[80] or for seizure to have been made pursuant to sections 50 or 51 CJPA[81]. Therefore, the Crown Court has no jurisdiction to give directions where seizure is made under a different power. A new power would therefore be necessary.

17.128 In our view, a person with an interest in electronic material (ie either an investigator or an owner) should be able to apply to the Crown Court for a judge to approve of or adjudicate on disputes regarding the way in which the investigator intends to examine electronic material. This would provide benefits to both investigators and those who own the electronic material.

17.129 For investigators, it would permit a tailored data examination strategy to be devised and approved so that the law enforcement agency can press ahead with the criminal investigation. To this end, there is cross-over with our discussion in respect of legally privileged material in Chapter 11. In our Consultation Paper, we proposed a procedure to enable the swift identification and segregation of privileged material.[82] This was by enabling an investigator to apply to the Crown Court to require an individual to identify legally privileged material. However, we conclude in Chapter 11 that there should instead be a procedure by which a Crown Court judge can adjudicate on disputes and claims regarding legal privilege. We discuss in that section how our policy aims can be achieved by the amendment discussed here.

17.130 For example, an investigator would be required to provide details on request of how legally privileged and protected material will be dealt with. The onus would be on the investigator to devise search protocols. The owner would be able to challenge the way in which the law enforcement agency states that it intends to deal with material under the search protocol. In support of an iterative process, the investigator would be able to issue a response. If a dispute remains, the occupier would be able to apply to the Crown Court to adjudicate on how protected material should be dealt with.

17.131 There are a number of benefits to individuals being permitted to challenge the way in which law enforcement agencies propose to examine their electronic material. Given the discretion afforded to investigators under the statutory duties recommended, it would ensure law enforcement agencies are accountable for their actions. There are clear instances in which there would be a public interest in an individual challenging the treatment of their electronic material, such as where electronic material may be lost or destroyed. As we explained at paragraph 14.106 above, one of the ways in which electronic data may be extracted from a device is through a “chip off procedure”. This may have the effect of irreversibly damaging an electronic device.

17.132 In our view, there are clear benefits to providing the Crown Court with a broad supervisory jurisdiction over the treatment of electronic material. This will assist in achieving practical justice and resolving disputes in a way that may avoid more expensive and lengthy litigation. The court will be able, on a case by case basis, to make appropriate directions. We are conscious that a flood of applications would itself cause expense and delay. Applications

---

80 Criminal Justice and Police Act 2001, s 59(5)(a).

81 Criminal Justice and Police Act 2001, s 59(5)(c).

82 Consultation Question 43.

could also be used as a means to delay examination. It is unclear how quickly a Crown Court could list and determine an application, particularly in light of the huge trial backlog which has been exacerbated by COVID-19. To that end, we agree with the Bar Council and the CBA that a Code of Practice would assist with resolving disputes without recourse to litigation.

Recommendation 61

17.133 We recommend that, under the new statutory regime in Recommendation 54 above, a person with an interest in electronic material be able to apply to the Crown Court for a judge to approve of or adjudicate on disputes regarding the way in which the investigator intends to examine electronic material.

Application for the return and/or deletion of electronic material

17.134 There are a number of provisions under which the return of material can be sought.[83] We conclude that a new regime should include a clear set of rules governing applications for the return and/or deletion of electronic material.

17.135 In our view, a person with an interest in electronic material ought to be able to apply to the Crown Court for the return and/or deletion[84] of particular electronic data or return of an electronic device on the grounds that either:

(1) the electronic material is reasonably required by the person with an interest in it; or

(2) continued retention by an investigator of the electronic material is not necessary.

17.136 There would be a number of benefits to this procedure. First, given that our recommendation regarding the return of electronic devices and non-responsive data affords a degree of discretion to law enforcement agencies, the right to make an application for the return and/or deletion of electronic material would ensure accountability. For example, while law enforcement agencies state that they may provide important files requested by an owner, the crucial word is *may*: a means of judicial oversight would ensure that privacy and property rights are respected post-seizure.

17.137 Secondly, we consider that the right to make an application is justified given the detrimental effects that can result from being without access to electronic material and heightened privacy implications that we discussed at paragraph 17.103 above. Thirdly, the procedure would permit practical justice to be achieved in each case with a set of rules that accounts for the specific nature of electronic material.

17.138 We again acknowledge the floodgates argument and risk of unmeritorious applications which seek to prejudice the criminal investigation. Mechanisms could be built in to address this. For example, a condition could be inserted that, where an application is refused, a

---

83 Criminal Justice and Police Act 2001, s 59(2); Police (Property) Act 1897, s 1; Magistrates' Courts Act 1980, s 48.

84 The terms used to refer to the acts to be undertaken by law enforcement agencies should be broad enough to capture the full range of activities which may be performed in respect of electronic material. For example, in the case of cryptocurrencies, the return of a person's private key has the effect of "releasing" assets to be dealt with. The assets themselves cannot in any sense be seized or returned.

further application shall not be entertained if made within three months after the date of the refusal.[85] We again consider that a Code of Practice would assist with resolving disputes without recourse to litigation. For example, if devices are returned to an owner, they can make reasoned and particularised requests for data deletion under section 59 of the CJPA.[86] Thought should also be given to measures to decrease the likelihood of unmeritorious applications, such as a permission filter and/or costs regime.

Recommendation 62

17.139 We recommend that, under the new statutory regime in Recommendation 54 above, a person with an interest in electronic material be able to apply to the Crown Court for the return or deletion of particular electronic data or return of an electronic device on the grounds that:

(1) the electronic material is reasonably required by the person with an interest in it; or

(2) continued retention by an investigator of the electronic material is not necessary.

A new Code of Practice governing the acquisition and treatment of electronic material

17.140 At several points in Chapters 15, 16 and this chapter of the report we have referred to recommending a Code of Practice governing the acquisition and treatment of electronic material. We consider that there are a number of benefits to the introduction of a new Code of Practice governing search warrant cases involving electronic material.

Reasons justifying a new Code of Practice

17.141 First, a Code of Practice could bring a number of existing guidance documents under one roof, making the law clearer and easier to follow. We outlined the various guidance documents relating to electronic material at paragraph 14.95 above. In particular, a new Code of Practice could incorporate, and more importantly update:

(1) the Attorney General's supplementary guidelines on digitally stored material;

(2) the Bar Council's guidelines on independent counsel;

(3) the Association of Chief Police Officers' guidance on digital evidence;

(4) the Crown Prosecution Service's guidelines on communications evidence; and

(5) the section in Code B of PACE on seizure and retention of property.

17.142 Secondly, while principles and relevant statements of law are already contained in these guidance documents, some are out of date and some are not sufficiently tailored to electronic material. For example, Code B of PACE states that searches must be conducted with due consideration for the property and privacy of the occupier and with no more

---

85 Road Traffic Offenders Act 1988, s 42(4).

86 *Business Energy Solutions Ltd v Crown Court at Preston* [2018] EWHC 1534 (Admin), [2018] 1 WLR 4887 at [110].

disturbance than necessary.[87] In our view, a new Code of Practice could expand on the application of principles such as these in the context of electronic material.

17.143 Secondly, a new Code of Practice would provide an opportunity to incorporate the internal guidance and best practice of other law enforcement agencies. Consultation responses have revealed differing approaches across agencies towards devising search strategies and examining electronic material, differing policies on invoking section 50 of the CJPA and differing views on what is legally permissible under the current law. A Code of Practice would provide an opportunity not only to capture best practice, but to harmonise the practices that do exist to ensure more consistent approaches across law enforcement agencies, where appropriate, recognising their different institutional structures and legal powers.

17.144 Thirdly, a Code of Practice would provide greater detail and flexibility in prescribing the methods by which statutory duties should be achieved. In particular, as technology and digital forensic practices continue to evolve, a Code of Practice would be easier to update. The Code would therefore complement several of our recommendations regarding electronic material.

17.145 Fourthly, a Code of Practice would provide enforceable standards on conduct. This can be contrasted with other pieces of guidance, such as the Attorney General's guidelines, which are neither a statement of law nor a policy which investigative agencies are obliged to follow.[88] Breaches of the Code would also be a factor for the court to take into account when considering an application to exclude evidence under section 78 of PACE, thereby ensuring regulation of investigators and providing a valuable safeguard for individuals.

17.146 Fifthly, in the context of human rights compliance, the Strasbourg court has made clear that it is necessary for there to be detailed rules governing the scope and application of automatic data processing tools to guard against the risk of abuse and arbitrariness.[89] A Code of Practice will assist in ensuring that the law is sufficiently clear and foreseeable, and the processing and retention of personal data is compliant with human rights and data protection law. To this end, it is noteworthy that the Information Commissioner's Office has recently recommended that a statutory code of practice be introduced to govern the practice of mobile phone data extraction to ensure that the law is sufficiently clear and foreseeable.[90]

Scope of a new Code of Practice

17.147 A new Code of Practice will require detailed consideration and consultation, including with privacy groups, digital forensic specialists and law enforcement agencies. Fundamental questions will need to be answered, one of which is its scope.

17.148 While constrained by our terms of reference, we observe that a Code of Practice would have clear application beyond criminal investigations involving search warrants. For example, the Code could usefully address mobile phone data extraction more generally.

---

87 Code B of PACE (2013) para 6.10.

88 *R (McKenzie) v Director of the Serious Fraud Office* [2016] EWHC 102 (Admin), [2016] 1 WLR 1308 at [22].

89 *S and Marper v United Kingdom* (2009) 48 EHRR 50 (App No 30562/04) at [99] and [103].

90 Information Commissioner's Office, *Investigation report: Mobile phone data extraction by police forces in England and Wales* (June 2020) p 52. Accessible at https://ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/.

Difficulty may also arise were the Code of Practice limited to criminal investigations involving search warrants: it may not be known whether a search warrant or other investigative power will be applied for or exercised during an investigation. Further, other statutory powers involving seizure or compulsory production may be exercised during the course of the same investigation in which a search warrant has been exercised. The scope of a Code of Practice is also a matter that should be considered as part of a wider review of the acquisition and treatment of electronic material in criminal investigations, which we recommend in Chapter 18.

17.149 We also recommend in Chapter 11 that that guidance on instructing independent counsel should be contained in the new Code of Practice. This is because issues surrounding legally privileged material often arise in the context of searches involving electronic material.

Content of a new Code of Practice

17.150 The content of a new Code of Practice would again require detailed consideration and consultation. Beyond setting out the aims of such a Code and the reasons justifying its creation, we do not regard it as desirable to prescribe its content. However, there are a number of matters which we consider should be included.

17.151 We consider that the Code of Practice should contain a list of overarching principles that should guide investigators when exercising powers in respect of electronic material. For example, proportionality is an important principle when considering the appropriateness of seizing and copying electronic devices. The importance of ensuring evidence retains its integrity and chain of custody should also feature in the Code. Another key feature that we have discussed is that the Code should encourage cooperation between investigators and defence teams and the resolution of disputes outside of court.

17.152 The Code should also contain detailed guidance on devising search strategies, applying for warrants in respect of electronic material, conducting searches, formulating post-search protocols and examining devices off-site. It should expand and give guidance on the ways in which to comply with statutory duties, such as the sifting of protected material. The Code should be written in such a way so as to account for the modern digital landscape and digital forensics.

Recommendation 63

17.153 We recommend the creation of a Code of Practice governing the acquisition and treatment of electronic material in criminal investigations involving search warrants.

Chapter 18: A wider review of the law governing electronic material

INTRODUCTION

18.1 In line with our terms our reference, our recommendations for reform regarding electronic material have been limited to search warrants legislation. Throughout the course of this project, we have become fortified in the view that there is a need for a wider review of the law governing the acquisition and treatment of electronic material. This stems from concerns about whether law enforcement agencies have the powers necessary to investigate crime, and whether adequate safeguards apply to ensure the use of powers is proportionate.

18.2 We begin this chapter by setting out the reasons justifying a wider review. We then set out those topics which we regard as germane to a wider review.

REASONS JUSTIFYING A WIDER REVIEW

18.3 First, at several points in our report we acknowledge that the problems being discussed transcended search warrants. For example, one of the issues with which we grapple is how electronic material should be treated when it falls into the hands of law enforcement agencies. In our view, there would be merit in considering these issues in a wider setting and not simply through a search warrants lens. As the Law Society put it, the topic of electronic material generally "seems to require separate, specialist consideration and consultation in its own right."

18.4 Secondly, in our view, while our recommendations would help rationalise and modernise the law of search warrants, amendment to search warrants legislation is not necessarily a viable long-term solution to the problems posed by cloud computing. Several consultees have argued for new investigative powers that are not tied to premises but rather to a person, a person's device or which permit remote execution. This may require a new kind of power.

18.5 Thirdly, and connected to the above, we have found ourselves constrained at times by the interconnectivity of investigative powers, which raises the question of where certain investigative powers should sit within the wider legal framework. Take as a hypothetical example the power to compel the production of material. While this power can be used under several statutes when executing a search warrant, it does not require a search warrant to have been executed before it can be used. Therefore, the power could be exercised in other circumstances not connected to a search warrant.

18.6 When considering hypothetical reform to these powers, one option would be to create a power restricted to search warrants. However, this may involve fragmenting the present law, causing it to become less comprehensible. On the other hand, a general amendment to these powers would have profound consequences for criminal investigations. A wider review could therefore take a holistic approach to these issues.

18.7 Fourthly, there is an argument that some of the recommendations we do make should apply beyond the search warrants context. For example, we recommend that particular statutory duties apply when an investigator acquires electronic devices during the execution of a search warrant. Big Brother Watch has questioned whether our proposals would extend to

complainants.[1] The short answer is that, owing to our terms of reference, they would not. There are strong arguments that bespoke safeguards should apply when complainants' devices are acquired by law enforcement.

18.8 Another recommendation that we make is for a Code of Practice governing the acquisition and treatment of electronic material. Specific concerns have been raised regarding data extraction devices and the lack of adequate guidance, such as a code of practice, to ensure human rights compliance. The Information Commissioner's Office has recently recommended that a statutory code of practice be introduced to govern the practice of mobile phone extraction to ensure that the law is sufficiently clear and foreseeable.[2] There is, accordingly, a strong argument that a code of practice should apply equally to powers of search and seizure exercised in respect of electronic devices and electronic data following, say, arrest. Therefore, several of our recommendations could provide a springboard for, overlap with and inform work in other fields.

18.9 Fifthly, and more fundamentally, we have identified several concerns about the lawfulness of current law enforcement practices around extracting electronic data from mobile phones and other electronic devices. For example, certain practices may constitute an offence of unlawful interception under section 3 of the Investigatory Powers Act 2016 ("IPA"). Such practices may also be non-compliant with the Data Protection Act 2018 as well as article 8 of the ECHR. In our view, these matters require addressing urgently.

18.10 Sixthly, we have received consultation responses which suggest that there are several statutory powers not reliant on search warrants that may require reform. For example, in the case of the powers of production under sections 19(4) and 20(1) of the Police and Criminal Evidence Act 1984 ("PACE"), Consultation Question 54 asked whether there is a need to reform these provisions not just within the context of our review. Consultation responses indicated that there are several aspects of these provisions which might require reform.

18.11 It is worth clarifying briefly what we mean by using the term "wider review". We do not necessarily mean that all of the matters discussed below should be examined in unison by a single body. We understand that there is significant work ongoing in many of these areas.[3] On the one hand, the areas may fall into discrete topics which lend themselves to isolated examination by specific bodies. On the other hand, there may be benefit in an integrated approach or a consortium to address the issues so that there is joined-up thinking and to reduce the duplication or overlap of work.

18.12 The Law Commission has, in recent times, undertaken several projects which consider how the law ought to adapt to take account of new and emerging technology within criminal and other spheres. The Law Commission stands ready to take on further work in these areas which concern electronic material.

---

1 Big Brother Watch, *Digital strip searches: The police's investigations of victims* (July 2019) p 14 to 15.

2 Information Commissioner's Office, *Investigation report: Mobile phone data extraction by police forces in England and Wales* (June 2020) p 52. Accessible at https://ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/.

3 Information Commissioner's Office, *Investigation report: Mobile phone data extraction by police forces in England and Wales* (June 2020) p 63. Accessible at https://ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/.

TOPICS RELEVANT AS PART OF A WIDER REVIEW

18.13 The topics that we have identified which would be suited to further review are:

(1) the desirability of a power to search electronic devices not contingent on premises;

(2) the desirability of a power to search electronic data directly;

(3) the operation of sections 19(4) and 20(1) of PACE;

(4) the regulation of data extraction devices; and

(5) the extraction of data from complainants' devices.

A power to search devices not contingent on premises

18.14 Dijen Basu QC suggested that special provision should be made for highly portable electronic devices as part of a revision of provisions concerning electronic material. A number of reasons justifying special provision were put forward.

18.15 First, it can be difficult to assert on a search warrant application that highly portable electronic storage devices, such as mobile phones, are to be found "on" premises, which is one of the statutory criteria required for the issue of a warrant. This is because the device will invariably be on the owner's person, and they may or may not be on premises.

18.16 Secondly, an electronic device will usually be found, and therefore need to be searched, on the owner's person. As we discuss at paragraph 7.121 above, it may be the case that the only way in which to search a person on premises is on arrest.

18.17 Thirdly, the fact that smart phones store such a large volume of data, including communications, was also said to justify the introduction of special provisions.

18.18 Fourthly, given the clear importance of electronic devices in many police investigations, creating special provisions to search for such devices might also avoid problems in the future posed by phones and laptops, such as being unable to satisfy the statutory conditions for the issue of a warrant.

18.19 We see the force in these arguments. It is no longer only physical premises which hold relevant evidence: it is often now data stored on, or accessible from, electronic devices that is relevant evidence. This raises the question of whether new powers should be introduced, and/or the current legal framework recalibrated, to facilitate the search for and of electronic devices not contingent on being stored on premises.

A power to search electronic data directly

18.20 The Whitehall Prosecutors' Group, while acknowledging the ambit of our project, considered that there should be a power to obtain a separate "e-warrant" in situations where access, search and seizure is not reliant on a condition precedent search of physical premises.

18.21 The Crown Prosecution Service ("CPS"), too, considered that there is a need for a wider and separate power of access to remotely stored data in a scenario unrelated to the search of premises. It was said that, irrespective of how the investigator comes to learn of remote electronic storage, they should be able to lawfully access, interrogate and seize its contents.

18.22 The CPS also suggested amending section 8 of and schedule 1 to PACE so that a judge may authorise access, search and seizure of remotely stored electronic material if satisfied that statutory access conditions are met, notwithstanding that no search of premises is sought at that time. This would allow for a standalone application to access remotely stored material even when no search is merited, or the occupier is not to be tipped off, but where access to the remotely stored material is possible.

18.23 We acknowledge that there may be instances in which there would be no need for an investigator to access electronic data through a particular electronic device. We understand that there are cases in which usernames and passwords for remote storage accounts have been obtained during a search, or subsequently extracted from seized electronic devices. In such circumstances, to enable the swift and efficient obtaining of evidence, there is an argument that authorisation ought to be obtainable to access remote storage accounts and copy relevant remotely stored data for use in criminal proceedings.

18.24 It is also noteworthy that there are powers of so-called "remote execution" of search warrants in other jurisdictions, which essentially permit law enforcement agencies to conduct a search from their own offices. The United States Federal Rules of Criminal Procedure permit a search warrant to be remotely executed,[4] as does the Australian Crimes Act 1914.[5] The New Zealand Search and Surveillance Act 2012 also permits the remote execution of a search warrant.[6] The New Zealand Law Commission and Ministry of Justice recommended replacing the remote execution provisions in their Search and Surveillance Act 2012 with a more transparent set of provisions.[7]

Reform to sections 19 and 20 of the Police and Criminal Evidence Act 1984

18.25 In the consultation paper, we discussed[8] the powers under sections 19(4) and 20(1) of PACE to require any information which is stored in any electronic form and is accessible from the premises to be produced.

18.26 Section 19(1) of PACE provides that section 19(4) is exercisable by a constable who is lawfully on premises. In full, section 19(4) then provides:

> The constable may require any information which is stored in any electronic form and is accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible or from which it can readily be produced in a visible and legible form if he has reasonable grounds for believing—
>
> (a) that—
>
> (i) it is evidence in relation to an offence which he is investigating or any other offence; or

---

4 Federal Rules of Criminal Procedure (United States), r 41(b)(6).

5 Crimes Act 1914 (Australia), s 3F(2D) (as amended by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, sch 3, para 3).

6 Search and Surveillance Act (New Zealand), ss 103(4)(k) and 111.

7 New Zealand Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012 / Ko te Arotake i te Search and Surveillance Act 2012*, NZLC R141 (2017) at 12.145 to 12.148.

8 Search Warrants (2018) Law Commission Consultation Paper No 235 paras 10.103 and following.

(ii) it has been obtained in consequence of the commission of an offence; and

(b) that it is necessary to do so in order to prevent it being concealed, lost, tampered with or destroyed.

18.27 Section 20(1) of PACE provides:

> Every power of seizure which is conferred by an enactment to which this section applies[9] on a constable who has entered premises in the exercise of a power conferred by an enactment shall be construed as including a power to require any information stored in any electronic form contained in a computer and accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible or from which it can readily be produced in a visible and legible form.

18.28 Similarly worded powers are contained in other enactments.[10] The provisions apply in a broad range of circumstances. For example, under section 19(4), a constable may be lawfully on premises, but without a search warrant, and they will be able to compel the production of information pertaining to *any* offence, irrespective of whether it is an offence that they are investigating.

18.29 In the consultation paper, we identified several points of ambiguity in respect of how the sections 19(4) and 20(1) applied to electronic material. After setting these out, we invited[11] consultees' views on the points of ambiguity, whether reform was needed and, if so, how the provisions ought to be reformed.

18.30 We received a number of consultation responses regarding sections 19(4) and 20(1) of PACE.[12] In addition to providing views on the operation of the provisions and whether reform was needed, it was indicated that it would be beneficial for the Law Commission to resolve the matters of ambiguity inherent in sections 19(4) and 20(1) of PACE.

18.31 In the sections that follow, we set out our interpretation of how sections 19(4) and 20(1) of PACE operate as a matter of law. Where necessary, we then discuss the desirability of reforming various aspects of the provisions. We discuss the following issues:

(1) whether the provisions permit a constable to search an electronic device;

(2) when material is deemed accessible;

(3) whether material stored remotely overseas can be required to be produced;

(4) whether the provisions permit a constable to require the production of passwords; and

---

9 Police and Criminal Evidence Act 1984, s 20(2): this section applies to (a) any enactment contained in an Act passed before the Police and Criminal Evidence Act 1984; (b) Police and Criminal Evidence Act 1984, ss 8 and 18; (c) Police and Criminal Evidence Act 1984, sch 1, para 13; and (d) any enactment contained in an Act passed after the Police and Criminal Evidence Act 1984.

10 Immigration Act 2016, s 48; Enterprise Act 2002, s 194; Competition Act 1998, ss 28A, 65F, 65G and 65H; Armed Forces (Powers of Stop and Search, Search, Seizure and Retention) Order 2009 (SI 2009 No 2056), art 14.

11 Consultation Question 54.

12 Crown Prosecution Service; National Crime Agency; Serious Fraud Office; Professor Richard Stone; Kent County Council Trading Standards; Insolvency Service; Law Society; Bar Council and the Criminal Bar Association; Competition and Markets Authority; Whitehall Prosecutors' Group.

(5) the consequences of non-compliance with a request.

18.32 Before embarking on this analysis, it is worth explaining briefly why there remains a clear interest in considering reform to these provisions, notwithstanding the recommendations in this report. First, while we recommend an avenue by which to search electronic devices when executing a search warrant, an investigator may not have the facilities or digital forensic tools to search devices. In such circumstances, recourse to sections 19(4) or 20(1) of PACE may be necessary. Therefore, even within a search warrants setting, these provisions are vitally important to securing evidence of criminality.

18.33 Secondly, the powers extend further than just instances where a constable is on premises pursuant to a search warrant. We have found during the course of this review that section 19 in particular, and not just subsection (4), is relied on as a legal basis for various forms of conduct. In our view, it is unclear whether section 19 does in fact provide a legal basis for certain conduct, with the consequence that law enforcement agencies may be acting unlawfully and even committing criminal offences.

The search of electronic devices

18.34 The first issue we identified in respect of sections 19(4) and 20(1) of PACE is that these provisions are not standalone powers of search. On a literal reading, neither section 19(4) nor 20(1) allow an investigator to interrogate a device and search it. The sections provide powers of production in certain situations, which would seemingly always require the assistance of a person on the premises.

18.35 The CPS agreed with our provisional assessment in our consultation paper that these are powers of production and seizure, not powers of search. However, we have been made aware that some investigators interpret these provisions as providing permission to search with or without the assistance of those on the premises. For example, section 19(4) does not specify to whom a constable may direct the requirement to produce information; one interpretation is that a constable may require, say, a fellow digital forensics officer on the premises to interrogate a device.

18.36 In our view, the provisions are clear: neither sections 19(4), 20(1), nor any other subsection within section 19 for that matter, of PACE permit a constable to search an electronic device manually. The Divisional Court has confirmed that these sections are concerned not with powers of search but instead with powers of seizure.[13] Further support for this interpretation comes from amendments proposed under the Environment Bill 2019-2021, which provide the following powers:[14]

(1) to require any information which is stored in electronic form and is accessible from the premises to be produced in a form in which it can be removed and—

(a) in which it is visible and legible, or

(b) from which it can readily be produced in a visible and legible form;

(2) to operate any equipment found on the premises for the purposes of producing such information in such a form.

---

13 *R* (*Cabot Global Ltd) v Barkingside Magistrates' Court* [2015] EWHC 1458 (Admin), [2015] 2 Cr App R 26 at [41].

14 Environment Bill 2019-2021, sch 10, para 5(2).

18.37 Subsection (1) mirrors the main power in sections 19(4) and 20(1). Subsection (2) provides an explicit power to search an electronic device for the purpose of producing such information. We understand that this amendment was introduced so that documents may be searched for on a seized device or in situ, indicating that the power contained in subsection (1) was regarded as insufficient for this purpose.

18.38 We are unimpressed by the suggestion that section 19(4) can be relied on to instruct a fellow officer to perform the search of an electronic device for a number of reasons. First, the act of requiring a person to produce information is a coercive command. Secondly, such a construction would mean that the power could be used when the owner of an electronic device is not on premises, and so no interaction would take place. Thirdly, if it was Parliament's intent for the power to operate in such a way to enable an investigator to conduct a search, we consider that it would have made this explicit. Fourthly, this is an instance in which we consider that the provision calls for a strict construction.[15]

18.39 Having reached the conclusion that sections 19(4) and 20(1) of PACE do not provide powers of search, we consider briefly the desirability of reform. While we recommend a power for law enforcement agencies to search for remotely stored material, this would only apply when executing certain search warrants.

18.40 There is an argument that sections 19(4) and 20(1) of PACE should provide powers of search to cover other instances in which law enforcement agencies are lawfully on premises. The Serious Fraud Office ("SFO") has pointed out that it is arguable that the provisions do not require production to be in the native digital form which is problematic for reasons of provenance, continuity and forensic integrity.[16] The fact that these sections are already relied on to conduct a search indicates that the power is regarded as necessary. Searching an electronic device without a lawful basis may also constitute criminal offences under IPA and the Computer Misuse Act 1990 ("CMA 1990").[17]

18.41 Set against this, there are clear privacy concerns that an innocent occupier may have their whole digital life searched through without any judicial authorisation. The Law Society argued that the provisions ought to be reformed to make clearer that they do *not* operate as a means to conduct a search. Any reform will therefore require careful consideration.

18.42 There are numerous ways in which a power to permit a constable to search an electronic device could be worded. Reform could be to section 19 of PACE or an entirely new power could be created. The CPS provided a suggested amendment to section 19 of PACE to include a power to require a person present who is specified in a warrant to provide information which will enable the constable to access and, if necessary, search a device. The suggested conditions for exercising the power were that the constable has reasonable grounds for believing:

(1) the electronic material has been accessed from the premises, or would have been stored on the premises but has been stored remotely, and this subsection operates so that even if it is said that the material is stored outside England or Wales, the material shall by virtue of its access or otherwise likely location be deemed to be inside England or Wales; and

---

15 D Bailey and L Norbury, *Bennion on Statutory Interpretation* (8th ed 2020) paras 27.2 and 27.9.

16 Serious Fraud Office.

17 See paragraphs 14.58 to 14.60 above.

(2) that:

(a) it is evidence in relation to an offence which he is investigating or any other offence; or

(b) it has been obtained in consequence of the commission of an offence; or

(c) within it he will find, upon a search conducted pursuant to this provision, either (a) or (b) above, and

(3) that it is necessary to do so in order to prevent it being concealed, lost, tampered with or destroyed.

When material is deemed accessible

18.43 The second issue is when material is deemed "accessible" such that the information can be lawfully required to be produced. When electronic data is concerned, there are a multitude of factors that will affect its accessibility. Further, the answer will depend on the question of to whom the electronic data must be accessible. Some provisions make this clear.[18] An occupier, with their knowledge of passwords and encryption keys, will be able to access electronic data which an investigator may not.

18.44 As pointed out by Andrew Smith, Partner at Corker Binning, there is no case law on what is meant by the term "accessible from the premises".[19] Andrew Smith writes:

> Absent judicial guidance, it is submitted that resolving whether electronic data is "accessible from the premises" is a question of fact. Data is likely to be deemed "accessible" if the occupier of the premises can, of his own volition, retrieve it via an electronic device. That is, if the data can be retrieved at the push of a button, it is accessible, even if the server or cloud on which the data is stored is outside the UK. Likewise, if the data is encrypted, so that the occupier of the premises needs to enter a password in order to retrieve the data, it is still accessible. The process of accessing the data takes place entirely domestically.

18.45 The CPS were also of the view that the question of accessibility ought to be read as "accessible by the occupier". We agree with this interpretation. Namely, the requirement whether data is "accessible from the premises" under sections 19(4) and 20(1) of PACE and similarly worded provisions depends on whether it is accessible to the person to whom the command is issued.

Material stored remotely overseas

18.46 The third issue with sections 19(4) and 20(1) of PACE is whether the provisions extend to data stored remotely overseas. Several consultees, including the CPS, NCA and CMA, considered that clarification on this issue was necessary.

---

[18] See Consumer Rights Act 2015, sch 5, paras 14 and 27, which permit an investigator to require the production of material "to which the trader has access".

[19] Andrew Smith, "Do search warrants have extraterritorial effect?" Corker Binning Blog (7 February 2018) (available at https://www.corkerbinning.com/do-search-warrants-have-extraterritorial-effect/).

18.47 On the basis of our interpretation of the phrase “accessible”, overseas data is clearly still capable of being accessible to the owner of an electronic device. For example, by unlocking a phone and opening an app, data stored remotely overseas may become accessible.

18.48 As explained at paragraph 16.31 above, there is a rebuttable presumption that statutes do not extend to matters outside the jurisdiction and therefore have only territorial effect. Whether this principle applies depends on whether compelling an individual within the jurisdiction to produce material to which they have access there and then outside of the jurisdiction amounts to an extraterritorial use of enforcement powers.

18.49 We explain at paragraphs 16.28 to 16.60 above that there is debate over whether the use of production powers against individuals within the jurisdiction can be regarded as an extraterritorial use of enforcement powers. We conclude that the arguments for and against the production of overseas data being classed as extraterritorial are finely balanced. Looking at the matter in the round, it is arguable either way whether the search, seizure or requiring the production of overseas data involves an extraterritorial exercise of power

18.50 Assuming that the use of production powers in the way envisaged would involve an extraterritorial use of enforcement powers, the question whether a provision applies to matters outside of the jurisdiction is one of statutory construction.

18.51 In our view, there are a number of factors which point towards sections 19(4) and 20(1) of PACE permitting a constable to require the production of data stored remotely overseas. First, sections 19(4) and 20(1) of PACE contain no words of express jurisdictional limitation.

18.52 Secondly, such an interpretation accords with the purpose of the provisions, which is to enable constables to acquire evidence of criminality that is not stored directly on the premises but is accessible from it.

18.53 Thirdly, the fact that cloud storage and other new technology were not available at the time PACE was enacted does not prevent the provisions from permitting a constable to require the production of overseas data. Lord Wilberforce in *Royal College of Nursing* observed that the question is whether the new state of affairs falls within the parliamentary intention.[20] In our view, the parliamentary intention behind enacting sections 19(4) and 20(1) of PACE leads to the conclusion that the provisions capture data stored remotely overseas in cloud storage and online accounts.

18.54 Fourthly, permitting a constable to require the production of data stored remotely overseas would prevent the powers from becoming ineffective. We asked a consultation question on whether law enforcement require powers of extraterritorial production.[21] By this we meant the power to require the production of information from an individual within the jurisdiction. The Whitehall Prosecutors’ Group, and a number of individual law enforcement agencies, argued that law enforcement agencies need a power to require any person on the premises to exercise their ability to access cloud-stored data and download a copy to be produced to the officer executing the warrant in order to effectively obtain relevant evidence.

---

20 *Royal College of Nursing of the United Kingdom v Department of Health and Social Security* [1980] UKHL 10, [1981] AC 800 at 822.

21 Consultation Question 55.

18.55 Fifthly, utilising Lord Mance JSC's practical touchstone in *Masri*,[22] such an interpretation would not, in our view, cause eyebrows to be raised that Parliament would have conferred the power in question, nor would it offend the sovereignty of other sovereign states.

18.56 Support for this interpretation can also be found in the joint consultation response from the Bar Council and the Criminal Bar Association ("CBA"). They considered that, in the light of the Administrative Court's decision on the SFO's powers of production in *KBR*, it is more than arguable that section 19(4) extends to information held remotely and in other jurisdictions. They suggested that the control against excessive jurisdiction is the need for the material to be accessible from the premises, although they recognised that more certainty is required about what "accessible" actually means. It was suggested at the very least that "accessible" should mean a substantial connection between the device on the premises and the material held remotely.

Requiring the production of passwords

18.57 The fourth issue with sections 19(4) and 20(1) is that it is not clear whether the provisions permit a constable to require the production of passwords. We have been informed that the provisions have been used in practice to compel the production of passwords, as has section 2(3) of the Criminal Justice Act 1987. In our section above on relevant legal regimes, we explained there are powers to compel the production of electronic device passwords under the Regulation of Investigatory Powers Act 2000[23] and the Terrorism Act 2000.[24]

18.58 The Bar Council and the CBA did not see any principled objection to section 19(4) of PACE being used to compel the surrendering of passwords. They could see no reason why RIPA part 3, with its significant maximum sentence for non-compliance, should provide the only means by which passwords may be required.

18.59 In our view, it is unlikely that section 19(4) of PACE permits a constable to require the production of a password. There are three main hurdles posed by the provision. These hurdles reveal a crucial distinction between electronic data stored in electronic form, at which the provision is aimed, and information, such as a password, which allows access to such data.

18.60 The first hurdle is that section 19(4) only applies to information stored in electronic form. A password may exist only in the mind of an account holder and so not be stored in electronic form. This can be contrasted with paragraph 5(a) of schedule 7 to the Terrorism Act 2000, which has been held to include the provision of passwords.[25] The paragraph provides that a person who is questioned under the Act must give the examining officer "any information in his possession which the officer requests". An individual who knows a password can be said to possess knowledge of it. There is no requirement for the password to be stored in electronic form.

18.61 This hurdle may be surmountable if the password is stored in password manager software. Some electronic devices include software that permits a user to save and store account names and passwords, which the software will prompt a user to allow it to retrieve when

---

22 *Masri v Consolidated Contractors International (UK) Ltd* [2009] UKHL 43, [2010] 1 AC 90 at [24].

23 Regulation of Investigatory Powers Act 2000, s 49.

24 Terrorism Act 2000, sch 7, para 5(a). See *Rabbani v DPP* [2018] EWHC 1156 (Admin).

25 *Rabbani v DPP* [2018] EWHC 1156 (Admin).

accessing relevant websites or accounts. For example, Apple's iCloud keychain is a password manager software that is built into Apple electronic devices, allowing passwords to be stored and synced across devices. Google use similar software for Android devices. There are countless other companies that produce password manager applications.[26] Where an account name and password is saved in such databases, the password will be information that is stored in electronic form and accessible from the premises.

18.62 Two further hurdles remain. Section 19(4)(a)(i) of PACE would require the password to be itself evidence in relation to an offence being investigated. Section 19(4)(b) of PACE would also require production of the password to be necessary in order to prevent the password itself being concealed, lost, tampered with or destroyed. As indicated at paragraph 18.59 above, the difficulties posed by these hurdles flow from the provisions being clearly directed at the electronic data itself and not the information which renders the data accessible. By way of analogy, the provision envisages the holder of the information opening the lockbox and handing over the files contained therein; it does not envisage the holder of the information handing over the key itself.

18.63 Even if section 19(4) of PACE and other powers of production, such as section 2(3) of the Criminal Justice Act 1987, could be used to compel the production of passwords, we express the view at paragraph 16.214 above that these provisions do not provide a sufficiently robust framework to govern such activity.

18.64 At paragraphs 16.214 to 16.222 above, we discuss the desirability of introducing new powers to compel the production of passwords when executing a search warrants. We recognise the force of arguments for reform while acknowledging the significant privacy implications of such a power. There are a host of issues which will require detailed thought before deciding whether to introduce a power to compel passwords, including the adequacy of the power under part 3 of RIPA. We reach no definitive view but recommend that the Government considers the desirability of a power to compel the production of passwords, including where a search warrant is not being executed.

The consequences of failing to comply with a request

18.65 The fifth issue that we identified with sections 19(4) and 20(1) of PACE is that the consequences of the occupier refusing to produce the information in a visible and legible form are unclear. The CPS agreed that the penalty attached to non-compliance with the sections lacks clarity.

18.66 The power provided in section 19(4) of PACE is a power bestowed on the constable to require something to be done. This is distinct from a positive obligation imposed on the occupier with sanctions for non-compliance as in, for example, the Financial Services and Markets Act 2000[27] or the Terrorism Act 2000.[28]

18.67 In our view, the answer lies in the offence of obstruction. Under section 89(2) of the Police Act 1996, any person who resists or wilfully obstructs a constable (or a person assisting a constable) in the execution of their duty is guilty of an offence.

---

26 For example, LastPass is a web browser extension that stored encrypted passwords online.

27 Financial Services and Markets Act 2000, ss 131E and 131L.

28 Terrorism Act 2000, sch 7, para 18. See *Rabbani v DPP* [2018] EWHC 1156 (Admin).

18.68 A person obstructs a constable if that person makes it more difficult for the constable to carry out their duty.[29] While liability for omissions is exceptional in the criminal law, a refusal to act may amount to a wilful obstruction where the law imposes an obligation to act in a manner requested by an officer.[30] Sections 19(4) and 20(1) clearly impose an obligation to act in a manner required by a constable, namely by producing information. It follows that a person who fails to comply with a requirement to produce information may commit the offence of wilful obstruction of a constable under section 89(2) of the Police Act 1996.

The regulation of data extraction tools

A summary of the concerns raised

18.69 The use of data extraction tools has become an area of increasing concern. The Bristol Cable, an independent media company, was one of the first to report on the use of data extraction tools by UK police forces in 2017.[31] The concerns raised by the Bristol Cable's article included:

(1) the prolific use of data extraction tools by police forces, including in "low-level crime";

(2) the potency of data extraction tools to circumvent security features;

(3) the insufficiency of officer training before using data extraction tools;

(4) the proportionality of searches using data extraction tools; and

(5) the lack of necessary judicial authorisation regarding the use of data extraction tools.

18.70 Privacy International has since carried out a substantial amount of work surrounding data extraction tools.[32] Particular concern has been raised regarding the lack of a clear legal basis, policies, guidance and judicial authorisation. In summary, Privacy International has called for:

(1) the use of intrusive data extraction technology to be properly regulated, with independent oversight so that abuse and misuse does not go undetected;

(2) a proper warrant regime to be implemented, so that the technology cannot be used arbitrarily;

(3) people to be informed of their rights if the police want to search their phone.

18.71 A large amount of activity in the field has occurred in Scotland. In May 2018, the UK's Information Commissioner's Office announced it would investigate Police Scotland after a complaint was filed by Privacy International. The central concern raised by Privacy International was that the police's use of data extraction devices, which when connected to an electronic device can view all its electronic data, violated data protection legislation.

---

29 *Hinchcliffe v Sheldon* [1955] 3 All ER 406.

30 *Lunt v DPP* [1993] Crim LR 534.

31 Accessible at: https://thebristolcable.org/2017/01/phone-cracking-tech/.

32 See Privacy International, *Digital stop and search* (March 2018) and Privacy International, *Cloud extraction technology* (January 2020).

18.72 In March 2019, the Scottish Human Rights Commission informed the Scottish Parliament that there was a lack of clarity about the precise legal basis for the use of data extraction devices, as well as an absence of sufficient oversight safeguards.[33] In April 2019, the Scottish Parliament's Justice Sub-Committee on Policing published a report on Police Scotland's proposal to introduce electronic extraction devices.[34]

18.73 Police Scotland announced on 31 January 2019 that they would not proceed with introducing the technology until clear legal authority was in place. Following independent legal advice,[35] Police Scotland announced in January 2020 that it would proceed with the phased introduction of data extraction devices.[36]

18.74 In England and Wales, there has also been scrutiny of the use of data extraction devices. A complaint was made by Privacy International to the Information Commissioner's Office ("ICO"), who in June 2020 published a report explaining how current mobile phone extraction practices and rules risk negatively affecting public confidence in the criminal justice system.[37] Thirteen recommendations were made by the ICO, including the introduction of a statutory code of practice in order to provide greater clarity and foreseeability about when, why and how law enforcement agencies use mobile phone extraction.[38]

18.75 Privacy International contacted us during our consultation period. They demonstrated to us the powerful nature of data extraction devices when we visited their offices. They also submitted a detailed and comprehensive consultation response, highlighting a number of concerns.

18.76 First, Privacy International pointed out that search warrants are just one avenue by which the state may extract data from mobile phones. They noted that mobile phone extraction is widespread and affected individuals include suspects, witnesses, complainants and other third parties. For example, the extraction of data from mobile phones may occur during a stop and search and following arrest. For this reason, they argued that better regulation was required.

18.77 Secondly, Privacy International pointed out that, amongst the various police forces that have disclosed their local guidance, there is uncertainty and inconsistency as to the legal basis under which they can extract data from mobile phones. This indicated, in their view, that PACE does not provide an adequate legal basis for extracting data from mobile phones. Privacy International observed that this absence has implications under the ECHR but also

---

[33] Accessible at https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/20190312SHRC-CyberKiosks.pdf.

[34] Accessible at https://sp-bpr-en-prod-cdnep.azureedge.net/published/JSP/2019/4/8/Report-on-Police-Scotland-s-proposal-to-introduce-the-use-of-digital-device-triage-systems--cyber-kiosks-/JSPS052019R01.pdf.

[35] Accessible at https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/20190430SeniorCounselOpinion.pdf.

[36] https://www.bbc.co.uk/news/uk-scotland-51110586.

[37] Information Commissioner's Office, *Investigation report: Mobile phone data extraction by police forces in England and Wales* (June 2020). Accessible at https://ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/.

[38] Information Commissioner's Office, *Investigation report: Mobile phone data extraction by police forces in England and Wales* (June 2020). Accessible at https://ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/.

could be catastrophic in cases where the product of a download has formed the basis of a criminal charge or where disclosure obligations have not been discharged.

18.78 Thirdly, Privacy International argued that little, if any, consideration has been given to the potential that mobile phone extraction may constitute both interception and equipment interference and threaten the security of target devices. We have set out the law governing the interception of communications under IPA within our section on relevant legal regimes at paragraphs 16.54 to 16.60 above, including the bases on which interception will be lawful. Of significance is that consent of a single party is insufficient to amount to lawful authority.

18.79 Privacy International believed that the interception of communications occurs through mobile phone extraction. The point was also made by Privacy International that there is a statutory prohibition on the use of intercept material being used or disclosed in legal proceedings.[39]

18.80 Privacy International has therefore recommended that the Home Office conduct a consultation in relation to mobile phone extraction and urged the Law Commission to endorse this recommendation. Since writing to us, Privacy International has produced another report drawing attention to cloud extraction technology.[40]

Analysis

18.81 It is important to note from the outset that data extraction devices have a number of benefits for the investigation of crime. They allow electronic data to be quickly and easily searched, filtered and sorted to identify suspects, victims and locations. In doing so, they can recover deleted data and overcome electronic devices' security and encryption. Another benefit of data extraction devices is that they can preserve the integrity and what is known as the "chain of custody" of evidence, which prevents contamination and challenges to the admissibility of evidence at trial. It follows that data extraction devices can improve the state's capability to investigate, detect and prevent crime.

18.82 From a human rights perspective, the legal opinion provided to Police Scotland on the lawfulness of mobile phone extraction identifies a number of arguments that the use of mobile phone extraction might serve to enhance the human rights of individuals.[41] First, in terms of the right to life (article 2 of the ECHR), the quick examination of an electronic device might materially assist in the prevention of homicide or the expeditious location of a missing person.

18.83 Secondly, in relation to the right to a fair trial (article 6 of the ECHR), electronic extraction devices may identify exculpatory evidence. Thirdly, in terms of freedom of expression (article 10 of the ECHR), the rapid return of an electronic device might enable an individual to resume channels of communication. In our view, the reasoning on this last point could legitimately be extended to the right to respect for private and family life (article 8 of the ECHR).

18.84 Therefore, on the one hand, there are clear public benefits in law enforcement agencies utilising devices to extract data quickly and safely when executing search warrants or otherwise investigating crime.

---

39 Investigatory Powers Act 2016, s 56.

40 Privacy International, *Cloud extraction technology* (January 2020).

41 Accessible at https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/20190430SeniorCounselOpinion.pdf.

18.85 At the same time, questions have rightly been raised regarding the lawfulness and proportionality of data extraction devices. There can be no dispute that these are highly intrusive tools which require appropriate regulation. There are a number of matters raised which we consider support the need for a review of the use of data extraction devices.

18.86 First, the legal basis for the use of data extraction devices is unclear. It is telling that police forces are unable to point in unison to the legal basis under which the power emanates.[42] It seems that sections 19 and 20 of PACE are the most often cited provisions which are said to provide a lawful basis.[43] Without expressing a firm view on whether these provisions do permit the use of data extraction devices, we observe that these provisions provide broad powers. However, in our view, they are too general in their wording to govern adequately the use of data extraction devices. These provisions also require a constable to be lawfully on premises, which may not always be the case when extraction is performed. As we have alluded to at several times throughout this report, a lack of lawful basis also means that offences may be committed under IPA and the CMA 1990.

18.87 Secondly, we consider that the human rights concerns raised connected to the use of data extraction devices are well-founded. It is clear that the use of data extraction devices may engage all of the rights (private and family life, home and correspondence) protected by article 8 of the ECHR.

18.88 As we observed in our section on relevant legal regimes, for an interference with article 8 of the ECHR to be justified, it must satisfy the requirements of lawfulness and proportionality. The question of whether use of data extraction devices is in accordance with the law requires scrutiny of both its legal basis and the sufficiency of its legal framework.

18.89 It is noteworthy that the Scottish Human Rights Commission's submission to the Scottish Parliament's Justice Sub-Committee on Police considered that these requirements were not met.[44] In their view, consideration should be given to new legislation along with statutory guidance and/or a code of conduct for digital forensics that integrates article 8 requirements.

18.90 Thirdly, there are interconnected data protection issues. Data extraction devices are able to extract large amounts of data which is likely to be irrelevant and constitute "special category data" under the Data Protection Act 2018. There are also a number of important data protection principles, including data minimisation.

18.91 Fourthly, the issues raised by data extraction devices pose difficult questions which merit careful scrutiny. For example, it may be said that one way of solving both the issue of a lack of lawful basis for data extraction devices and ensuring such devices are used proportionately would be to require a judicially authorised warrant. The question of whether a separate warrant should be required to search an electronic device has been considered in a number of other jurisdictions, which reveal several different approaches.

18.92 The United States Supreme Court, in *Riley v California*,[45] unanimously held that the warrantless search and seizure of digital contents of a cell phone during an arrest was

---

[42] Privacy International, *Digital stop and search* (March 2018) pp 20 to 21.

[43] Privacy International, *Digital stop and search* (March 2018) pp 20 to 21.

[44] Accessible at https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/20190312SHRC-CyberKiosks.pdf.

[45] 573 US ___ (2014).

unconstitutional. In reaching this conclusion, the Court emphasised that a search of digital information on a mobile phone implicates substantially greater individual privacy interests than a brief physical search. The Court also referred to the recognised exception of exigent circumstances, such as the need to prevent the imminent destruction of evidence, which might render a warrantless search objectively reasonable.[46]

18.93 The Supreme Court of Canada in *Fearon* set out the requirements for the common law police power to search mobile phones on arrest to be constitutionally compliant:

(1) the arrest was lawful;

(2) the search is truly incidental to the arrest in that the police have a reason based on a valid law enforcement purpose to conduct the search, and that reason is objectively reasonable. The valid law enforcement purposes in this context are:

(a) protecting the police, the accused, or the public;

(b) preserving evidence; or

(c) discovering evidence, including locating additional suspects, in situations in which the investigation will be stymied or significantly hampered absent the ability to promptly search the cell phone incident to arrest;

(3) the nature and the extent of the search are tailored to the purpose of the search; and

(4) the police take detailed notes of what they have examined on the device and how it was searched.[47]

18.94 The New Zealand Law Commission and Ministry of Justice in their joint review of their Search and Surveillance Act 2012 recommended removing the automatic ability to search an electronic device during the lawful execution of a warrantless power.[48] Instead, it was recommended that, in the course of executing a warrantless power, a police officer should be able to seize and secure an electronic device. To search it, the officer should obtain a search warrant, with the exception of urgent situations involving a risk to life or safety.

18.95 What these approaches reveal is that there are no simple answers to the issues posed by data extraction devices. Accordingly, a wider review is necessary so that appropriate consideration can be given to these issues.

Extraction of data from complainants' mobile phones

18.96 An offshoot of the concern relating to data extraction devices is the extraction of data from complainants' mobile phones. Big Brother Watch has carried out detailed work in this area and produced a report.[49] In essence, consent is currently relied on as a lawful basis to extract data from the mobile phones of complainants, predominantly complainants of rape

---

46 573 US ___ (2014) at p 26.

47 *R v Fearon* [2014] SCC 77, [2014] SCR 621 at [83]. The Supreme Court then went on to observe at [84] that the search of mobile phones may be an area in which legislation may well be desirable.

48 New Zealand Law Commission and Ministry of Justice *Review of the Search and Surveillance Act 2012 / Ko te Arotake i te Search and Surveillance Act 2012*, NZLC R141 (2017) at 12.32 to 12.43.

49 Big Brother Watch, *Digital Strip Searches: The Police's Data Investigations of Victims* (July 2019).

and serious sexual offences. This is achieved through asking complainants to sign consent forms, which detail the reasoning for extracting data and how data will be extracted. The purpose of extracting data is to pursue reasonable lines of enquiry. The topic has been the subject of recent case law.[50]

18.97 Big Brother Watch submit that the current procedures fall foul of the General Data Protection Regulation ("GDPR"). This is because:

(1) consent cannot be considered to be "freely given" in current practices due to the imbalanced relationship between the complainant and police, the likelihood of trauma, and complainants' competing considerations such as justice and public safety;

(2) the consent is not specific, but rather performs as a catch-all abdication of data protection rights and the right to privacy under article 8 of the ECHR; and

(3) consent may not be fully informed because complainants would not reasonably expect the sheer scale of data seizure and examination into their private lives or the complex legal and practical implications that could arise in the course of the investigation and trial.

18.98 The question of whether this practice complies with the GDPR and Data Protection Act 2018, namely that consent must be free and informed, was considered by the ICO. In addition to its report published in June 2020,[51] which highlights the inappropriateness of consent as a condition for processing personal data,[52] the ICO is due to report later this year on a broader investigation that it is carrying out into the processing of victims' data in the criminal justice system.

18.99 There is also a question of whether extracting data in this way amounts to an offence of unlawful interception under IPA. As explained at paragraph 14.56(2) above, consent can only be a lawful basis for the interception of communications where the sender and the intended recipient of the communication have each consented to its interception,[53] or if either the sender or the intended recipient has consented and direct surveillance has been authorised under part 2 of RIPA.[54] We raise this to indicate matters requiring consideration: we do not express a view on this issue for it would be inappropriate to pre-empt any future review that might take place.

18.100 For the above reasons, we consider the extraction of electronic data from complainants' electronic devices should be considered as part of a wider review of the law governing the acquisition and treatment of electronic material in criminal investigations.

---

50 See *R v Bater-James* [2020] EWCA Crim 790 in which the Court of Appeal provided guidance on obtaining and examining witness's electronic devices. See also *R v McPartland* [2019] EWCA Crim 1782, [2019] 4 WLR 153 at [44] for a case in which the Court of Appeal criticised the taking and analysis of a complainant's mobile phone.

51 Information Commissioner's Office, *Investigation report: Mobile phone data extraction by police forces in England and Wales* (June 2020). Accessible at https://ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/.

52 Information Commissioner's Office, *Investigation report: Mobile phone data extraction by police forces in England and Wales* (June 2020) p 62. Accessible at https://ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/.

53 Investigatory Powers Act 2016, s 44(1).

54 Investigatory Powers Act 2016, s 44(2).

Recommendation 64

18.101 We recommend a wider review of the operation of powers of search, production and seizure in respect of electronic material when investigating criminal offences not confined to cases where such powers are exercised pursuant to a search warrant or in respect of premises. In particular, such a review should consider:

(1) whether law enforcement have the necessary powers to investigate crime where remotely stored data is involved; and

(2) whether sufficient safeguards accompany such powers to ensure that they are used only where necessary and proportionate.

Chapter 19: Consolidating search warrants legislation

INTRODUCTION

19.1 In this chapter, we discuss the desirability of consolidating search warrant provisions, as well as repealing unnecessary provisions and standardising certain statutory conditions. In our Consultation Paper, we identified 176 search warrant provisions contained in 138 separate pieces of legislation. Since publication, four more search warrant provisions have been added to the statute book.[1] Each provision has its own grounds for issuing a warrant and its own conditions under which the warrant can be executed. In addition to authoring entry and search, some provisions authorise associated powers (for example the use of reasonable force or testing equipment on premises).

19.2 In the consultation paper, based on discussions with stakeholders, we noted that the sheer number of provisions puts a significant burden on issuing authorities and investigative agencies who deal with a wide range of warrants. We received evidence from stakeholders that some agencies find it difficult to decide the most suitable provision under which to apply for a search warrant. We were also informed that warrants have been refused because the issuing authority considered that the application should have been made under different legislation.

19.3 We were informed by several stakeholders that the number and complexity of search warrant powers often leads to errors. To address these issues, in Chapter 11 of the consultation paper, we asked a series of consultation questions about legislative repeal, consolidation (either wholesale or by grouping related powers) and codification (ie creating common conditions across provisions). We discuss each of these options in more detail below:

(1) repealing unnecessary search warrant provisions;

(2) consolidating search warrant provisions into a single statute;

(3) alternatively, partially consolidating search warrant provisions into related groups of powers; and

(4) standardising the accessibility conditions through codification.

19.4 We do not recommend the repeal of any search warrant provisions in this chapter because we have insufficient evidence to conclude that particular provisions are obsolete and that their repeal would not adversely affect enforcement powers. Instead, we set out possible methods by which potentially obsolete search warrant provisions could be identified in the future.

19.5 As for consolidation, we remain of the view expressed in our consultation paper that search warrants legislation should not be consolidated into a single statute, either through

---

1 Public Health (Minimum Price for Alcohol) (Wales) Act 2018, s 14; Ivory Act 2018, s 17; Counter-Terrorism Act 2008, s 56A (inserted by the Counter-Terrorism and Border Security Act 2019, s 13); Wild Animals in Circuses Act 2019, sch 1, para 3.

codification or "strict consolidation".[2] Search warrant provisions form part of wider enforcement regimes and sit better in the statutes that regulate each law enforcement agency more generally, especially given the presence of related investigative powers in those statutes that interact with search warrant provisions. The burden of consolidation, in terms of the Law Commission, Parliamentary Counsel, consultees and Parliament's time, would be unlikely to outweigh any benefit. Other changes, including issuing clearer guidance, would be a more proportionate response to the problems with the current law.

19.6 For the reasons above, we also do not consider it desirable to pursue partial consolidation by grouping related search warrant provisions, nor the standardisation of accessibility conditions given that the sets of conditions are tailored to the particular statutory regime.

REPEALING UNNECESSARY SEARCH WARRANT PROVISIONS

The consultation paper

19.7 Stakeholders with whom we spoke while drafting our consultation paper indicated that some statutory provisions are now redundant in light of the general nature of section 8 of the Police and Criminal Evidence Act 1984 ("PACE"). Professor Richard Stone argued that, given the broad nature of section 8 of PACE, many specific search warrant provisions could potentially be repealed without any adverse effects on police powers.

19.8 Rupert Bowers QC of Doughty Street Chambers agreed that section 8 covers most situations and pointed out that the provisions for issuing warrants in the Theft Act 1968 ("TA 1968"), Misuse of Drugs Act 1971 ("MDA 1971"), Sexual Offences Act 2003 ("SOA 2003") and others seem to be unnecessary given the existence of section 8 of PACE, but warrants under these provisions are still often sought.

19.9 The Metropolitan Police Service ("MPS") agreed that section 8 of PACE will invariably be the provision of choice. However, they noted that the existence of other provisions may lead the issuing authority to question why a section 8 warrant was sought. For example, where a large quantity of drugs is allegedly imported, the issuing authority may query why a search warrant under the MDA 1971 was not sought.

19.10 Samantha Riggs, a barrister at 25 Bedford Row, reported a similar experience in two cases involving environmental offences. In a case in London, the application for a warrant was made under the Environment Act 1995 and criticised on the grounds that it should have been made under PACE. In an almost identical case in Liverpool, the application was made under PACE and criticised on the grounds that it should have been made under the Environment Act 1995.

19.11 In the light of this experience, we invited consultees' views on whether there are any search warrant provisions that are unnecessary and therefore ought to be repealed.[3] We pointed out that care must be taken to avoid leaving gaps in investigatory powers by repealing statutory provisions without due consideration.

---

2 We use this term to mean consolidation which would not in itself effect a change in the law.

3 Consultation Question 58.

Consultation responses

19.12 Twelve consultees[4] answered this question. Several consultees agreed in principle that powers which replicate section 8 of PACE should be repealed.[5] They argued that to do so would help to make applications more consistent[6] and make the law simpler for applicants.[7]

19.13 Consultees indicated that the following provisions are now obsolete owing to section 8 of PACE:

(1) section 23(3) of the MDA 1971;[8]

(2) section 26 of the TA 1968;[9] and

(3) section 4 of the Protection of Children Act 1978 ("PCA 1978").[10]

19.14 Professor Richard Stone suggested that a survey of which powers are currently used would be helpful in order to identify which powers could be repealed.

19.15 Some consultees stated that they were unaware of any unnecessary search warrant provisions.[11]

Analysis

19.16 We remain of the view that, in principle, obsolete search warrant provisions should be repealed. We agree that repealing unnecessary provisions would make applications more consistent and reduce the likelihood of warrants being refused because the issuing authority is of the view that it should have been applied for under different legislation.

19.17 We did not receive sufficient evidence to enable us to conclude that any particular search warrant provisions are unnecessary and suitable for repeal. Given the potential risk of creating gaps in enforcement regimes, we make no recommendations as to repeal.

19.18 Four search warrant provisions were identified as being obsolete by three consultees, and one stakeholder otherwise than in a consultation response.[12] We have concluded that

---

4 DS Clayton Ford; Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Birmingham Law Society; The Law Society; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; Metropolitan Police Service; National Crime Agency; Competition and Markets Authority.

5 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Birmingham Law Society; Justices' Clerks' Society; Magistrates Association; Metropolitan Police Service.

6 Justices' Clerks' Society.

7 Metropolitan Police Service.

8 HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate).

9 HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate).

10 DS Clayton Ford, Essex Police.

11 Law Society; National Crime Agency; Competition and Markets Authority.

12 Theft Act 1968, s 26; Misuse of Drugs Act 1971, s 23(3); Protection of Children Act 1978, s 4; Sexual Offences Act 2003, s 96B.

repealing these provisions may adversely affect the police's investigative powers for the following reasons:

(1) *Section 26(1) of the TA 1968* – a search warrant issued under the TA 1968 can authorise the search of persons. Given that a search warrant issued under section 8 of PACE cannot authorise a search of persons, section 26 of the TA 1968 is not, in our view, obsolete. We recommend at Recommendation 28 that section 8 of PACE is amended such that if particular conditions are met a search of persons will be permissible. If section 8 of PACE were amended, we consider that section 26 of the TA 1968 could be repealed without adversely affecting police powers.

(2) *Section 23(3) of the MDA 1971* – as with the TA 1968, a search warrant under the MDA 1971 permits the search of persons. It also has a lower threshold than section 8 of PACE for granting a warrant: the issuing authority need only be satisfied that there are reasonable grounds for suspecting, rather than believing, the statutory access conditions have been met.

(3) *Section 4 of the PCA 1978* – as with the MDA 1971, the PCA 1978 only requires the issuing authority to be satisfied that there are reasonable grounds for suspecting, rather than believing, the statutory access conditions have been met.

(4) *Section 96B of the SOA 2003* – the power under the SOA 2003 is much narrower than that under section 8 of PACE. This reflects the purpose of the provision: to enable a police officer to enter premises in order to assess the risks posed by a person subject to notification requirements. This assessment could not be carried out under section 8 of PACE, which is designed to enable police to search for evidence, and not to assess a person who has already been convicted of a specified offence or received a caution.

19.19 In our examination of whether any search warrant provisions are unnecessary and ought to be repealed, we have taken into consideration the review of powers of entry conducted from 2013 to 2014. This review stemmed from the Protection of Freedoms Act 2012, which placed a duty on Secretaries of State to review the powers of entry for which they are responsible, which included search warrant provisions. The purpose of the review was to examine each power and decide, amongst other things, if that power was still required or should be repealed.

19.20 Cabinet Ministers of each department laid their final reports in Parliament on 27 November 2014,[13] which showed that a total of 1,237 powers of entry had been reviewed. To date, no powers of entry have been repealed.[14] We are not aware of any search warrant provisions that were identified as candidates for repeal. This might indicate that there are no unnecessary search warrant provisions on the statute book, however, it is difficult to assess the truth of this without knowing the reasoning adopted for retaining each search warrant provision.

19.21 Our consultation and stakeholder engagement revealed only four candidates for repeal, however, there are two other possible approaches to identifying unnecessary search warrant provisions. The first approach is to assess each search warrant provision to determine

---

13 See https://www.gov.uk/government/collections/reviews-of-all-powers-of-entry.

14 See *Post-Legislative Scrutiny of the Protection of Freedoms Act 2012* (6 March 2018) p 34, https://www.gov.uk/government/publications/post-legislative-scrutiny-of-the-protection-of-freedoms-act-2012 .

whether a functionally equivalent power exists. We have done this above for the four search warrant provisions drawn to our attention.[15] The resources available for this project do not permit us to consider all 169 remaining powers in detail. In addition, any candidate for repeal should be the subject of further consultation in order to take into account the views of law enforcement agencies and departments before reaching a firm conclusion.

19.22 The second approach would be to analyse search warrants data. It may be possible to identify redundant search warrant provisions based on the number of times that search warrants are sought under each provision. If a provision is never used, that would be a strong indication that it is no longer needed, and this could trigger the further analysis and consultation described above. However, the contrary does not follow: Just because search warrants are still applied for under a particular provision does not mean that there is not a functionally equivalent power which renders that provision obsolete. There are also search warrant provisions that are rarely used, such as section 9 of the Official Secrets Act 1911, that relate to national security and whose powers are not replicated in other provisions.

19.23 At present, data permitting the analysis described in the previous paragraph does not exist. We recommend that such data be collected and reported at Recommendation 24.

CONSOLIDATING ALL SEARCH WARRANT PROVISIONS

19.24 It is important to distinguish between two forms of consolidation. The first would involve altering the law through codification to bring all search warrant provisions under a single statute with either a single set, or several sets, of conditions and powers. The second form of consolidation would involve creating a single statute which contains all of the law on search warrants but does not actually alter the law (what we termed strict consolidation). An example of this second form of consolidation is the Law Commission's recent sentencing code project, which is in the process of being implemented through the Sentencing Bill and Sentencing (Pre-consolidation Amendments) Act 2020.[16]

The consultation paper

19.25 Many of the stakeholders we spoke to while writing the consultation paper argued that consideration should be given to consolidating all search warrant provisions into a single regime. Further suggestions were made to consolidate codes of practice, guidance and related powers of seizure. It was also argued that codification would make the law clearer and easier to navigate.

19.26 However, the prospect of some or all search warrant provisions being codified concerned some stakeholders. The Serious Fraud Office ("SFO") considered that interfering with a bespoke suite of investigative powers such as theirs risked disrupting regimes that function well and diluting search powers in undesirable ways.

19.27 Another concern was that jurisdictional anomalies might arise: for example, the SFO's enforcement powers extend to Northern Ireland.[17] Codifying the search warrant provisions in England and Wales would mean that the SFO's search powers in England and Wales would

---

15 Theft Act 1968, s 26; Misuse of Drugs Act 1971, s 23(3); Protection of Children Act 1978, s 4; Sexual Offences Act 2003, s 96B.

16 The Sentencing Code – Volume 1 (2018) Law Com No 382.

17 Criminal Justice Act 1987, s 17(3).

have a different statutory footing to their search powers in Northern Ireland. Similar concerns were expressed by the legal adviser to the Royal Military Police and Deputy Director of Service Prosecutions, who both considered that service law search warrants ought to remain within a stand-alone military law code.

19.28 Jonathan Hall QC, a barrister at 6KBW College Hill, also made the point that separate powers for separate agencies can be a good thing, as it keeps agencies focused on their specific remit. Further, agencies become accustomed to using their search powers, which reduces the risk of error.

19.29 Consolidating all search warrant provisions would be a significant undertaking, even if confined to warrants issued for the purposes of a criminal investigation. For the reasons set out above, we considered that the disadvantages of consolidating all search warrant provisions outweighed the benefits. Accordingly, we provisionally concluded[18] that there should not be a single statute consolidating all search warrant provisions.

Consultation responses

19.30 Seventeen consultees expressed views about whether there should be a single statute consolidating all search warrant provisions. Of those, 15 were against consolidating all search warrant provisions;[19] and two were in favour of consolidation.[20]

19.31 There was almost complete agreement among consultees that there should not be a single statute consolidating all search warrant provisions. Some consultees considered that the biggest hurdle is how varied search warrant provisions are: what powers are authorised, who can exercise those powers and the purpose of the search warrant differs from one provision to another.[21] The scale of the task also led one consultee to conclude that any benefits would be outweighed by the amount of work that would be required.[22]

19.32 The point was also made that consolidation may lead to jurisdictional confusion of the kind described at paragraph 19.27 above.[23] Given this, it was suggested that consolidation would create more problems than it solves.[24]

19.33 A few consultees also proposed that greater transparency and clarity could be achieved through other means, such as clearer guidance.[25] The Justices' Clerks' Society stated that issuing explanatory material and/or guidance to investigators and courts is more important

---

18 Consultation Question 59.

19 Professor Richard Stone; HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Kent County Council Trading Standards; Southern Derbyshire Magistrates' Bench; The Law Society; Independent Office for Police Conduct; Justices' Clerks' Society; Magistrates Association; Bar Council and the Criminal Bar Association; Metropolitan Police Service; Competition and Markets Authority; Financial Conduct Authority; Serious Fraud Office; National Crime Agency.

20 Birmingham Law Society; Dijen Basu QC.

21 HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Southern Derbyshire Magistrates' Bench; Justices' Clerks' Society.

22 Magistrates Association.

23 Magistrates Association.

24 Justices' Clerks' Society.

25 Magistrates Association.

than consolidating legislation. They hoped that full and detailed guidance for investigators on each power, which could be updated with new case law as necessary, could be produced urgently.

19.34 Consultees also emphasised that consolidation may mean that the unique features of specialist regimes are lost.[26] In particular, there is a risk that creating a single procedure designed for all law enforcement agencies could weaken the protections that exist in specialist regimes.[27]

19.35 Some consultees disagreed. One consultee did not agree that having their own statutory regime focuses authorities on their remit.[28] The example was given of the Proceeds of Crime Act 2002 ("POCA"), under which different agencies have their own sets of powers under separate chapters of the legislation.

19.36 Another consultee argued that a single search warrants statute would make it easier for the issuing authority to assess applications, improve consistency for investigators and make it possible to design a single interactive warrant application form and code of practice.[29]

Analysis

19.37 We have considered the desirability of both forms of consolidation (codification and strict consolidation) in the light of consultees' responses. On balance, we remain of the view that there should not be a single statute consolidating all search warrant provisions, be it through codification or strict consolidation.

Codifying search warrant provisions in a single statute

19.38 We still consider that codifying search warrant provisions would risk diluting or rendering inoperable law enforcement powers. If the statutory conditions and associated powers within search warrant provisions are merged, some agencies may have to satisfy more onerous conditions for the grant of a search warrant or lose powers exercisable on premises that they current have. Further, search warrant provisions invariably form part of a wider set of enforcement powers which are tailored to particular agencies and interact with other investigative powers. Therefore, having a range of search warrant provisions with different access conditions and associated powers is justified by the differing purposes of statutory regimes.

19.39 To illustrate this point, take the power of the SFO to apply for a search warrant under section 2(4) of the Criminal Justice Act 1987 ("CJA"). The statutory access conditions are predicated on non-compliance with, or the impracticability of serving, an information notice under section 2(3) of the CJA. Excising the search warrant provision of the CJA would first mean that the SFO would have to straddle between two enforcement regimes when exercising investigative powers. The fact that the CJA search warrant provision dovetails with the CJA information notice provision and permits the search for a wider category of material than can be searched for under section 8 of PACE means that a single clear and comprehensible

---

26 Kent County Council Trading Standards; Law Society; Serious Fraud Office; Metropolitan Police Service; Competition and Markets Authority; Serious Fraud Office.

27 Competition and Markets Authority.

28 Birmingham Law Society.

29 Dijen Basu QC.

overarching search warrant power could not be drafted that retains the nuances of each pre-existing regime.

19.40 We recognise that some statutes, like POCA, contain enforcement regimes which are utilised by several different agencies. However, the scale and subject matter of POCA is far more limited than the entire landscape of search warrant provisions. Another example is the Crime (Overseas Production Orders) Act 2019, which contains a single regime under which multiple agencies can apply for an overseas production order. Its scope, however, is narrow: it is limited to investigating indictable offences or terrorism. It therefore does not capture the variety of purposes for issuing a search warrant, which include obtaining evidence, rescuing persons[30] or animals,[31] assessing compliance with certain conditions,[32] and immobilising dangerous objects.[33]

19.41 We are not persuaded that consolidation would make the law clearer or easier to navigate for applicants and issuing authorities. In this regard, it is helpful to compare search warrants legislation with the law on sentencing. It is useful for a judge to have a single reference point when sentencing an offender, given how varied sentencing powers are. In contrast, when issuing a search warrant, the issuing authority need only consider whether the statutory access conditions for that particular warrant are satisfied.

19.42 Furthermore, each law enforcement agency, or internal department within that agency, will apply for the same limited set of warrants. For example, a police unit investigating firearms offences will likely only apply for search warrants under section 8 of PACE or section 46 of the Firearms Act 1968. By way of another example, the Competition and Markets Authority need only be aware of the search warrant provisions under the Competition Act 1998, the Enterprise Act 2002 and the Consumer Rights Act 2015. Similarly, the SFO need only concern themselves with the search warrant provisions under the Criminal Justice Act 1987 and POCA.

19.43 Another important distinction between search warrants law and sentencing law is the empirical research which underpins the consolidation exercise. A study conducted on sentencing appeals before the Court of Appeal (Criminal Division) indicated that 36% of sentences passed were wrong in law.[34] The sentencing code proposed by the Law Commission seeks to reduce the number of unlawful sentences by providing a single reference point. In relation to search warrants, there is no evidential basis to suggest that significant problems arise in practice due to the sheer number of search warrant provisions on the statute book, nor that consolidation would lead to fewer defective warrants.

The strict consolidation of search warrant provisions in a single statute

19.44 We do not consider that consolidation would be any more desirable if it were limited to strict consolidation that would not substantively affect the law. We accept that the central plank of the argument against consolidation, namely the risk of diluting current law enforcement powers, falls away if strict consolidation is pursued.

---

30 Mental Health Act 1983, s 135.

31 Animal Welfare Act 2006, s 19.

32 Sexual Offences Act 2003, s 96B.

33 Chemical Weapons Act 1996, s 5(2).

34 R Banks, *Banks on Sentencing* (8th ed 2013), vol 1, p xii.

19.45 The only effect of strict consolidation would be to have all search warrant provisions in a single Act. The benefit to be gained from this, if any at all, would be substantially outweighed by the time spent achieving it. We remain convinced that a single consolidated statute would not render search warrants law clearer and more accessible. It would be an unwieldy piece of legislation if all the access conditions, associated powers and statutory definitions were retained. It may also in fact increase the risk of errors being made when warrants are applied for, issued, and executed as investigators would have to swap between different the new search warrants act and their splintered enforcement regimes when exercising powers.

19.46 Consolidation could therefore not easily be limited to search warrants. As discussed at paragraph 19.38 above, search warrants often form part of a package of enforcement powers. There are often powers to compel production, enter without a warrant and enter under warrant within an agency's enforcement regime. If search warrant powers alone were removed from agencies' enforcement regimes, gaps would be left behind. An investigator would have to refer to their own bespoke regime until a warrant is sought, at which point they would have to switch to the new search warrants legislation.

19.47 Investigative powers form a network of interdependent provisions.[35] For instance, enforcement provisions concerning compulsory production may refer to search warrant provisions, and vice versa. Obtaining a search warrant is typically a measure of last resort where other investigatory powers have been exhausted or are impracticable. Search warrant provisions would therefore not be easily severable from broader enforcement regimes in which they sit.

19.48 Therefore, even if we were convinced that consolidation in either form was worthwhile, the case for limiting it to search warrant provisions is unconvincing. Given the interconnected nature of investigative powers, any discussion about consolidating search warrant provisions would have to take place within a broader discussion of consolidating all enforcement powers.

19.49 We also agree with the observations made by the Magistrates Association and Justices' Clerks' Society that detailed guidance on using search warrant powers would be valuable. To that end, we make several recommendations in this report concerning issuing or updating guidance on search warrants. We are also persuaded that a practitioners' text in this area would be useful.

19.50 Part of the rationale behind consolidation is the sheer number of search warrant provisions on the statute book. One of the strands of the Government's policy on legislative powers of entry is to limit the creation of new powers to those that are necessary and proportionate. Consequently, departments cannot create new powers of entry or modify old ones without achieving "collective policy agreement". In practice, this means that departments should:

> Consider carefully whether a new power is necessary, other similar powers might be applied, or whether alternative enforcement options or sanctions could be used instead.[36]

19.51 Given that this guidance was issued recently, we hope that the risk of unnecessary overlap between powers will decrease over time. Where law enforcement agencies remain able to

---

35 Alex Davidson, "Extraterritoriality and Statutory Interpretation: The Increasing Reach of Investigative Powers" (2020) 1 *Public Law* 1 at 13.

36 Home Office, *Powers of Entry Guidance for Departments* (2018), p 5.

apply for a warrant under more than one provision, we consider that the following observation of the Administrative Court should be borne in mind:

> Where Parliament provides two different procedures which are available to the state in respect of the same subject matter … it is for the state to choose which to use. The state ought to choose the procedure which will produce the greatest benefit to the public, providing that no injustice is caused to the respondent.[37]

PARTIAL CONSOLIDATION OF SEARCH WARRANT PROVISIONS

The consultation paper

19.52 After concluding that search warrant provisions should not be consolidated in their entirety through either codification or strict consolidation, we considered whether a more limited exercise, consolidating only certain categories of powers, would be beneficial.

19.53 After examining the underlying purposes of search warrant provisions and the statutory access conditions, we reached the preliminary view that there were three possible headings under which search warrants could be consolidated. Accordingly, we invited consultees' views on whether it would be beneficial to pursue some degree of consolidation of those search warrants concerned with the following common purposes.

(1) *Search warrants for the purpose of finding evidence relevant to a criminal offence* – the main search warrant provision used to find evidence relevant to a criminal offence is section 8 of PACE. Several other search warrant provisions are similar to section 8 of PACE, however, there are crucial differences. Some search warrant provisions:

(a) apply not only to a possible offence which has been committed, but also to a possible offence which is being or is about to be committed, on the premises or elsewhere;[38]

(b) require a lower threshold of reasonable grounds to suspect, rather than reasonable grounds to believe;[39]

(c) do not require an application to be made by a constable;[40] or

(d) allow an application in respect of summary only offences.[41]

(2) *Search warrants sought to remedy dangerous or unlawful situations* – some warrants are issued because there is potentially a forbidden article or a dangerous or unlawful situation on the premises rather than evidence of the commission of an offence. In

---

37 *National Crime Agency v Simkus* [2016] EWHC 255 (Admin), [2016] 1 WLR 3481 at [105].

38 Firearms Act 1968, s 46(1); Customs and Excise Management Act 1979, s 118C; Copyright Act 1996, 21A; Chemical Weapons Act 1996, s 29; Biological Weapons Act 1974, s 4;

39 Firearms Act 1968, s 46(1); Misuse of Drugs Act 1971, s 23(3).

40 Criminal Justice Act 1987, s 2(4); Financial Services and Markets Act 2000, s 176; Proceeds of Crime Act 2002, s 352.

41 Animal Welfare Act 2006, s 23(1); Conservation of Habitats and Species Regulations 2017 (SI 2010 No 1012), reg 115(3).

some cases, the remedying of the dangerous or unlawful situation is the sole purpose of the warrant and not the collection of evidence.[42]

(3) *Search warrants in default of production orders* – some warrants are issued as part of more complex investigations, for example in the field of financial services. These do not necessarily involve a criminal offence, although a criminal prosecution may be one option considered by the investigator.[43]

19.54 We invited consultees' views on whether consolidation in respect of the three categories outlined above would be desirable, and if so what degree of consolidation.[44] We also asked whether consultees favoured any schemes of consolidation not described above, and if so what.[45]

Consultation responses

19.55 Sixteen consultees responded to the question asking whether it would be beneficial to consolidate search warrants concerned with finding evidence relevant to suspected criminal offences: nine agreed;[46] five disagreed;[47] and three expressed other views.[48]

19.56 Ten consultees responded to the question asking whether it would be beneficial to consolidate search warrants concerned with preventing or remedying dangerous or unlawful situations: five agreed;[49] and five disagreed.[50]

19.57 Twelve consultees responded to the question asking whether it would be beneficial to consolidate search warrants concerned with investigations in which production orders or similar procedures are available: four agreed;[51] five disagreed;[52] and three expressed other views.[53]

---

42 Mental Health Act 1983, s 135.

43 Competition Act 1998, s 28; Financial Services and Markets Act 2000, s 176.

44 Consultation Questions 60, 61 and 62.

45 Consultation Question 63.

46 HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Council of Her Majesty's Circuit Judges; West London Magistrates' Bench; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; Metropolitan Police Service.

47 Bar Council and the Criminal Bar Association; Competition and Markets Authority; Financial Conduct Authority; Serious Fraud Office; Law Society.

48 Professor Richard Stone; National Crime Agency; Whitehall Prosecutors' Group.

49 HM Council of District Judges (Magistrates' Court); Senior District Judge (Chief Magistrate); Justices' Clerks' Society; Magistrates Association; Dijen Basu QC.

50 Kent County Council Trading Standards; The Law Society; Bar Council and the Criminal Bar Association; Competition and Markets Authority; Financial Conduct Authority.

51 Senior District Judge (Chief Magistrate); Justices' Clerks' Society; Magistrates Association; National Crime Agency}.

52 The Law Society; Bar Council and the Criminal Bar Association; Competition and Markets Authority; Financial Conduct Authority; Serious Fraud Office.

53 HM Council of District Judges (Magistrates' Court); Kent County Council Trading Standards; Dijen Basu QC.

19.58 Three consultees answered the question about whether a different scheme of consolidation should be pursued.[54]

Partial consolidation in general

19.59 Some consultees discussed partial consolidation in general rather than any particular form of consolidation.

19.60 Several agreed with partial consolidation where possible. They argued that it would improve consistency and increase the likelihood of agencies applying the correct statutory test.[55] As one consultee put it:

> the fewer provisions for obtaining search warrants and the more consistent they are, the more likely that correct, appropriate applications will be made and granted by the court and thereafter, the more likely that warrants will be properly executed.[56]

19.61 However, there was little detailed discussion about the form partial consolidation should take. One consultee suggested that the distinction between there being reasonable grounds to suspect and reasonable grounds to believe that an offence has been committed is unnecessary and that provisions could be made more consistent with a single formulation.[57]

19.62 Other consultees did not support partial consolidation. Some saw no benefit either generally,[58] or as it would apply to their investigative regimes.[59] One consultee did not believe that partial consolidation along the lines we suggested would be feasible, as it would require a very substantial degree of legal analysis to ensure that law enforcement agencies retained properly functioning enforcement powers.[60]

19.63 One consultee supported partial consolidation where possible, but did not consider it a priority. They argued that having clear guidance covering each power was more important.[61] Another consultee suggested that it would be unnecessary to seek further consolidation if those provisions which duplicate section 8 of PACE were repealed.[62]

19.64 Some consultees also argued that ensuring that warrants permit the effective search and seizure of electronic material is more important than pursuing consolidation.[63]

---

54 HM Council of District Judges (Magistrates' Court); The Law Society; Justices' Clerks' Society.

55 Magistrates Association.

56 Metropolitan Police Service.

57 West London Magistrates' Bench.

58 Law Society.

59 Competition and Markets Authority; Serious Fraud Office.

60 Financial Conduct Authority.

61 Justices' Clerks' Society.

62 Professor Richard Stone.

63 Whitehall Prosecutors' Group; National Crime Agency.

Consolidating search warrants relating to evidence of a criminal offence

19.65 One consultee agreed in principle with consolidating search warrants relating to finding evidence, but did not think that consolidation should include the provisions under the Terrorism Act 2000 given that it is a bespoke regime.[64]

19.66 Another consultee provided a suggestion as to the form which consolidation could take.[65] Some search warrant provisions are hybrids, in that they concern both obtaining evidence and remedying dangerous or unlawful situations. This consultee suggested that the preventative elements of search warrant provisions could be severed and preserved in part of an Act. The relevant offences or situations which the provisions seek to prevent could then be included in a schedule to the Act, along with a description of the person or persons entitled to apply for each warrant.

Consolidating search warrants to remedy dangerous situations

19.67 The only consultation response which discussed consolidating search warrants sought to remedy dangerous or unlawful situations expressed concern that these powers would be difficult to consolidate as they vary so significantly and are likely to be enforced by different agencies.[66]

Consolidating search warrants issued in default of production orders

19.68 HM Council of District Judges (Magistrates' Court) considered that partial consolidation could potentially be achieved by consolidating the statutory conditions and then including the items that should be produced under a given production order in a separate schedule. Dijen Basu QC suggested that production orders should be rolled up into the same Act as search warrants, just as schedule 1 to PACE provides statutory conditions for both warrants and production orders.

19.69 The Law Society argued that consolidating these warrants could be detrimental to the agencies who use them because they are part of a specialised set of powers which are integral to specialist investigations.

Different schemes of consolidation

19.70 Only HM Council of District Judges (Magistrates' Court) suggested methods of consolidation beyond those outlined by us. They suggested consolidating:

(1) search warrants relating to special procedure material, excluded material and legally privileged material; and

(2) search warrants relating to terrorism.

Analysis

19.71 On balance, we do not consider that partial consolidation of search warrant provisions would be desirable because it would not overcome the issues which we identified in the previous section.

---

64 Senior District Judge (Chief Magistrate).

65 Dijen Basu QC.

66 Kent County Council Trading Standards.

19.72 In respect of codification, we have concluded that even partial consolidation risks diluting or rendering inoperable law enforcement powers for the reasons set out at paragraphs 19.38 and 19.39 above. Even where search warrants have similar purposes, the access conditions and associated powers will often be tailored to the purpose of the search warrant in question. For example, we think it is right that the access conditions under section 29 of the Chemical Weapons Act 1996 allow for a warrant to be obtained where there are reasonable grounds for suspecting that an offence under that Act is about to be committed. However, this statutory access condition would be too broad for section 8 of PACE, which applies to all indictable offences.

19.73 In addition, many of the problems identified above in relation to complete consolidation also apply to partial consolidation. First, while some acts contain a single enforcement regime which can be utilised by several agencies, the number of and variations between search warrant provisions make adopting this approach unsuitable. Secondly, partial consolidation is unlikely to make the law clearer or easier to navigate. Thirdly, when applying for a search warrant, each law enforcement agency and internal department will apply for the same limited set of warrants. Finally, we do not have the evidential basis to suggest that significant problems arise in practice due to the sheer number of search warrant provisions on the statute book.

19.74 We are also of the view that partial consolidation would be no more desirable if it were limited to strict consolidation. Partially consolidated acts may be clearer and more accessible than an act which consolidated all search warrant provisions, but may still be less accessible than the current law. The concerns we raised above about creating gaps by removing search warrant provisions from broader enforcement regimes and consolidating search warrants in a vacuum also apply.

19.75 It may be the case that some form of very minimal consolidation would avoid the above concerns. However, the benefits of consolidation on such a small scale, if any, would be nominal.

STANDARDISING THE ACCESSIBILITY CONDITIONS

The consultation paper

19.76 Each search warrant provision has a set of statutory conditions which must be satisfied in order for a warrant to be issued. These may include that there are reasonable grounds for believing that an offence has been committed and that there is relevant material on the premises. We refer to these as “access conditions”.

19.77 Most access conditions include a requirement that the warrant is needed because the material cannot be obtained by other means. For example, section 8(1)(e) of PACE states that there must be reasonable grounds for believing that any of the conditions specified in section 8(3) apply. These conditions include that it is not practicable to communicate with any person entitled to grant entry to the premises or that entry to the premises will not be granted unless a warrant is produced.

19.78 The exact conditions vary from one statute to another. We therefore use the term “accessibility conditions” to describe the subset of access conditions that relate to the impracticability of gaining access to the premises or material without a search warrant.

19.79 We identified variations across the accessibility conditions. For one, the accessibility conditions themselves varied across provisions. Another variation was that, in some

provisions, the issuing authority need only be satisfied that there is reason to believe that one of the accessibility conditions is met; in others they must be satisfied that one of the conditions is in fact met. We considered that it would make more sense if:

(1) where the condition relates to a verifiable past or existing fact (such as that admission has been refused or that the premises are unoccupied), the issuing authority must be satisfied of the truth of that fact; and

(2) where the condition relates to a person's state of mind or a hypothetical prediction (such as that admission is likely to be refused or that giving notice would defeat the object of the investigation), the issuing authority need only have reasonable grounds for belief or suspicion.

19.80 To this end, we provisionally proposed[67] that there should be a standard set of accessibility conditions for all search warrant provisions.

19.81 We invited consultees who agreed to give us their views on whether those accessibility conditions should include that the issuing authority has:

(1) reason to believe that, without a warrant, the investigator could not obtain access to the premises within a reasonable time or at all (and it is not reasonably practicable to identify or have access to the required material without access to those premises);

(2) reason to believe that, without a warrant, the investigator could not obtain access to the materials within a reasonable time or at all; and

(3) reason to suspect that, unless a warrant is issued, the materials might be destroyed, tampered with, concealed or removed or the purposes of the investigation might be otherwise impeded or frustrated.

19.82 We also invited consultees' views on whether, in appropriate cases, there should be further conditions, depending on the purpose of the power, such as that:

(1) a production order has been made and not complied with; or

(2) there are reasonable grounds for suspecting that immediate access to the premises or the materials is required to prevent a dangerous situation or rescue a person or animal in pain or danger.

Consultation responses

19.83 Sixteen consultees answered these questions: 12 agreed with our provisional proposal that there should be a standard set of accessibility conditions for all search warrant provisions;[68] and four disagreed.[69] Although most consultees agreed with our provisional proposals, very

---

67 Consultation Question 64.

68 Professor Richard Stone; Senior District Judge (Chief Magistrate); Birmingham Law Society; Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate; Southern Derbyshire Magistrates' Bench; Independent Office for Police Conduct; The Law Society; Justices' Clerks' Society; Magistrates Association; Dijen Basu QC; Metropolitan Police Service; National Crime Agency.

69 Bar Council and the Criminal Bar Association; Competition and Markets Authority; Financial Conduct Authority; Serious Fraud Office.

few provided reasons to support their position. Of those who did provide detailed responses, none agreed with the proposed accessibility conditions wholesale.

19.84 Two consultees were confused why the mental element was not the same across all of the accessibility conditions we suggested.[70] The tests which we set out at paragraph 19.81 above use the phrase "reasons for believing" as the mental element for conditions (1) and (2) but "reasons for suspecting" as the mental element for condition (3). One consultee suggested elevating the test in (3) to reasonable belief to align with (1) and (2).[71]

19.85 As for further conditions, one consultee agreed with including as an accessibility condition that no production order has been sought because there are reasonable grounds for believing that it would not be complied with.[72] It was also suggested that the additional access conditions we proposed could be swept up into a broader public interest test, which could include a number of non-exhaustive examples.[73] Another consultee queried how a "dangerous situation" would be defined.[74]

19.86 Some consultees strongly disagreed with our provisional proposal. They argued that a uniform set of accessibility conditions could not apply equally to all types of warrant or replicate the conditions available under current legislation.[75] Therefore, any uniform set of accessibility conditions would still need to be tailored to individual statutory regimes, rendering standardisation of little use.

19.87 Several law enforcement consultees expressed concern that standardising accessibility conditions may weaken protections for those under investigation or make it more difficult to investigate alleged criminality.[76] For example, the Financial Conduct Authority argued that our proposals would have a negative impact on their regime under the Financial Services and Markets Act 2000. First, it would remove avenues currently available under their regime to obtain a search warrant. Secondly, it would remove some of the statutory preconditions necessary to obtain a warrant. Thirdly, the proposals fail to recognise the distinct nature of search warrant provisions under the Financial Services and Markets Act 2000, which are predicated on a unique statutory test.

19.88 The SFO was strongly of the view that new accessibility conditions should not be added to statutory regimes, particularly the Criminal Justice Act 1987 and POCA. They considered that standardisation would disrupt and complicate the self-contained regimes within these Acts. According to the SFO, standardisation would have implications beyond search warrant provisions. Further, the SFO considered that replacing carefully tailored, specialised and comprehensive schemes with a "one size fits all" approach may have undesirable and unforeseen consequences.

---

70 Metropolitan Police Service; Dijen Basu QC.

71 Dijen Basu QC.

72 Metropolitan Police Service.

73 Dijen Basu QC.

74 National Crime Agency.

75 Bar Council and the Criminal Bar Association.

76 Competition and Markets Authority; Financial Conduct Authority; Serious Fraud Office.

Analysis

19.89 We accept that the uniform set of accessibility conditions we suggested would not operate successfully in their current form. On reflection, we do not see sufficient value in standardising the statutory conditions.

19.90 We share the concerns of consultees that introducing a uniform set of accessibility conditions risks lessening protections for those under investigation or making it more difficult to investigate alleged criminality. In addition, consultees have not indicated to us that the way specific accessibility conditions are formulated creates substantial problems in practice.

Chapter 20: List of recommendations

Recommendation 1

20.1 We recommend that statutory safeguards, modelled on sections 15 and 16 of the Police and Criminal Evidence Act 1984, be inserted into the Criminal Justice Act 1987.

Paragraph 2.56

Recommendation 2

20.2 We recommend that the PACE Strategy Board consider amending Code B of the Police and Criminal Evidence Act 1984 to provide guidance for non-police investigators in complying with the provisions of the Code.

Paragraph 2.98

Recommendation 3

20.3 We recommend that section 15(1) of the Police and Criminal Evidence Act 1984 be amended to clarify that entry, search and seizure are unlawful unless *the warrant, entry and search* comply with sections 15 and 16 of the Police and Criminal Evidence Act 1984.

Paragraph 2.111

Recommendation 4

20.4 We recommend that section 15(1) of the Police and Criminal Evidence Act 1984 be amended to clarify that an entry on, search of, or *seizure* of materials from, any premises under a warrant is unlawful unless *the warrant, entry and search* comply with sections 15 and 16 of the Police and Criminal Evidence Act 1984.

Paragraph 2.121

Recommendation 5

20.5 We recommend that the NHS Counter Fraud Authority and the NHS Counter Fraud Service Wales be given powers to apply for a search warrant where there has been non-compliance with, or it is impracticable to issue, a production notice. Such powers should include searching for medical records and other related material which might constitute "excluded material" under the Police and Criminal Evidence Act 1984.

Paragraph 3.41

Recommendation 6

20.6 We recommend that the Insolvency Service be given the statutory power to apply for a search warrant under section 8 of the Police and Criminal Evidence Act 1984 and to apply for a "mixed warrant" relating to both ordinary material and special procedure material under schedule 1 to that Act.

Paragraph 3.46

Recommendation 7

20.7 We recommend that a search warrant applied for by the NHS Counter Fraud Authority or NHS Counter Fraud Service Wales permit either that agency or a constable to execute the warrant.

20.8 An NHS Counter Fraud Authority officer or NHS Counter Fraud Services Wales officer authorised to accompany a constable under a warrant should be able to exercise powers of search and seizure under the warrant irrespective of whether they are in the company, or under the supervision, of a constable, after the constable has effected entry.

Paragraphs 3.68 and 3.69

Recommendation 8

20.9 We recommend that the Insolvency Service be empowered to execute search warrants obtained under the Police and Criminal Evidence Act 1984 (Department of Trade and Industry Investigations) Order 2002, without the need to accompany a constable. This would extend to exercising the powers of entry as well as search.

20.10 We also recommend that sections 19 to 22 of the Police and Criminal Evidence Act 1984 be extended to the Insolvency Service, with necessary modifications.

Paragraphs 3.80 and 3.81

Recommendation 9

20.11 We recommend that the following powers be exercisable by members of the Serious Fraud Office and the Financial Conduct Authority (in addition to appropriate officers and authorised officers) irrespective of whether they are in the company, or under the supervision, of a constable:

(1) the power of search in section 2(5)(a) of the Criminal Justice Act 1987, and the additional powers in section 2(5)(b); and

(2) the powers in section 176(5)(b) to (d) of the Financial Services and Markets Act 2000.

20.12 We also recommend:

(1) that the duties in section 16(8) to (12) of the Police and Criminal Evidence Act 1984 apply to members of the Serious Fraud Office and the Financial Conduct Authority who are executing search warrants not in the presence of a constable;

(2) that consideration be given to how the safeguards in section 16(5) to (7) of the Police and Criminal Evidence Act 1984 should apply; and

(3) the creation of an offence of wilfully obstructing a person who is acting in the exercise of a power conferred by a warrant issued under section 2 of the Criminal Justice Act 1987.

Paragraphs 3.105 and 3.106

Recommendation 10

20.13 We recommend that the Criminal Procedure Rule Committee consider designing two entry warrant application forms:

(1) a specific entry warrant application form for applications under paragraph 32 of schedule 5 to the Consumer Rights Act 2015; and

(2) a generic entry warrant application form which can be modified for other entry warrant provisions.

Paragraph 4.34

Recommendation 11

20.14 We recommend that the Criminal Procedure Rule Committee consider amending search warrant application forms to include within the guidance notes an extensive (but non-exhaustive) list of factors which could be relevant to discharging the duty of candour. Some of the factors may also lend themselves to specific questions: where this is appropriate these should be included in the application form.

Paragraph 4.54

Recommendation 12

20.15 We recommend that the Criminal Procedure Rule Committee consider prescribing a standard entry warrant template.

Paragraph 4.134

Recommendation 13

20.16 We recommend that Her Majesty's Courts and Tribunals Service consider the practicability of designing and implementing an interactive online search warrants application portal.

Paragraph 4.154

Recommendation 14

20.17 We recommend that the duty of candour be codified in section 15 of the Police and Criminal Evidence Act 1984.

Paragraph 5.55

Recommendation 15

20.18 We recommend that the Criminal Procedure Rule Committee and the PACE Strategy Board consider amending the Criminal Practice Directions and Code B of the Police and Criminal Evidence Act 1984 to set out the duty of candour in greater detail. This should include consideration of the desirability of devising a non-exhaustive list of information which may be relevant to discharging the duty of candour.

Paragraph 5.69

Recommendation 16

20.19 We recommend that all law enforcement agencies take steps to ensure that sufficient training is provided to officers involved in applying for and executing search warrants to ensure that applications are consistently completed to a high standard.

Paragraph 5.126

Recommendation 17

20.20 We recommend that Her Majesty's Courts and Tribunals Service consider the practicability of making more search warrant application hearing slots available or pursuing other measures which would decrease both the length of time it takes to obtain a search warrant and the disruption to other court business.

Paragraph 5.133

Recommendation 18

20.21 We recommend that the PACE Strategy Board consider amending Code B of the Police and Criminal Evidence Act 1984 to include the requirement that a person applying for a search warrant has adequate knowledge to answer questions asked by the issuing authority.

Paragraph 5.149

Recommendation 19

20.22 We recommend that only those magistrates who have undergone specialist training should have the power to issue a search warrant.

Paragraph 6.48

Recommendation 20

20.23 We recommend that the requirement for a magistrate hearing a search warrant application to be advised by a legal adviser be formalised in the Criminal Procedure Rules.

Paragraph 6.62

Recommendation 21

20.24 We recommend that Her Majesty's Courts and Tribunals Service review the current magistrates' courts' out of hours search warrant application procedures across all regions to ensure that:

(1) proper use is being made of technology to increase the efficiency of out of hours applications; and

(2) there are sufficient resources to hear out of hours applications urgently and without undue delay.

Paragraph 6.99

Recommendation 22

20.25 We recommend that an application system for court hours applications be formalised nationwide to provide that:

(1) applications for a search warrant to a magistrates' court or the Crown Court should be submitted electronically, unless it is not practicable in the circumstances to do so; and

(2) unless it is not practicable in the circumstances to do so, applications to a magistrates' court should be screened by legal advisers, who would:

(a) return applications that obviously do not comply with statutory criteria or contain obvious errors; and

(b) list other cases for a hearing by video link, telephone, or in court, to be arranged with sufficient notice to read the documents in advance and sufficient time at the hearing for adequate scrutiny. There should be a presumption for remote hearings unless there are compelling reasons to hold a hearing in person.

Paragraph 6.141

Recommendation 23

20.26 We recommend that the Ministry of Justice examines the practicability of audio recording search warrants hearings in the magistrates' court and out of hours. Should such facilities be available, we consider that audio recordings should only be transcribed and made available to the occupier in the same way, and on the same conditions, as the information sworn in support of the warrant under the Criminal Procedure Rules.

Paragraph 6.176

Recommendation 24

20.27 We recommend that the following warrants data be collected and published by Her Majesty's Courts and Tribunals Service, with the assistance of law enforcement agencies where possible:

(1) the number of warrant applications received under each statutory power and by which agency (by court centre, including out of hours);

(2) the number of warrants granted and refused (by court centre, including out of hours); and

(3) the number of searches pursuant to a warrant in which material is successfully recovered.

Paragraph 6.204

Recommendation 25

20.28 We recommend that the following statutes be amended to make clear that an applicant need only specify the function or description of the person to accompany the officer executing the warrant rather than their name:

(1) the Police and Criminal Evidence Act 1984;

(2) the Criminal Justice Act 1987;

(3) the Competition Act 1998;

(4) the Financial Services and Markets Act 2000; and

(5) the Enterprise Act 2002.

Paragraph 7.40

Recommendation 26

20.29 We recommend that the following search warrant provisions be amended to provide for the authority to enter and search premises on more than one occasion (a "multiple entry warrant"):

(1) section 2 of the Criminal Justice Act 1987;

(2) section 352 of the Proceeds of Crime Act 2002; and

(3) section 176 of the Financial Services and Markets Act 2000.

20.30 The statutory condition for granting such a warrant should be that the issuing authority is satisfied that it is necessary to authorise multiple entries in order to achieve the purpose for which they issue the warrant.

20.31 We also recommend that comparable safeguards to those under the Police and Criminal Evidence Act 1984 should apply.

Paragraphs 7.74 to 7.76

Recommendation 27

20.32 We recommend that the following search warrant provisions be amended to enable a warrant to provide authority to enter and search any premises occupied or controlled by a person specified in the application, including such sets of premises as are so specified (an "all premises warrant"):

(1) section 2 of the Criminal Justice Act 1987;

(2) section 176 of the Financial Services and Markets Act 2000; and

(3) section 352 of the Proceeds of Crime Act 2002.

20.33 The statutory condition for granting such a warrant should be that the issuing authority is satisfied that:

(1) there are reasonable grounds for believing (or suspecting, if that is the test adopted in the regime) that it is necessary to search premises occupied or controlled by the person in question which are not specified in the application in order to find the documents, information or material specified; and

(2) it is not reasonably practicable to specify in the application all the premises which the person occupies or controls and which might need to be searched.

20.34 We also recommend that comparable safeguards to those under the Police and Criminal Evidence Act 1984 apply.

Paragraphs 7.105 to 7.107

Recommendation 28

20.35 We recommend that the Police and Criminal Evidence Act 1984 be amended to include a power to search any person found on premises searched pursuant to a warrant under section 8 of, or paragraph 12 of schedule 1 to, the Act. The power should be subject to stringent safeguards regarding when the power can be exercised and the manner in which it can be exercised.

Paragraph 7.126

Recommendation 29

20.36 We recommend that the Criminal Procedure Rule Committee consider amending application forms to invite the issuing authority to record their reasons for granting a warrant which may be executed outside usual hours.

Paragraph 7.153

Recommendation 30

20.37 We recommend that the PACE Strategy Board consider amending Code B of the Police and Criminal Evidence Act 1984 to provide guidance as to what constitutes a reasonable hour, including consideration of:

(1) the impact of carrying out a search at night in the presence or likely presence of children or other vulnerable people; and

(2) the different considerations to which regard should be had when searching commercial and dwelling premises.

Paragraph 7.155

Recommendation 31

20.38 We recommend that the PACE Strategy Board consider amending Code B of the Police and Criminal Evidence Act 1984 to take account of developments in case law, namely to clarify that:

(1) a copy of the full warrant must be supplied, including any schedule appended to it;

(2) a warrant is "produced" where the occupier is given a chance to inspect it;

(3) non-compliance with section 16(5)(a) and (b) of PACE may be justified where it appears to the officer, once lawful entry is effected, that the search may be frustrated; and

(4) it is permissible for all premises warrants to be redacted to omit the identity of other premises to be searched.

Paragraph 7.162

Recommendation 32

20.39 We recommend that:

(1) section 16(5) of the Police and Criminal Evidence Act 1984 be amended, and provisions under other statutes as is necessary, to require that the constable or other investigator produce a notice of powers and rights; and

(2) section 16(7) of the Police and Criminal Evidence Act 1984 be amended, and provisions under other statutes as is necessary, to provide that the constable or other investigator must also leave a copy of the notice of powers and rights in a prominent place on the premises.

Paragraph 7.179

Recommendation 33

20.40 We recommend the introduction of a specific search warrants "your rights and the law" webpage on the Government website. This should involve consultation with those with experience of the needs of individuals affected by a warrant.

Paragraph 7.183

Recommendation 34

20.41 We recommend that the PACE Strategy Board consider amending Code B of the Police and Criminal Evidence Act 1984 to state that a legal representative must be allowed to be present and observe a search under warrant in order to make their own notes. This should be subject to the following exception and requirement currently contained in Code B of the Police and Criminal Evidence Act 1984:

(1) a legal representative need not be allowed to be present and observe the search if the officer in charge of the search has reasonable grounds for believing the presence of the person asked for would unreasonably delay the search, seriously hinder the investigation or endanger officers or other people; and

(2) a record of the action taken should also be made on the premises search record, including the grounds for refusing the occupier's request for a legal representative.

Paragraph 7.217

Recommendation 35

20.42 We recommend that a judge hearing an application under section 59 of the Criminal Justice and Police Act 2001 have the power to order costs between parties.

Paragraph 8.94

Recommendation 36

20.43 We recommend that a judge hearing a judicial review of a search warrant have the powers and duties of the Crown Court in relation to the return or retention of material under section 59 of the Criminal Justice and Police Act 2001.

Paragraph 8.101

Recommendation 37

20.44 We recommend that the Criminal Procedure Rule Committee consider amending the Criminal Procedure Rules to include rules governing the storage of sensitive material provided to the court during a search warrant application.

Paragraph 9.44

Recommendation 38

20.45 We recommend that the Criminal Procedure Rule Committee consider the desirability of amending the requirement under rule 5.7(6) that an investigator has 14 days to issue a notice of objection after being served with a request for the supply of information.

Paragraph 9.72

Recommendation 39

20.46 We recommend that the Criminal Procedure Rule Committee consider amending the Criminal Practice Directions to set out matters that should be considered by the court when determining whether sensitive material ought to be withheld on the grounds of public interest immunity.

Paragraph 9.77

Recommendation 40

20.47 We recommend that the Government considers whether the law relating to iniquitous material in the context of criminal investigations ought to be reformed.

Paragraph 10.71

Recommendation 41

20.48 We recommend that the procedure for instructing independent counsel or other experts to resolve issues of legal privilege be dealt with in a new Code of Practice which we recommend at Recommendation 63 of this Report.

Paragraph 11.35

Recommendation 42

20.49 We recommend that the Government considers whether the law governing access to confidential personal records, human tissue and tissue fluid under the Police and Criminal Evidence Act 1984 strikes the right balance between (1) the prevention and investigation of serious crime; and (2) the protection of the confidentiality of health and counselling records, and whether the law ought to be reformed.

Paragraph 12.111

Recommendation 43

20.50 We recommend that the Government considers whether the law governing access to confidential journalistic material under the Police and Criminal Evidence Act 1984 strikes the right balance between (1) the prevention and investigation of serious crime; and (2) the freedom of the press and the protection of journalistic sources, and whether the law ought to be reformed.

Paragraph 12.173

Recommendation 44

20.51 We recommend that the PACE Strategy Board consider amending Code B of the Police and Criminal Evidence Act 1984 to provide guidance on when material constitutes special procedure material.

Paragraph 13.72

Recommendation 45

20.52 We recommend that search warrant provisions be amended to clarify that, when electronic data is sought, electronic devices can be the target of a search warrant so long as the data satisfies the statutory conditions relating to the target material.

Paragraph 15.34

Recommendation 46

20.53 We recommend that the Criminal Procedure Rule Committee consider amending search warrant application forms to require an investigator, when they are seeking to obtain a warrant to search for and seize electronic devices to acquire electronic data, to explain in as much detail as practicable what information on devices is sought.

Paragraph 15.62

Recommendation 47

20.54 We recommend that the Criminal Procedure Rule Committee consider amending search warrant application forms to require an investigator, when they are seeking to obtain a warrant to search for and seize electronic devices to acquire electronic data, to explain why they believe that the information is on the device and why the information would satisfy the statutory conditions.

Paragraph 15.66

Recommendation 48

20.55 We recommend that search warrants be required to contain two parts when electronic devices are sought for the purpose of obtaining information in the form of electronic data:

(1) the first part should specify the electronic device(s) to be searched for and seized; and

(2) the second part should specify the information on the electronic device(s) that is sought.

Paragraph 15.118

Recommendation 49

20.56 We recommend that search warrant provisions be amended, where necessary, to make clear that the power to seize an electronic device includes the power to copy all or some of the electronic data stored on an electronic device while on premises.

Paragraph 15.159

Recommendation 50

20.57 We recommend that search warrant provisions be amended to permit an investigator to apply for authority to conduct a search of electronic devices found during the course of a search where it is necessary to do so for the purpose for which the warrant is issued.

20.58 If granted, the search warrant should authorise the search for and copying of any electronic data stored on the device that corresponds to the information specified in the second part of the warrant.

Paragraphs 15.193 and 15.194

Recommendation 51

20.59 We recommend that the Government considers the desirability of amending the law to permit law enforcement agencies to obtain authorisation to search for and copy remotely stored data when executing a search warrant.

Paragraph 16.197

Recommendation 52

20.60 We recommend that the Government considers the desirability of amending the law governing the power to compel the production of passwords and other access information with the aim of making the law clearer and more effective. This should include consideration of an integrated power to form part of search warrant regimes.

Paragraph 16.222

Recommendation 53

20.61 We recommend that the Government considers the desirability of introducing a power to modify or alter remotely stored data exercisable pursuant to a search warrant for the purposes of preventing interference with or preserving the data.

Paragraph 16.238

Recommendation 54

20.62 We recommend the introduction of a new statutory regime governing the treatment of electronic material. The regime ought to apply whenever a relevant power of seizure or production is exercised in respect of electronic material following the execution of a search warrant.

Paragraph 17.74

Recommendation 55

20.63 We recommend that, under the new statutory regime in Recommendation 54 above, an investigator be required to provide as specific a description of what was seized as reasonably practicable to a person with an interest in the electronic material within a reasonable time from the making of the request for it.

Paragraph 17.85

Recommendation 56

20.64 We recommend that, under the new statutory regime in Recommendation 54 above, an investigator be required to provide details of what action was taken in respect of electronic devices on premises, in as much detail as practicable, to a person with an interest in the electronic device within a reasonable time from the making of the request for it.

Paragraph 17.95

Recommendation 57

20.65 We recommend that, under the new statutory regime in Recommendation 54 above, an investigator be required to provide protocols setting out how electronic material is to be examined to a person with an interest in the property within a reasonable time from the making of the request for it.

Paragraph 17.101

Recommendation 58

20.66 We recommend that, under the new statutory regime in Recommendation 54 above, an investigator be required to return electronic devices following seizure on premises as soon as reasonably practicable.

Paragraph 17.110

Recommendation 59

20.67 We recommend that, under the new statutory regime in Recommendation 54 above, an investigator be required to return and/or delete protected electronic material as soon as reasonably practicable.

Paragraph 17.117

Recommendation 60

20.68 We recommend that, under the new statutory regime in Recommendation 54 above, an investigator be required to return and/or delete non-responsive electronic material, so far as is reasonably practicable.

Paragraph 17.125

Recommendation 61

20.69 We recommend that, under the new statutory regime in Recommendation 54 above, a person with an interest in electronic material be able to apply to the Crown Court for a judge to approve of or adjudicate on disputes regarding the way in which the investigator intends to examine electronic material.

Paragraph 17.133

Recommendation 62

20.70 We recommend that, under the new statutory regime in Recommendation 54 above, a person with an interest in electronic material be able to apply to the Crown Court for the return or deletion of particular electronic data or return of an electronic device on the grounds that:

(1) the electronic material is reasonably required by the person with an interest in it; or

(2) continued retention by an investigator of the electronic material is not necessary.

Paragraph 17.139

Recommendation 63

20.71 We recommend the creation of a Code of Practice governing the acquisition and treatment of electronic material in criminal investigations involving search warrants.

Paragraph 17.153

Recommendation 64

20.72 We recommend a wider review of the operation of powers of search, production and seizure in respect of electronic material when investigating criminal offences not confined to cases where such powers are exercised pursuant to a search warrant or in respect of premises. In particular, such a review should consider:

(1) whether law enforcement have the necessary powers to investigate crime where remotely stored data is involved; and

(2) whether sufficient safeguards accompany such powers to ensure that they are used only where necessary and proportionate.

Paragraph 18.101

Appendix 1: List of consultees

1.1 This appendix lists those individuals and organisations who submitted a consultation response and whose views have informed the recommendations contained in this report.

(1) 5 members of the public.

(2) Metropolitan Police Service.

(3) Staffordshire Police.

(4) Another police force.[1]

(5) DS Clayton Ford, Essex Police.

(6) DS Parminder Kang, Leicestershire Police.

(7) City of London Police Economic Crime Academy.

(8) Norfolk and Suffolk joint Cyber, Intelligence and Serious Organised Crime Directorate.

(9) Independent Office for Police Conduct.

(10) Whitehall Prosecutors' Group.

(11) Crown Prosecution Service.

(12) National Crime Agency.

(13) HM Revenue & Customs.

(14) Serious Fraud Office.

(15) Financial Conduct Authority.

(16) Competition and Markets Authority.

(17) Insolvency Service.

(18) Association of Chief Trading Standards Officers.

(19) Kent County Council Trading Standards.

(20) NHS Counter Fraud Authority.

(21) Department for Work and Pensions.

(22) The Law Society of England and Wales.

[1] Anonymity requested owing to the police force's ongoing criminal investigation.

(23) Birmingham Law Society.

(24) The Bar Council and the Criminal Bar Association.

(25) Dijen Basu QC.

(26) Jonathan Hall QC.

(27) Magistrates Association.

(28) Justices' Clerks' Society.

(29) West London Magistrates' Bench (Ealing and Uxbridge Magistrates' Courts).

(30) Southern Derbyshire Magistrates' Bench.

(31) Robert Della-Sala JP.

(32) Nigel Shock JP.

(33) Kevin Giles JP.

(34) Judge Emma Arbuthnot, Senior District Judge (Chief Magistrate).

(35) HM Council of District Judges (Magistrates' Court).

(36) HM Council of Circuit Judges.

(37) Criminal Procedure Rule Committee.

(38) Siân Jones, Head of Legal and Professional Services at HMCTS.

(39) News Media Association.

(40) Guardian News and Media.

(41) Privacy International.

(42) Professor Richard Stone.

(43) Northumbria Centre for Evidence and Criminal Justice Studies.

Appendix 2: Extracts from relevant legislation

1.2 This appendix provides relevant extracts from the text of the following legislation:

(1) The Police and Criminal Evidence Act 1984; and

(2) The Criminal Justice and Police Act 2001.

POLICE AND CRIMINAL EVIDENCE ACT 1984

8.— Power of justice of the peace to authorise entry and search of premises.

(1) If on an application made by a constable a justice of the peace is satisfied that there are reasonable grounds for believing—

(a) that an indictable offence has been committed; and

(b) that there is material on premises mentioned in subsection (1A) below which is likely to be of substantial value (whether by itself or together with other material) to the investigation of the offence; and

(c) that the material is likely to be relevant evidence; and

(d) that it does not consist of or include items subject to legal privilege, excluded material or special procedure material; and

(e) that any of the conditions specified in subsection (3) below applies in relation to each set of premises specified in the application,

he may issue a warrant authorising a constable to enter and search the premises.

(1A) The premises referred to in subsection (1)(b) above are—

(a) one or more sets of premises specified in the application (in which case the application is for a "specific premises warrant"); or

(b) any premises occupied or controlled by a person specified in the application, including such sets of premises as are so specified (in which case the application is for an "all premises warrant").

(1B) If the application is for an all premises warrant, the justice of the peace must also be satisfied—

(a) that because of the particulars of the offence referred to in paragraph (a) of subsection (1) above, there are reasonable grounds for believing that it is necessary to search premises occupied or controlled by the person in question which are not specified in the application in order to find the material referred to in paragraph (b) of that subsection; and

(b) that it is not reasonably practicable to specify in the application all the premises which he occupies or controls and which might need to be searched.

(1C) The warrant may authorise entry to and search of premises on more than one occasion if, on the application, the justice of the peace is satisfied that it is necessary to authorise multiple entries in order to achieve the purpose for which he issues the warrant.

(1D) If it authorises multiple entries, the number of entries authorised may be unlimited, or limited to a maximum.

(2) A constable may seize and retain anything for which a search has been authorised under subsection (1) above.

(3) The conditions mentioned in subsection (1)(e) above are—

(a) that it is not practicable to communicate with any person entitled to grant entry to the premises;

(b) that it is practicable to communicate with a person entitled to grant entry to the premises but it is not practicable to communicate with any person entitled to grant access to the evidence;

(c) that entry to the premises will not be granted unless a warrant is produced;

(d) that the purpose of a search may be frustrated or seriously prejudiced unless a constable arriving at the premises can secure immediate entry to them.

(4) In this Act "relevant evidence", in relation to an offence, means anything that would be admissible in evidence at a trial for the offence.

(5) The power to issue a warrant conferred by this section is in addition to any such power otherwise conferred.

(6) This section applies in relation to a relevant offence as defined in section 28D(4) of the Immigration Act 1971 as it applies in relation to an indictable offence.

(7) Section 4 of the Summary Jurisdiction (Process) Act 1881 (execution of process of English courts in Scotland) shall apply to a warrant issued on the application of an officer of Revenue and Customs under this section by virtue of section 114 below.

9.— Special provisions as to access.

(1) A constable may obtain access to excluded material or special procedure material for the purposes of a criminal investigation by making an application under Schedule 1 below and in accordance with that Schedule.

(2) Any Act (including a local Act) passed before this Act under which a search of premises for the purposes of a criminal investigation could be authorised by the issue of a warrant to a constable shall cease to have effect so far as it relates to the authorisation of searches—

(a) for items subject to legal privilege; or

(b) for excluded material; or

(c) for special procedure material consisting of documents or records other than documents.

(2A) Section 4 of the Summary Jurisdiction (Process) Act 1881 (c. 24) (which includes provision for the execution of process of English courts in Scotland) and section 29 of the Petty Sessions (Ireland) Act 1851 (c. 93) (which makes equivalent provision for execution in Northern Ireland) shall each apply to any process issued by a judge under Schedule 1 to this Act as it applies to process issued by a magistrates' court under the Magistrates' Courts Act 1980 (c. 43).

10.— Meaning of 'items subject to legal privilege'.

(1) Subject to subsection (2) below, in this Act "items subject to legal privilege" means—

(a) communications between a professional legal adviser and his client or any person representing his client made in connection with the giving of legal advice to the client;

(b) communications between a professional legal adviser and his client or any person representing his client or between such an adviser or his client or any such representative and any other person made in connection with or in contemplation of legal proceedings and for the purposes of such proceedings; and

(c) items enclosed with or referred to in such communications and made—

(i) in connection with the giving of legal advice; or

(ii) in connection with or in contemplation of legal proceedings and for the purposes of such proceedings,

(iii) when they are in the possession of a person who is entitled to possession of them.

(2) Items held with the intention of furthering a criminal purpose are not items subject to legal privilege.

11.— Meaning of "excluded material".

(1) Subject to the following provisions of this section, in this Act "excluded material" means—

(a) personal records which a person has acquired or created in the course of any trade, business, profession or other occupation or for the purposes of any paid or unpaid office and which he holds in confidence;

(b) human tissue or tissue fluid which has been taken for the purposes of diagnosis or medical treatment and which a person holds in confidence;

(c) journalistic material which a person holds in confidence and which consists—

(i) of documents; or

(ii) of records other than documents.

(2) A person holds material other than journalistic material in confidence for the purposes of this section if he holds it subject—

(a) to an express or implied undertaking to hold it in confidence; or

(b) to a restriction on disclosure or an obligation of secrecy contained in any enactment, including an enactment contained in an Act passed after this Act.

(3) A person holds journalistic material in confidence for the purposes of this section if—

(a) he holds it subject to such an understanding, restriction or obligation; and

(b) it has been continuously held (by one or more persons) subject to such an undertaking, restriction or obligation since it was first acquired or created for the purposes of journalism.

12.— Meaning of "personal records".

In this Part of this Act "personal records" means documentary and other records concerning an individual (whether living or dead) who can be identified from them and relating—

(a) to his physical or mental health;

(b) to spiritual counselling or assistance given or to be given to him; or

(c) to counselling or assistance given or to be given to him, for the purposes of his personal welfare, by any voluntary organisation or by any individual who—

(i) by reason of his office or occupation has responsibilities for his personal welfare; or

(ii) by reason of an order of a court has responsibilities for his supervision.

13.— Meaning of "journalistic material".

(1) Subject to subsection (2) below, in this Act "journalistic material" means material acquired or created for the purposes of journalism.

(2) Material is only journalistic material for the purposes of this Act if it is in the possession of a person who acquired or created it for the purposes of journalism.

(3) A person who receives material from someone who intends that the recipient shall use it for the purposes of journalism is to be taken to have acquired it for those purposes.

14.— Meaning of "special procedure material".

(1) In this Act "special procedure material" means—

(a) material to which subsection (2) below applies; and

(b) journalistic material, other than excluded material.

(2) Subject to the following provisions of this section, this subsection applies to material, other than items subject to legal privilege and excluded material, in the possession of a person who—

(a) acquired or created it in the course of any trade, business, profession or other occupation or for the purpose of any paid or unpaid office; and

(b) holds it subject—

(i) to an express or implied undertaking to hold it in confidence; or

(ii) to a restriction or obligation such as is mentioned in section 11(2)(b) above.

(3) Where material is acquired—

(a) by an employee from his employer and in the course of his employment; or

(b) by a company from an associated company,

it is only special procedure material if it was special procedure material immediately before the acquisition.

(4) Where material is created by an employee in the course of his employment, it is only special procedure material if it would have been special procedure material had his employer created it.

(5) Where material is created by a company on behalf of an associated company, it is only special procedure material if it would have been special procedure material had the associated company created it.

(6) A company is to be treated as another's associated company for the purposes of this section if it would be so treated under section 449 of the Corporation Tax Act 2010.

15.— Search warrants–safeguards.

(1) This section and section 16 below have effect in relation to the issue to constables under any enactment, including an enactment contained in an Act passed after this Act, of warrants to enter and search premises; and an entry on or search of premises under a warrant is unlawful unless it complies with this section and section 16 below.

(2) Where a constable applies for any such warrant, it shall be his duty—

(a) to state—

(i) the ground on which he makes the application;

(ii) the enactment under which the warrant would be issued; and

(iii) if the application is for a warrant authorising entry and search on more than one occasion, the ground on which he applies for such a warrant, and whether he seeks a warrant authorising an unlimited number of entries, or (if not) the maximum number of entries desired;

(b) to specify the matters set out in subsection (2A) below; and

(c) to identify, so far as is practicable, the articles or persons to be sought.

(2A) The matters which must be specified pursuant to subsection (2)(b) above are—

(a) if the application relates to one or more sets of premises specified in the application, each set of premises which it is desired to enter and search;

(b) if the application relates to any premises occupied or controlled by a person specified in the application–

(i) as many sets of premises which it is desired to enter and search as it is reasonably practicable to specify;

(ii) the person who is in occupation or control of those premises and any others which it is desired to enter and search;

(iii) why it is necessary to search more premises than those specified under sub-paragraph (i); and

(iv) why it is not reasonably practicable to specify all the premises which it is desired to enter and search.

(3) An application for such a warrant shall be made ex parte and supported by an information in writing.

(4) The constable shall answer on oath any question that the justice of the peace or judge hearing the application asks him.

(5) A warrant shall authorise an entry on one occasion only unless it specifies that it authorises multiple entries.

(5A) If it specifies that it authorises multiple entries, it must also specify whether the number of entries authorised is unlimited, or limited to a specified maximum.

(6) A warrant —

(a) shall specify —

(i) the name of the person who applies for it;

(ii) the date on which it is issued;

(iii) the enactment under which it is issued; and

(iv) each set of premises to be searched, or (in the case of an all premises warrant) the person who is in occupation or control of premises to be searched, together with any premises under his occupation or control which can be specified and which are to be searched; and

(b) shall identify, so far as is practicable, the articles or persons to be sought.

(7) Two copies shall be made of a warrant which specifies only one set of premises and does not authorise multiple entries; and as many copies as are reasonably required may be made of any other kind of warrant.

(8) The copies shall be clearly certified as copies.

16.— Execution of warrants.

(1) A warrant to enter and search premises may be executed by any constable.

(2) Such a warrant may authorise persons to accompany any constable who is executing it.

(2A) A person so authorised has the same powers as the constable whom he accompanies in respect of—

(a) the execution of the warrant, and

(b) the seizure of anything to which the warrant relates.

(2B) But he may exercise those powers only in the company, and under the supervision, of a constable.

(3) Entry and search under a warrant must be within three months from the date of its issue.

(3A) If the warrant is an all premises warrant, no premises which are not specified in it may be entered or searched unless a police officer of at least the rank of inspector has in writing authorised them to be entered.

(3B) No premises may be entered or searched for the second or any subsequent time under a warrant which authorises multiple entries unless a police officer of at least the rank of inspector has in writing authorised that entry to those premises.

(4) Entry and search under a warrant must be at a reasonable hour unless it appears to the constable executing it that the purpose of a search may be frustrated on an entry at a reasonable hour.

(5) Where the occupier of premises which are to be entered and searched is present at the time when a constable seeks to execute a warrant to enter and search them, the constable—

(a) shall identify himself to the occupier and, if not in uniform, shall produce to him documentary evidence that he is a constable;

(b) shall produce the warrant to him; and

(c) shall supply him with a copy of it.

(6) Where—

(a) the occupier of such premises is not present at the time when a constable seeks to execute such a warrant; but

(b) some other person who appears to the constable to be in charge of the premises is present,

subsection (5) above shall have effect as if any reference to the occupier were a reference to that other person.

(7) If there is no person who appears to the constable to be in charge of the premises, he shall leave a copy of the warrant in a prominent place on the premises.

(8) A search under a warrant may only be a search to the extent required for the purpose for which the warrant was issued.

(9) A constable executing a warrant shall make an endorsement on it stating—

(a) whether the articles or persons sought were found; and

(b) whether any articles were seized, other than articles which were sought

and, unless the warrant is a warrant specifying one set of premises only, he shall do so separately in respect of each set of premises entered and searched, which he shall in each case state in the endorsement.

(10) A warrant shall be returned to the appropriate person mentioned in subsection (10A) below—

(a) when it has been executed; or

(b) in the case of a specific premises warrant which has not been executed, or an all premises warrant, or any warrant authorising multiple entries, upon the expiry of the period of three months referred to in subsection (3) above or sooner.

(10A) The appropriate person is—

(a) if the warrant was issued by a justice of the peace, the designated officer for the local justice area in which the justice was acting when he issued the warrant;

(b) if it was issued by a judge, the appropriate officer of the court from which he issued it.

(11) A warrant which is returned under subsection (10) above shall be retained for 12 months from its return—

(a) by the designated officer for the local justice area, if it was returned under paragraph (i) of that subsection; and

(b) by the appropriate officer, if it was returned under paragraph (ii).

(12) If during the period for which a warrant is to be retained the occupier of premises to which it relates asks to inspect it, he shall be allowed to do so.

17.— Entry for purpose of arrest etc.

(1) Subject to the following provisions of this section, and without prejudice to any other enactment, a constable may enter and search any premises for the purpose—

(a) of executing—

(i) a warrant of arrest issued in connection with or arising out of criminal proceedings; or

(ii) a warrant of commitment issued under section 76 of the Magistrates' Courts Act 1980;

(b) of arresting a person for an indictable offence;

(c) of arresting a person for an offence under—

(i) section 1 (prohibition of uniforms in connection with political objects), of the Public Order Act 1936;

(ii) any enactment contained in sections 6 to 8 or 10 of the Criminal Law Act 1977 (offences relating to entering and remaining on property);

(iii) section 4 of the Public Order Act 1986 (fear or provocation of violence);

(iiia) section 4 (driving etc. when under influence of drink or drugs) or 163 (failure to stop when required to do so by constable in uniform) of the Road Traffic Act 1988;

(iiib) section 27 of the Transport and Works Act 1992 (which relates to offences involving drink or drugs);

(iv) section 76 of the Criminal Justice and Public Order Act 1994 (failure to comply with interim possession order);

(v) any of sections 4, 5, 6(1) and (2), 7 and 8(1) and (2) of the Animal Welfare Act 2006 (offences relating to the prevention of harm to animals);

(vi) section 144 of the Legal Aid, Sentencing and Punishment of Offenders Act 2012 (squatting in a residential building);

(ca) of arresting, in pursuance of section 32(1A) of the Children and Young Persons Act 1969, any child or young person who has been remanded to local authority accommodation or youth detention accommodation under section 91 of the Legal Aid, Sentencing and Punishment of Offenders Act 2012;

(caa) of arresting a person for an offence to which section 61 of the Animal Health Act 1981 applies;

(cab) of arresting a person under any of the following provisions—

(i) section 30D(1) or (2A);

(ii) section 46A(1) or (1A);

(iii) section 5B(7) of the Bail Act 1976 (arrest where a person fails to surrender to custody in accordance with a court order);

(iv) section 7(3) of the Bail Act 1976 (arrest where a person is not likely to surrender to custody etc);

(v) section 97(1) of the Legal Aid, Sentencing and Punishment of Offenders Act 2012 (arrest where a child is suspected of breaking conditions of remand);

(cb) of recapturing any person who is, or is deemed for any purpose to be, unlawfully at large while liable to be detained—

(i) in a prison, young offender institution, secure training centre or secure college , or

(ii) in pursuance of section 92 of the Powers of Criminal Courts (Sentencing) Act 2000 (dealing with children and young persons guilty of grave crimes), in any other place;

(d) of recapturing any person whatever who is unlawfully at large and whom he is pursuing; or

(e) of saving life or limb or preventing serious damage to property.

(2) Except for the purpose specified in paragraph (e) of subsection (1) above, the powers of entry and search conferred by this section—

(a) are only exercisable if the constable has reasonable grounds for believing that the person whom he is seeking is on the premises; and

(b) are limited, in relation to premises consisting of two or more separate dwellings, to powers to enter and search—

(i) any parts of the premises which the occupiers of any dwelling comprised in the premises use in common with the occupiers of any other such dwelling; and

(ii) any such dwelling in which the constable has reasonable grounds for believing that the person whom he is seeking may be.

(3) The powers of entry and search conferred by this section are only exercisable for the purposes specified in subsection (1)(c)(ii), (iv) or (vi) above by a constable in uniform.

(4) The power of search conferred by this section is only a power to search to the extent that is reasonably required for the purpose for which the power of entry is exercised.

(5) Subject to subsection 6 below, all the rules of common law under which a constable has power to enter premises without a warrant are hereby abolished.

(6) Nothing in subsection (5) above affects any power of entry to deal with or prevent a breach of the peace.

18.— Entry and search after arrest.

(1) Subject to the following provisions of this section, a constable may enter and search any premises occupied or controlled by a person who is under arrest for an indictable offence, if he has reasonable grounds for suspecting that there is on the premises evidence, other than items subject to legal privilege, that relates—

(a) to that offence; or

(b) to some other indictable offence which is connected with or similar to that offence.

(2) A constable may seize and retain anything for which he may search under subsection (1) above.

(3) The power to search conferred by subsection (1) above is only a power to search to the extent that is reasonably required for the purpose of discovering such evidence.

(4) Subject to subsection (5) below, the powers conferred by this section may not be exercised unless an officer of the rank of inspector or above has authorised them in writing.

(5) A constable may conduct a search under subsection (1)—

(a) before the person is taken to a police station or released under section 30A, and

(b) without obtaining an authorisation under subsection (4),

if the condition in subsection (5A) is satisfied.

(5A) The condition is that the presence of the person at a place (other than a police station) is necessary for the effective investigation of the offence.

(6) If a constable conducts a search by virtue of subsection (5) above, he shall inform an officer of the rank of inspector or above that he has made the search as soon as practicable after he has made it.

(7) An officer who—

(a) authorises a search; or

(b) is informed of a search under subsection (6) above, shall make a record in writing—

(i) of the grounds for the search; and

(ii) of the nature of the evidence that was sought.

(8) If the person who was in occupation or control of the premises at the time of the search is in police detention at the time the record is to be made, the officer shall make the record as part of his custody record.

19.— General power of seizure etc.

(1) The powers conferred by subsections (2), (3) and (4) below are exercisable by a constable who is lawfully on any premises.

(2) The constable may seize anything which is on the premises if he has reasonable grounds for believing—

(a) that it has been obtained in consequence of the commission of an offence; and

(b) that it is necessary to seize it in order to prevent it being concealed, lost, damaged, altered or destroyed.

(3) The constable may seize anything which is on the premises if he has reasonable grounds for believing—

(a) that it is evidence in relation to an offence which he is investigating or any other offence; and

(b) that it is necessary to seize it in order to prevent the evidence being concealed, lost, altered or destroyed.

(4) The constable may require any information which is stored in any electronic form and is accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible or from which it can readily be produced in a visible and legible form if he has reasonable grounds for believing—

(a) that—

(i) it is evidence in relation to an offence which he is investigating or any other offence; or

(ii) it has been obtained in consequence of the commission of an offence; and

(b) that it is necessary to do so in order to prevent it being concealed, lost, tampered with or destroyed.

(5) The powers conferred by this section are in addition to any power otherwise conferred.

(6) No power of seizure conferred on a constable under any enactment (including an enactment contained in an Act passed after this Act) is to be taken to authorise the seizure of an item which the constable exercising the power has reasonable grounds for believing to be subject to legal privilege.

20.— Extension of powers of seizure to computerised information.

(1) Every power of seizure which is conferred by an enactment to which this section applies on a constable who has entered premises in the exercise of a power conferred by an enactment shall be construed as including a power to require any information stored in any electronic form contained in a computer and accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible or from which it can readily be produced in a visible and legible form.

(2) This section applies—

(a) to any enactment contained in an Act passed before this Act;

(b) to sections 8 and 18 above;

(c) to paragraph 13 of Schedule 1 to this Act; and

(d) to any enactment contained in an Act passed after this Act.

21. — Access and copying.

(1) A constable who seizes anything in the exercise of a power conferred by any enactment, including an enactment contained in an Act passed after this Act, shall, if so requested by a person showing himself—

(a) to be the occupier of premises on which it was seized; or

(b) to have had custody or control of it immediately before the seizure,

provide that person with a record of what he seized.

(2) The officer shall provide the record within a reasonable time from the making of the request for it.

(3) Subject to subsection (8) below, if a request for permission to be granted access to anything which—

(a) has been seized by a constable; and

(b) is retained by the police for the purpose of investigating an offence,

is made to the officer in charge of the investigation by a person who had custody or control of the thing immediately before it was so seized or by someone acting on behalf of such a person, the officer shall allow the person who made the request access to it under the supervision of a constable.

(4) Subject to subsection (8) below, if a request for a photograph or copy of any such thing is made to the officer in charge of the investigation by a person who had custody or control of the thing immediately before it was so seized, or by someone acting on behalf of such a person, the officer shall—

(a) allow the person who made the request access to it under the supervision of a constable for the purpose of photographing or copying it; or

(b) photograph or copy it, or cause it to be photographed or copied.

(5) A constable may also photograph or copy, or have photographed or copied, anything which he has power to seize, without a request being made under subsection (4) above.

(6) Where anything is photographed or copied under subsection (4)(b) above, the photograph or copy shall be supplied to the person who made the request.

(7) The photograph or copy shall be so supplied within a reasonable time from the making of the request.

(8) There is no duty under this section to grant access to, or to supply a photograph or copy of, anything if the officer in charge of the investigation for the purposes of which it was seized has reasonable grounds for believing that to do so would prejudice—

(a) that investigation;

(b) the investigation of an offence other than the offence for the purposes of investigating which the thing was seized; or

(c) any criminal proceedings which may be brought as a result of—

(i) the investigation of which he is in charge; or

(ii) any such investigation as is mentioned in paragraph (b) above.

(9) The references to a constable in subsections (1), (2), (3)(a) and (5) include a person authorised under section 16(2) to accompany a constable executing a warrant.

(10) The references to a constable in subsections (1) and (2) do not include a constable who has seized a thing under paragraph 19ZE of Schedule 3 to the Police Reform Act 2002.

22.— Retention.

(1) Subject to subsection (4) below, anything which has been seized by a constable or taken away by a constable following a requirement made by virtue of section 19 or 20 above may be retained so long as is necessary in all the circumstances.

(2) Without prejudice to the generality of subsection (1) above—

(a) anything seized for the purposes of a criminal investigation may be retained, except as provided by subsection (4) below—

(i) for use as evidence at a trial for an offence; or

(ii) for forensic examination or for investigation in connection with an offence; and

(b) anything may be retained in order to establish its lawful owner, where there are reasonable grounds for believing that it has been obtained in consequence of the commission of an offence.

(3) Nothing seized on the ground that it may be used—

(a) to cause physical injury to any person;

(b) to damage property;

(c) to interfere with evidence; or

(d) to assist in escape from police detention or lawful custody,

may be retained when the person from whom it was seized is no longer in police detention or the custody of a court or is in the custody of a court but has been released on bail.

(4) Nothing may be retained for either of the purposes mentioned in subsection (2)(a) above if a photograph or copy would be sufficient for that purpose.

(5) Nothing in this section affects any power of a court to make an order under section 1 of the Police (Property) Act 1897.

(6) This section also applies to anything retained by the police under section 28H(5) of the Immigration Act 1971.

(7) The reference in subsection (1) to anything seized by a constable includes anything seized by a person authorised under section 16(2) to accompany a constable executing a warrant.

23. — Meaning of "premises" etc.

In this Act—

"premises" includes any place and, in particular, includes—

(a) any vehicle, vessel, aircraft or hovercraft;

(b) any offshore installation;

(ba) any renewable energy installation;

(c) any tent or movable structure;

"offshore installation" has the meaning given to it by section 1 of the Mineral Workings (Offshore Installations) Act 1971.

"renewable energy installation" has the same meaning as in Chapter 2 of Part 2 of the Energy Act 2004.

24.— Arrest without warrant: constables

(1) A constable may arrest without a warrant—

(a) anyone who is about to commit an offence;

(b) anyone who is in the act of committing an offence;

(c) anyone whom he has reasonable grounds for suspecting to be about to commit an offence;

(d) anyone whom he has reasonable grounds for suspecting to be committing an offence.

(2) If a constable has reasonable grounds for suspecting that an offence has been committed, he may arrest without a warrant anyone whom he has reasonable grounds to suspect of being guilty of it.

(3) If an offence has been committed, a constable may arrest without a warrant—

(a) anyone who is guilty of the offence;

(b) anyone whom he has reasonable grounds for suspecting to be guilty of it.

(4) But the power of summary arrest conferred by subsection (1), (2) or (3) is exercisable only if the constable has reasonable grounds for believing that for any of the reasons mentioned in subsection (5) it is necessary to arrest the person in question.

(5) The reasons are—

(a) to enable the name of the person in question to be ascertained (in the case where the constable does not know, and cannot readily ascertain, the person's name, or has reasonable grounds for doubting whether a name given by the person as his name is his real name);

(b) correspondingly as regards the person's address;

(c) to prevent the person in question—

(i) causing physical injury to himself or any other person;

(ii) suffering physical injury;

(iii) causing loss of or damage to property;

(iv) committing an offence against public decency (subject to subsection (6)); or

(v) causing an unlawful obstruction of the highway;

(d) to protect a child or other vulnerable person from the person in question;

(e) to allow the prompt and effective investigation of the offence or of the conduct of the person in question;

(f) to prevent any prosecution for the offence from being hindered by the disappearance of the person in question.

(6) Subsection (5)(c)(iv) applies only where members of the public going about their normal business cannot reasonably be expected to avoid the person in question.

32. — Search upon arrest.

(1) A constable may search an arrested person, in any case where the person to be searched has been arrested at a place other than a police station, if the constable has reasonable grounds for believing that the arrested person may present a danger to himself or others.

(2) Subject to subsections (3) to (5) below, a constable shall also have power in any such case—

(a) to search the arrested person for anything—

(i) which he might use to assist him to escape from lawful custody; or

(ii) which might be evidence relating to an offence; and

(b) if the offence for which he has been arrested is an indictable offence, to enter and search any premises in which he was when arrested or immediately before he was arrested for evidence relating to the offence.

(3) The power to search conferred by subsection (2) above is only a power to search to the extent that is reasonably required for the purpose of discovering any such thing or any such evidence.

(4) The powers conferred by this section to search a person are not to be construed as authorising a constable to require a person to remove any of his clothing in public other than an outer coat, jacket or gloves but they do authorise a search of a person's mouth.

(5) A constable may not search a person in the exercise of the power conferred by subsection (2)(a) above unless he has reasonable grounds for believing that the person to be searched may have concealed on him anything for which a search is permitted under that paragraph.

(6) A constable may not search premises in the exercise of the power conferred by subsection (2)(b) above unless he has reasonable grounds for believing that there is evidence for which a search is permitted under that paragraph on the premises.

(7) In so far as the power of search conferred by subsection (2)(b) above relates to premises consisting of two or more separate dwellings, it is limited to a power to search—

(a) any dwelling in which the arrest took place or in which the person arrested was immediately before his arrest; and

(b) any parts of the premises which the occupier of any such dwelling uses in common with the occupiers of any other dwellings comprised in the premises.

(8) A constable searching a person in the exercise of the power conferred by subsection (1) above may seize and retain anything he finds, if he has reasonable grounds for believing that the person searched might use it to cause physical injury to himself or to any other person.

(9) A constable searching a person in the exercise of the power conferred by subsection (2)(a) above may seize and retain anything he finds, other than an item subject to legal privilege, if he has reasonable grounds for believing—

(a) that he might use it to assist him to escape from lawful custody; or

(b) that it is evidence of an offence or has been obtained in consequence of the commission of an offence.

(10) Nothing in this section shall be taken to affect the power conferred by section 43 of the Terrorism Act 2000.

Schedule 1 to the Police and Criminal Evidence Act 1984.

1.

If on an application made by a constable a judge[1] is satisfied that one or other of the sets of access conditions is fulfilled, he may make an order under paragraph 4 below.

2.

The first set of access conditions is fulfilled if—

(a) there are reasonable grounds for believing—

(i) that an indictable offence has been committed;

(ii) that there is material which consists of special procedure material or includes special procedure material and does not also include excluded material on premises specified in the application, or on premises occupied or controlled by a person specified in the application (including all such premises on which there are reasonable grounds for believing that there is such material as it is reasonably practicable so to specify);

(iii) that the material is likely to be of substantial value (whether by itself or together with other material) to the investigation in connection with which the application is made; and

(iv) that the material is likely to be relevant evidence;

(b) other methods of obtaining the material—

(i) have been tried without success; or

(ii) have not been tried because it appeared that they were bound to fail; and

(c) it is in the public interest, having regard—

(i) to the benefit likely to accrue to the investigation if the material is obtained; and

(ii) to the circumstances under which the person in possession of the material holds it,

that the material should be produced or that access to it should be given.

---

[1] It is unclear whether District Judges (Magistrates' Courts) also have jurisdiction, along with Circuit judges, to hear applications for production orders and search warrants under the Police and Criminal Evidence Act 1984, sch 1. For a discussion of this issue see Alex Davidson, "Production Orders: R (BBC) v Newcastle Crown Court (Case Comment)" [2020] *Criminal Law Review* 247, 250.

3.

The second set of access conditions is fulfilled if—

(a) there are reasonable grounds for believing that there is material which consists of or includes excluded material or special procedure material on premises specified in the application or on premises occupied or controlled by a person specified in the application (including all such premises on which there are reasonable grounds for believing that there is such material as it is reasonably practicable so to specify);

(b) but for section 9(2) above a search of such premises for that material could have been authorised by the issue of a warrant to a constable under an enactment other than this Schedule; and

(c) the issue of such a warrant would have been appropriate.

4.

An order under this paragraph is an order that the person who appears to the judge to be in possession of the material to which the application relates shall—

(a) produce it to a constable for him to take away; or

(b) give a constable access to it,

not later than the end of the period of seven days from the date of the order or the end of such longer period as the order may specify.

5.

Where the material consists of information stored in any electronic form—

(a) an order under paragraph 4(a) above shall have effect as an order to produce the material in a form in which it can be taken away and in which it is visible and legible or from which it can readily be produced in a visible and legible form; and

(b) an order under paragraph 4(b) above shall have effect as an order to give a constable access to the material in a form in which it is visible and legible.

6.

For the purposes of sections 21 and 22 above material produced in pursuance of an order under paragraph 4(a) above shall be treated as if it were material seized by a constable.

7.

An application for an order under paragraph 4 above that relates to material that consists of or includes journalistic material shall be made inter partes.

8.

Notice of an application for an order under paragraph 4 above that relates to material that consists of or includes journalistic material may be served on a person either by delivering it to him or by leaving it at his proper address or by sending it by post to him in a registered letter or by the recorded delivery service.

9.

Notice of an application for an order under paragraph 4 above that relates to material that consists of or includes journalistic material may be served—

(a) on a body corporate, by serving it on the body's secretary or clerk or other similar officer; and

(b) on a partnership, by serving in on one of the partners.

10.

For the purposes of paragraph 8, and of section 7 of the Interpretation Act 1978 in its application to paragraph 8 , the proper address of a person, in the case of secretary or clerk or other similar officer of a body corporate, shall be that of the registered or principal office of that body, in the case of a partner of a firm shall be that of the principal office of the firm, and in any other case shall be the last known address of the person to be served.

11.

Where notice of an application for an order under paragraph 4 above has been served on a person, he shall not conceal, destroy, alter or dispose of the material to which the application relates except—

(a) with the leave of a judge; or

(b) with the written permission of a constable,

until—

(i) the application is dismissed or abandoned; or

(ii) he has complied with an order under paragraph 4 above made on the application.

12.

If on an application made by a constable a judge—

(a) is satisfied—

(i) that either set of access conditions is fulfilled; and

(ii) that any of the further conditions set out in paragraph 14 below is also fulfilled in relation to each set of premises specified in the application; or

(b) is satisfied—

(i) that the second set of access conditions is fulfilled; and

(ii) that an order under paragraph 4 above relating to the material has not been complied with,

he may issue a warrant authorising a constable to enter and search the premises or (as the case may be) all premises occupied or controlled by the person referred to in paragraph 2(a)(ii) or 3(a), including such sets of premises as are specified in the application (an "all premises warrant") .

12A.

The judge may not issue an all premises warrant unless he is satisfied—

(a) that there are reasonable grounds for believing that it is necessary to search premises occupied or controlled by the person in question which are not specified in the application, as well as those which are, in order to find the material in question; and

(b) that it is not reasonably practicable to specify all the premises which he occupies or controls which might need to be searched.

13.

A constable may seize and retain anything for which a search has been authorised under paragraph 12 above.

14.

The further conditions mentioned in paragraph 12 (a)(ii) above are—

(a) that it is not practicable to communicate with any person entitled to grant entry to the premises;

(b) that it is practicable to communicate with a person entitled to grant entry to the premises but it is not practicable to communicate with any person entitled to grant access to the material;

(c) that the material contains information which—

(i) is subject to a restriction or obligation such as is mentioned in section 11(2)(b) above; and

(ii) is likely to be disclosed in breach of it if a warrant is not issued;

(d) that service of notice of an application for an order under paragraph 4 above may seriously prejudice the investigation.

15.

(1) If a person fails to comply with an order under paragraph 4 above, a judge may deal with him as if he had committed a contempt of the Crown Court.

(2) Any enactment relating to contempt of the Crown Court shall have effect in relation to such a failure as if it were such a contempt.

15A.

Criminal Procedure Rules may make provision about proceedings under this Schedule, other than proceedings for an order under paragraph 4 above that relates to material that consists of or includes journalistic material.

16.

The costs of any application under this Schedule and of anything done or to be done in pursuance of an order made under it shall be in the discretion of the judge.

17.

In this Schedule “judge” means a Circuit judge a qualifying judge advocate (within the meaning of the Senior Courts Act 1981) or a District Judge (Magistrates' Courts).[2]

CRIMINAL JUSTICE AND POLICE ACT 2001

50.— Additional powers of seizure from premises

(1) Where —

(a) a person who is lawfully on any premises finds anything on those premises that he has reasonable grounds for believing may be or may contain something for which he is authorised to search on those premises,

(b) a power of seizure to which this section applies or the power conferred by subsection (2) would entitle him, if he found it, to seize whatever it is that he has grounds for believing that thing to be or to contain, and

(c) in all the circumstances, it is not reasonably practicable for it to be determined, on those premises—

(i) whether what he has found is something that he is entitled to seize, or

(ii) the extent to which what he has found contains something that he is entitled to seize,

that person’s powers of seizure shall include power under this section to seize so much of what he has found as it is necessary to remove from the premises to enable that to be determined.

(2) Where—

(a) a person who is lawfully on any premises finds anything on those premises (“the seizable property”) which he would be entitled to seize but for its being comprised in something else that he has (apart from this subsection) no power to seize,

(b) the power under which that person would have power to seize the seizable property is a power to which this section applies, and

(c) in all the circumstances it is not reasonably practicable for the seizable property to be separated, on those premises, from that in which it is comprised,

that person’s powers of seizure shall include power under this section to seize both the seizable property and that from which it is not reasonably practicable to separate it.

---

[2] It is unclear whether District Judges (Magistrates’ Courts) also have jurisdiction, along with Circuit judges, to hear applications for production orders and search warrants under the Police and Criminal Evidence Act 1984, sch 1. For a discussion of this issue see Alex Davidson, “Production Orders: R (BBC) v Newcastle Crown Court (Case Comment)” [2020] *Criminal Law Review* 247, 250.

(3) The factors to be taken into account in considering, for the purposes of this section, whether or not it is reasonably practicable on particular premises for something to be determined, or for something to be separated from something else, shall be confined to the following—

(a) how long it would take to carry out the determination or separation on those premises;

(b) the number of persons that would be required to carry out that determination or separation on those premises within a reasonable period;

(c) whether the determination or separation would (or would if carried out on those premises) involve damage to property;

(d) the apparatus or equipment that it would be necessary or appropriate to use for the carrying out of the determination or separation; and

(e) in the case of separation, whether the separation—

(i) would be likely, or

(ii) if carried out by the only means that are reasonably practicable on those premises, would be likely,

to prejudice the use of some or all of the separated seizable property for a purpose for which something seized under the power in question is capable of being used.

(4) Section 19(6) of the 1984 Act and Article 21(6) of the Police and Criminal Evidence (Northern Ireland) Order 1989 (S.I. 1989 1341 (N.I. 12)) (powers of seizure not to include power to seize anything that a person has reasonable grounds for believing is legally privileged) shall not apply to the power of seizure conferred by subsection (2).

(5) This section applies to each of the powers of seizure specified in Part 1 of Schedule 1.

(6) Without prejudice to any power conferred by this section to take a copy of any document, nothing in this section, so far as it has effect by reference to the power to take copies of documents under section 28(2)(b) of the Competition Act 1998 (c. 41), shall be taken to confer any power to seize any document.

51.— Additional powers of seizure from the person.

(1) Where —

(a) a person carrying out a lawful search of any person finds something that he has reasonable grounds for believing may be or may contain something for which he is authorised to search,

(b) a power of seizure to which this section applies or the power conferred by subsection (2) would entitle him, if he found it, to seize whatever it is that he has grounds for believing that thing to be or to contain, and

(c) in all the circumstances it is not reasonably practicable for it to be determined, at the time and place of the search—

(i) whether what he has found is something that he is entitled to seize, or

(ii) the extent to which what he has found contains something that he is entitled to seize,

that person's powers of seizure shall include power under this section to seize so much of what he has found as it is necessary to remove from that place to enable that to be determined.

(2) Where—

(a) a person carrying out a lawful search of any person finds something ("the seizable property") which he would be entitled to seize but for its being comprised in something else that he has (apart from this subsection) no power to seize,

(b) the power under which that person would have power to seize the seizable property is a power to which this section applies, and

(c) in all the circumstances it is not reasonably practicable for the seizable property to be separated, at the time and place of the search, from that in which it is comprised,

that person's powers of seizure shall include power under this section to seize both the seizable property and that from which it is not reasonably practicable to separate it.

(3) The factors to be taken into account in considering, for the purposes of this section, whether or not it is reasonably practicable, at the time and place of a search, for something to be determined, or for something to be separated from something else, shall be confined to the following—

(a) how long it would take to carry out the determination or separation at that time and place;

(b) the number of persons that would be required to carry out that determination or separation at that time and place within a reasonable period;

(c) whether the determination or separation would (or would if carried out at that time and place) involve damage to property;

(d) the apparatus or equipment that it would be necessary or appropriate to use for the carrying out of the determination or separation; and

(e) in the case of separation, whether the separation—

(i) would be likely, or

(ii) if carried out by the only means that are reasonably practicable at that time and place, would be likely,

to prejudice the use of some or all of the separated seizable property for a purpose for which something seized under the power in question is capable of being used.

(4) Section 19(6) of the 1984 Act and Article 21(6) of the Police and Criminal Evidence (Northern Ireland) Order 1989 (S.I. 1989 1341 (N.I. 12)) (powers of seizure not to include power to seize anything a person has reasonable grounds for believing is legally privileged) shall not apply to the power of seizure conferred by subsection (2).

(5) This section applies to each of the powers of seizure specified in Part 2 of Schedule 1.

52.— Notice of exercise of power under s. 50 or 51.

(1) Where a person exercises a power of seizure conferred by section 50, it shall (subject to subsections (2) and (3)) be his duty, on doing so, to give to the occupier of the premises a written notice—

(a) specifying what has been seized in reliance on the powers conferred by that section;

(b) specifying the grounds on which those powers have been exercised;

(c) setting out the effect of sections 59 to 61;

(d) specifying the name and address of the person to whom notice of an application under section 59(2) to the appropriate judicial authority in respect of any of the seized property must be given; and

(e) specifying the name and address of the person to whom an application may be made to be allowed to attend the initial examination required by any arrangements made for the purposes of section 53(2).

(2) Where it appears to the person exercising on any premises a power of seizure conferred by section 50—

(a) that the occupier of the premises is not present on the premises at the time of the exercise of the power, but

(b) that there is some other person present on the premises who is in charge of the premises,

subsection (1) of this section shall have effect as if it required the notice under that subsection to be given to that other person.

(3) Where it appears to the person exercising a power of seizure conferred by section 50 that there is no one present on the premises to whom he may give a notice for the purposes of complying with subsection (1) of this section, he shall, before leaving the premises, instead of complying with that subsection, attach a notice such as is mentioned in that subsection in a prominent place to the premises.

(4) Where a person exercises a power of seizure conferred by section 51 it shall be his duty, on doing so, to give a written notice to the person from whom the seizure is made—

(a) specifying what has been seized in reliance on the powers conferred by that section;

(b) specifying the grounds on which those powers have been exercised;

(c) setting out the effect of sections 59 to 61;

(d) specifying the name and address of the person to whom notice of any application under section 59(2) to the appropriate judicial authority in respect of any of the seized property must be given; and

(e) specifying the name and address of the person to whom an application may be made to be allowed to attend the initial examination required by any arrangements made for the purposes of section 53(2).

(5) The Secretary of State may by regulations made by statutory instrument, after consultation with the Scottish Ministers, provide that a person who exercises a power of seizure conferred by section 50 shall be required to give a notice such as is mentioned in subsection (1) of this section to any person, or send it to any place, described in the regulations.

(6) Regulations under subsection (5) may make different provision for different cases.

(7) A statutory instrument containing regulations under subsection (5) shall be subject to annulment in pursuance of a resolution of either House of Parliament.

53.— Examination and return of property seized under s. 50 or 51.

(1) This section applies where anything has been seized under a power conferred by section 50 or 51.

(2) It shall be the duty of the person for the time being in possession of the seized property in consequence of the exercise of that power to secure that there are arrangements in force which (subject to section 61) ensure—

(a) that an initial examination of the property is carried out as soon as reasonably practicable after the seizure;

(b) that that examination is confined to whatever is necessary for determining how much of the property falls within subsection (3);

(c) that anything which is found, on that examination, not to fall within subsection (3) is separated from the rest of the seized property and is returned as soon as reasonably practicable after the examination of all the seized property has been completed; and

(d) that, until the initial examination of all the seized property has been completed and anything which does not fall within subsection (3) has been returned, the seized property is kept separate from anything seized under any other power.

(3) The seized property falls within this subsection to the extent only—

(a) that it is property for which the person seizing it had power to search when he made the seizure but is not property the return of which is required by section 54;

(b) that it is property the retention of which is authorised by section 56; or

(c) that it is something which, in all the circumstances, it will not be reasonably practicable, following the examination, to separate from property falling within paragraph (a) or (b).

(4) In determining for the purposes of this section the earliest practicable time for the carrying out of an initial examination of the seized property, due regard shall be had to the desirability of allowing the person from whom it was seized, or a person with an interest in that property, an opportunity of being present or (if he chooses) of being represented at the examination.

(5) In this section, references to whether or not it is reasonably practicable to separate part of the seized property from the rest of it are references to whether or not it is reasonably practicable to do so without prejudicing the use of the rest of that property, or a part of it, for purposes for which (disregarding the part to be separated) the use of the whole or of a part of the rest of the property, if retained, would be lawful.

54.— Obligation to return items subject to legal privilege.

(1) If, at any time after a seizure of anything has been made in exercise of a power of seizure to which this section applies—

(a) it appears to the person for the time being having possession of the seized property in consequence of the seizure that the property—

(i) is an item subject to legal privilege, or

(ii) has such an item comprised in it,

and

(b) in a case where the item is comprised in something else which has been lawfully seized, it is not comprised in property falling within subsection (2),

it shall be the duty of that person to secure that the item is returned as soon as reasonably practicable after the seizure.

(2) Property in which an item subject to legal privilege is comprised falls within this subsection if—

(a) the whole or a part of the rest of the property is property falling within subsection (3) or property the retention of which is authorised by section 56; and

(b) in all the circumstances, it is not reasonably practicable for that item to be separated from the rest of that property (or, as the case may be, from that part of it) without prejudicing the use of the rest of that property, or that part of it, for purposes for which (disregarding that item) its use, if retained, would be lawful.

(3) Property falls within this subsection to the extent that it is property for which the person seizing it had power to search when he made the seizure, but is not property which is required to be returned under this section or section 55.

(4) This section applies—

(a) to the powers of seizure conferred by sections 50 and 51;

(b) to each of the powers of seizure specified in Parts 1 and 2 of Schedule 1; and

(c) to any power of seizure (not falling within paragraph (a) or (b)) conferred on a constable by or under any enactment, including an enactment passed after this Act.

55.— Obligation to return excluded and special procedure material.

(1) If, at any time after a seizure of anything has been made in exercise of a power to which this section applies—

(a) it appears to the person for the time being having possession of the seized property in consequence of the seizure that the property—

(i) is excluded material or special procedure material, or

(ii) has any excluded material or any special procedure material comprised in it,

(b) its retention is not authorised by section 56, and

(c) in a case where the material is comprised in something else which has been lawfully seized, it is not comprised in property falling within subsection (2) or (3),

it shall be the duty of that person to secure that the item is returned as soon as reasonably practicable after the seizure.

(2) Property in which any excluded material or special procedure material is comprised falls within this subsection if—

(a) the whole or a part of the rest of the property is property for which the person seizing it had power to search when he made the seizure but is not property the return of which is required by this section or section 54; and

(b) in all the circumstances, it is not reasonably practicable for that material to be separated from the rest of that property (or, as the case may be, from that part of it) without prejudicing the use of the rest of that property, or that part of it, for purposes for which (disregarding that material) its use, if retained, would be lawful.

(3) Property in which any excluded material or special procedure material is comprised falls within this subsection if—

(a) the whole or a part of the rest of the property is property the retention of which is authorised by section 56; and

(b) in all the circumstances, it is not reasonably practicable for that material to be separated from the rest of that property (or, as the case may be, from that part of it) without prejudicing the use of the rest of that property, or that part of it, for purposes for which (disregarding that material) its use, if retained, would be lawful.

(4) This section applies (subject to subsection (5)) to each of the powers of seizure specified in Part 3 of Schedule 1

(5) In its application to the powers of seizure conferred by—

(a) section 56(5) of the Drug Trafficking Act 1994 (c. 37),

(b) Article 51(5) of the Proceeds of Crime (Northern Ireland) Order 1996 (S.I. 1996 1299 (N.I. 6)), and

(c) section 352(4) of the Proceeds of Crime Act 2002,

this section shall have effect with the omission of every reference to special procedure material.

(6) In this section, except in its application to—

(a) the power of seizure conferred by section 8(2) of the 1984 Act,

(b) the power of seizure conferred by Article 10(2) of the Police and Criminal Evidence (Northern Ireland) Order 1989 (S.I. 1989 1341 (N.I. 12)),

(c) each of the powers of seizure conferred by the provisions of paragraphs 1 and 3 of Schedule 5 to the Terrorism Act 2000 (c. 11), and

(d) the power of seizure conferred by paragraphs 15 and 19 of Schedule 5 to that Act of 2000, so far only as the power in question is conferred by reference to paragraph 1 of that Schedule,

"special procedure material" means special procedure material consisting of documents or records other than documents.

56.— Property seized by constables etc.

(1) The retention of—

(a) property seized on any premises by a constable who was lawfully on the premises,

(b) property seized on any premises by a relevant person who was on the premises accompanied by a constable, and

(c) property seized by a constable carrying out a lawful search of any person,

is authorised by this section if the property falls within subsection (2) or (3).

(2) Property falls within this subsection to the extent that there are reasonable grounds for believing—

(a) that it is property obtained in consequence of the commission of an offence; and

(b) that it is necessary for it to be retained in order to prevent its being concealed, lost, damaged, altered or destroyed.

(3) Property falls within this subsection to the extent that there are reasonable grounds for believing—

(a) that it is evidence in relation to any offence; and

(b) that it is necessary for it to be retained in order to prevent its being concealed, lost, altered or destroyed.

(4) Nothing in this section authorises the retention (except in pursuance of section 54(2)) of anything at any time when its return is required by section 54.

(4A) Subsection (1)(a) includes property seized on any premises—

(a) by a person authorised under section 16(2) of the 1984 Act to accompany a constable executing a warrant, or

(b) by a person accompanying a constable under section 2(6) of the Criminal Justice Act 1987 in the execution of a warrant under section 2(4) of that Act.

(5) In subsection (1)(b) the reference to a relevant person's being on any premises accompanied by a constable is a reference only to a person who was so on the premises under the authority of—

(a) a warrant under section 448 of the Companies Act 1985 (c. 6) authorising him to exercise together with a constable the powers conferred by subsection (3) of that section;

(b) a warrant under Article 441 of the Companies (Northern Ireland) Order 1986 (S.I. 1986 1032 (N.I. 6)) authorising him to exercise together with a constable the powers conferred by paragraph (3) of that Article;

57.— Retention of seized items.

(1) This section has effect in relation to the following provisions (which are about the retention of items which have been seized and are referred to in this section as "the relevant provisions")—

(a) section 22 of the 1984 Act;

(b) Article 24 of the Police and Criminal Evidence (Northern Ireland) Order 1989 (S.I. 1989 1341 (N.I. 12));

(f) section 448(6) of the Companies Act 1985 (c. 6);

(k) paragraph 7(4) of Schedule 3B to the Human Fertilisation and Embryology Act 1990 (c. 37);

(l) section 5(4) of the Knives Act 1997 (c. 21);

(n) section 28(7) of the Competition Act 1998 (c. 41);

(o) sections 122E and 176A of the Financial Services and Markets Act 2000 (c. 8);

(p) paragraph 7(2) of Schedule 3 to the Freedom of Information Act 2000 (c. 36).

(q) paragraph 5(4) of Schedule 5 to the Human Tissue Act 2004;

(r) paragraph 12(3) of Schedule 2 to the Animal Welfare Act 2006;

(s) paragraphs 28(7) and 29(8) of Schedule 5 to the Consumer Rights Act 2015;

(t) paragraph 10 of Schedule 15 to the Data Protection Act 2018.

(2) The relevant provisions shall apply in relation to any property seized in exercise of a power conferred by section 50 or 51 as if the property had been seized under the power of seizure by reference to which the power under that section was exercised in relation to that property.

(3) Nothing in any of sections 53 to 56 authorises the retention of any property at any time when its retention would not (apart from the provisions of this Part) be authorised by the relevant provisions.

(4) Nothing in any of the relevant provisions authorises the retention of anything after an obligation to return it has arisen under this Part.

58.— Person to whom seized property is to be returned.

(1) Where—

(a) anything has been seized in exercise of any power of seizure, and

(b) there is an obligation under this Part for the whole or any part of the seized property to be returned,

the obligation to return it shall (subject to the following provisions of this section) be an obligation to return it to the person from whom it was seized.

(2) Where—

(a) any person is obliged under this Part to return anything that has been seized to the person from whom it was seized, and

(b) the person under that obligation is satisfied that some other person has a better right to that thing than the person from whom it was seized,

his duty to return it shall, instead, be a duty to return it to that other person or, as the case may be, to the person appearing to him to have the best right to the thing in question.

(3) Where different persons claim to be entitled to the return of anything that is required to be returned under this Part, that thing may be retained for as long as is reasonably necessary for the determination in accordance with subsection (2) of the person to whom it must be returned.

(4) References in this Part to the person from whom something has been seized, in relation to a case in which the power of seizure was exercisable by reason of that thing's having been found on any premises, are references to the occupier of the premises at the time of the seizure.

(5) References in this section to the occupier of any premises at the time of a seizure, in relation to a case in which—

(a) a notice in connection with the entry or search of the premises in question, or with the seizure, was given to a person appearing in the occupier's absence to be in charge of the premises, and

(b) it is practicable, for the purpose of returning something that has been seized, to identify that person but not to identify the occupier of the premises,

are references to that person.

59.— Application to the appropriate judicial authority.

(1) This section applies where anything has been seized in exercise, or purported exercise, of a relevant power of seizure.

(2) Any person with a relevant interest in the seized property may apply to the appropriate judicial authority, on one or more of the grounds mentioned in subsection (3), for the return of the whole or a part of the seized property.

(3) Those grounds are—

(a) that there was no power to make the seizure;

(b) that the seized property is or contains an item subject to legal privilege that is not comprised in property falling within section 54(2);

(c) that the seized property is or contains any excluded material or special procedure material which—

(i) has been seized under a power to which section 55 applies;

(ii) is not comprised in property falling within section 55(2) or (3); and

(iii) is not property the retention of which is authorised by section 56;

(d) that the seized property is or contains something seized under section 50 or 51 which does not fall within section 53(3);

and subsections (5) and (6) of section 55 shall apply for the purposes of paragraph (c) as they apply for the purposes of that section.

(4) Subject to subsection (6), the appropriate judicial authority, on an application under subsection (2), shall—

(a) if satisfied as to any of the matters mentioned in subsection (3), order the return of so much of the seized property as is property in relation to which the authority is so satisfied; and

(b) to the extent that that authority is not so satisfied, dismiss the application.

(5) The appropriate judicial authority—

(a) on an application under subsection (2),

(b) on an application made by the person for the time being having possession of anything in consequence of its seizure under a relevant power of seizure, or

may give such directions as the authority thinks fit as to the examination, retention, separation or return of the whole or any part of the seized property.

(6) On any application under this section, the appropriate judicial authority may authorise the retention of any property which—

(a) has been seized in exercise, or purported exercise, of a relevant power of seizure, and

(b) would otherwise fall to be returned,

if that authority is satisfied that the retention of the property is justified on grounds falling within subsection (7).

(7) Those grounds are that (if the property were returned) it would immediately become appropriate—

(a) to issue, on the application of the person who is in possession of the property at the time of the application under this section, a warrant in pursuance of which, or of the exercise of which, it would be lawful to seize the property; or

(b) to make an order under—

(i) paragraph 4 of Schedule 1 to the 1984 Act,

(ii) paragraph 4 of Schedule 1 to the Police and Criminal Evidence (Northern Ireland) Order 1989 (S.I. 1989 1341 (N.I. 12)),

(iii) section 20BA of the Taxes Management Act 1970 (c. 9), or

(iv) paragraph 5 of Schedule 5 to the Terrorism Act 2000 (c. 11),

under which the property would fall to be delivered up or produced to the person mentioned in paragraph (a).

(8) Where any property which has been seized in exercise, or purported exercise, of a relevant power of seizure has parts ("part A" and "part B") comprised in it such that—

(a) it would be inappropriate, if the property were returned, to take any action such as is mentioned in subsection (7) in relation to part A,

(b) it would (or would but for the facts mentioned in paragraph (a)) be appropriate, if the property were returned, to take such action in relation to part B, and

(c) in all the circumstances, it is not reasonably practicable to separate part A from part B without prejudicing the use of part B for purposes for which it is lawful to use property seized under the power in question,

the facts mentioned in paragraph (a) shall not be taken into account by the appropriate judicial authority in deciding whether the retention of the property is justified on grounds falling within subsection (7).

(9) If a person fails to comply with any order or direction made or given by a judge of the Crown Court in exercise of any jurisdiction under this section—

(a) the authority may deal with him as if he had committed a contempt of the Crown Court; and

(b) any enactment relating to contempt of the Crown Court shall have effect in relation to the failure as if it were such a contempt.

(10) The relevant powers of seizure for the purposes of this section are—

(a) the powers of seizure conferred by sections 50 and 51;

(b) each of the powers of seizure specified in Parts 1 and 2 of Schedule 1; and

(c) any power of seizure (not falling within paragraph (a) or (b)) conferred on a constable by or under any enactment, including an enactment passed after this Act.

(11) References in this section to a person with a relevant interest in seized property are references to—

(a) the person from whom it was seized;

(b) any person with an interest in the property; or

(c) any person, not falling within paragraph (a) or (b), who had custody or control of the property immediately before the seizure.

(12) For the purposes of subsection (11)(b), the persons who have an interest in seized property shall, in the case of property which is or contains an item subject to legal privilege, be taken to include the person in whose favour that privilege is conferred.

(13) Criminal Procedure Rules may make provision about proceedings under this section on an application to a judge of the Crown Court in England and Wales.

60.— Cases where duty to secure arises.

(1) Where property has been seized in exercise, or purported exercise, of any power of seizure conferred by section 50 or 51, a duty to secure arises under section 61 in relation to the seized property if—

(a) a person entitled to do so makes an application under section 59 for the return of the property;

(b) in relation to England, Wales and Northern Ireland, at least one of the conditions set out in subsections (2) and (3) is satisfied;

(c) in relation to Scotland, the condition set out in subsection (2) is satisfied; and

(d) notice of the application is given to a relevant person.

(2) The first condition is that the application is made on the grounds that the seized property is or contains an item subject to legal privilege that is not comprised in property falling within section 54(2).

(3) The second condition is that—

(a) the seized property was seized by a person who had, or purported to have, power under this Part to seize it by virtue only of one or more of the powers specified in subsection (6); and

(b) the application—

(i) is made on the ground that the seized property is or contains something which does not fall within section 53(3); and

(ii) states that the seized property is or contains special procedure material or excluded material.

(4) In relation to property seized by a person who had, or purported to have, power under this Part to seize it by virtue only of one or more of the powers of seizure conferred by—

(b) section 56(5) of the Drug Trafficking Act 1994 (c. 37),

(c) Article 51(5) of the Proceeds of Crime (Northern Ireland) Order 1996 (S.I. 1996 1299 (N.I. 6)), or

(d) section 352(4) of the Proceeds of Crime Act 2002,

the second condition is satisfied only if the application states that the seized property is or contains excluded material

(5) In relation to property seized by a person who had, or purported to have, power under this Part to seize it by virtue only of one or more of the powers of seizure specified in Part 3 of Schedule 1 but not by virtue of—

(a) the power of seizure conferred by section 8(2) of the 1984 Act,

(b) the power of seizure conferred by Article 10(2) of the Police and Criminal Evidence (Northern Ireland) Order 1989 (S.I. 1989 1341 (N.I. 12)),

(c) either of the powers of seizure conferred by paragraphs 1 and 3 of Schedule 5 to the Terrorism Act 2000 (c. 11), or

(d) either of the powers of seizure conferred by paragraphs 15 and 19 of Schedule 5 to that Act of 2000 so far as they are conferred by reference to paragraph 1 of that Schedule,

the second condition is satisfied only if the application states that the seized property is or contains excluded material or special procedure material consisting of documents or records other than documents.

(6) The powers mentioned in subsection (3) are—

(a) the powers of seizure specified in Part 3 of Schedule 1;

(b) the powers of seizure conferred by the provisions of Parts 2 and 3 of the 1984 Act (except section 8(2) of that Act);

(c) the powers of seizure conferred by the provisions of Parts 3 and 4 of the Police and Criminal Evidence (Northern Ireland) Order 1989 (except Article 10(2) of that Order);

(d) the powers of seizure conferred by the provisions of paragraph 11 of Schedule 5 to the Terrorism Act 2000; and

(e) the powers of seizure conferred by the provisions of paragraphs 15 and 19 of that Schedule so far as they are conferred by reference to paragraph 11 of that Schedule.

(7) In this section “a relevant person” means any one of the following—

(a) the person who made the seizure;

(b) the person for the time being having possession, in consequence of the seizure, of the seized property;

(c) the person named for the purposes of subsection (1)(d) or (4)(d) of section 52 in any notice given under that section with respect to the seizure.

61.— The duty to secure.

(1) The duty to secure that arises under this section is a duty of the person for the time being having possession, in consequence of the seizure, of the seized property to secure that arrangements are in force that ensure that the seized property (without being returned) is not, at any time after the giving of the notice of the application under section 60(1), either—

(a) examined or copied, or

(b) put to any use to which its seizure would, apart from this subsection, entitle it to be put,

except with the consent of the applicant or in accordance with the directions of the appropriate judicial authority.

(2) Subsection (1) shall not have effect in relation to any time after the withdrawal of the application to which the notice relates.

(3) Nothing in any arrangements for the purposes of this section shall be taken to prevent the giving of a notice under section 49 of the Regulation of Investigatory Powers Act 2000 (c. 23) (notices for the disclosure of material protected by encryption etc.) in respect of any information contained in the seized material; but subsection (1) of this section shall apply to anything disclosed for the purpose of complying with such a notice as it applies to the seized material in which the information in question is contained.

(4) Subsection (9) of section 59 shall apply in relation to any jurisdiction conferred on the appropriate judicial authority by this section as it applies in relation to the jurisdiction conferred by that section.

62.— Use of inextricably linked property.

(1) This section applies to property, other than property which is for the time being required to be secured in pursuance of section 61, if—

(a) it has been seized under any power conferred by section 50 or 51 or specified in Part 1 or 2 of Schedule 1, and

(b) it is inextricably linked property.

(2) Subject to subsection (3), it shall be the duty of the person for the time being having possession, in consequence of the seizure, of the inextricably linked property to ensure that arrangements are in force which secure that that property (without being returned) is not at any time, except with the consent of the person from whom it was seized, either—

(a) examined or copied, or

(b) put to any other use.

(3) Subsection (2) does not require that arrangements under that subsection should prevent inextricably linked property from being put to any use falling within subsection (4).

(4) A use falls within this subsection to the extent that it is use which is necessary for facilitating the use, in any investigation or proceedings, of property in which the inextricably linked property is comprised.

(5) Property is inextricably linked property for the purposes of this section if it falls within any of subsections (6) to (8).

(6) Property falls within this subsection if—

(a) it has been seized under a power conferred by section 50 or 51; and

(b) but for subsection (3)(c) of section 53, arrangements under subsection (2) of that section in relation to the property would be required to ensure the return of the property as mentioned in subsection (2)(c) of that section.

(7) Property falls within this subsection if—

(a) it has been seized under a power to which section 54 applies; and

(b) but for paragraph (b) of subsection (1) of that section, the person for the time being having possession of the property would be under a duty to secure its return as mentioned in that subsection.

(8) Property falls within this subsection if—

(a) it has been seized under a power of seizure to which section 55 applies; and

(b) but for paragraph (c) of subsection (1) of that section, the person for the time being having possession of the property would be under a duty to secure its return as mentioned in that subsection.

63.— Copies.

(1) Subject to subsection (3)—

(a) in this Part, “seize” includes “take a copy of”, and cognate expressions shall be construed accordingly;

(b) this Part shall apply as if any copy taken under any power to which any provision of this Part applies were the original of that of which it is a copy; and

(c) for the purposes of this Part, except sections 50 and 51, the powers mentioned in subsection (2) (which are powers to obtain hard copies etc. of information which is stored in electronic form) shall be treated as powers of seizure, and references to seizure and to seized property shall be construed accordingly.

(2) The powers mentioned in subsection (1)(c) are any powers which are conferred by—

(a) section 19(4) or 20 of the 1984 Act;

(b) Article 21(4) or 22 of the Police and Criminal Evidence (Northern Ireland) Order 1989 (S.I. 1989 1341 (N.I. 12));

(c) section 46(3) of the Firearms Act 1968 (c. 27);

(f) section 32(6)(b) of the Food Safety Act 1990 (c. 16);

(g) Article 34(6)(b) of the Food Safety (Northern Ireland) Order 1991 (S.I. 1991 762 (N.I. 7));

(ga) section 23E(5)(b) (as read with section 23K(2)) of the Criminal Law (Consolidation) (Scotland) Act 1995;

(h) section 28(2)(f) of the Competition Act 1998 (c. 41); or

(i) section 8(2)(c) of the Nuclear Safeguards Act 2000 (c. 5).

(3) Subsection (1) does not apply to section 50(6) or 57.

64.— Meaning of "appropriate judicial authority".

(1) Subject to subsection (2), in this Part "appropriate judicial authority" means—

(a) in relation to England and Wales and Northern Ireland, a judge of the Crown Court;

(b) in relation to Scotland, a sheriff.

(2) In this Part "appropriate judicial authority", in relation to the seizure of items under any power mentioned in subsection (3) and in relation to items seized under any such power, means—

(a) in relation to England and Wales and Northern Ireland, the High Court;

(b) in relation to Scotland, the Court of Session.

(3) Those powers are—

(a) the powers of seizure conferred by—

(i) section 448(3) of the Companies Act 1985 (c. 6);

(ii) Article 441(3) of the Companies (Northern Ireland) Order 1986 (S.I. 1986 1032 (N.I. 6)); and

(iii) section 28(2) of the Competition Act 1998;

(aa) the power of seizure conferred by section 352(4) of the Proceeds of Crime Act 2002, if the power is exercisable for the purposes of a civil recovery investigation or a detained cash investigation (within the meaning of Part 8 of that Act);

(b) any power of seizure conferred by section 50, so far as that power is exercisable by reference to any power mentioned in paragraph (a).

65.— Meaning of "legal privilege".

(1) Subject to the following provisions of this section, references in this Part to an item subject to legal privilege shall be construed—

(a) for the purposes of the application of this Part to England and Wales, in accordance with section 10 of the 1984 Act (meaning of "legal privilege");

(b) for the purposes of the application of this Part to Scotland, in accordance with section 412 of the Proceeds of Crime Act 2002 (interpretation); and

(c) for the purposes of the application of this Part to Northern Ireland, in accordance with Article 12 of the Police and Criminal Evidence (Northern Ireland) Order 1989 (S.I. 1989 1341 (N.I. 12)) (meaning of "legal privilege").

(2) In relation to property which has been seized in exercise, or purported exercise, of—

(a) the power of seizure conferred by section 28(2) of the Competition Act 1998, or

(b) so much of any power of seizure conferred by section 50 as is exercisable by reference to that power,

references in this Part to an item subject to legal privilege shall be read as references to a privileged communication within the meaning of section 30 of that Act.

(3A) In relation to property which has been seized in exercise, or purported exercise, of—

(a) the power of seizure conferred by section 352(4) of the Proceeds of Crime Act 2002, or

(b) so much of any power of seizure conferred by section 50 as is exercisable by reference to that power,

references in this Part to an item subject to legal privilege shall be read as references to privileged material within the meaning of section 354(2) of that Act.

(4) An item which is, or is comprised in, property which has been seized in exercise, or purported exercise, of the power of seizure conferred by section 448(3) of the Companies Act 1985 (c. 6) shall be taken for the purposes of this Part to be an item subject to legal privilege if, and only if, the seizure of that item was in contravention of section 452(2) of that Act (privileged information).

(5) An item which is, or is comprised in, property which has been seized in exercise, or purported exercise, of the power of seizure conferred by Article 441(3) of the Companies (Northern Ireland) Order 1986 (S.I. 1986 1032 (N.I. 6)) shall be taken for the purposes of this Part to be an item subject to legal privilege if, and only if, the seizure of that item was in contravention of Article 445(2) of that Order (privileged information).

(6) An item which is, or is comprised in, property which has been seized in exercise, or purported exercise, of the power of seizure conferred by sub-paragraph (2) of paragraph 3 of Schedule 2 to the Timeshare Act 1992 (c. 35) shall be taken for the purposes of this Part to be an item subject to legal privilege if, and only if, the seizure of that item was in contravention of sub-paragraph (4) of that paragraph (privileged documents).

(7) An item which is, or is comprised in, property which has been seized in exercise, or purported exercise, of the power of seizure conferred by paragraphs 1 and 2 of Schedule 15 to the Data Protection Act 2018 shall be taken for the purposes of this Part to be an item subject to legal privilege if, and only if, the seizure of that item was in contravention of paragraph 11 (matters exempt from inspection and seizure: privileged communications) of that Schedule (privileged communications).

(8) An item which is, or is comprised in, property which has been seized in exercise, or purported exercise, of the power of seizure conferred by paragraph 1 of Schedule 3 to the Freedom of Information Act 2000 (c. 36) shall be taken for the purposes of this Part to be an item subject to legal privilege if, and only if, the seizure of that item was in contravention of paragraph 9 of that Schedule (privileged communications).

(8B) An item which is, or is comprised in, property which has been seized in exercise or purported exercise of the power of seizure conferred by paragraph 27(1)(b) or 29(1) of Schedule 5 to the Consumer Rights Act 2015 shall be taken for the purposes of this Part to be an item subject to legal privilege if, and only if, the seizure of that item was in contravention of paragraph 27(6) or (as the case may be) 29(6) of that Schedule (privileged documents).

(9) An item which is, or is comprised in, property which has been seized in exercise, or purported exercise, of so much of any power of seizure conferred by section 50 as is exercisable by reference to a power of seizure conferred by—

(a) section 448(3) of the Companies Act 1985,

(b) Article 441(3) of the Companies (Northern Ireland) Order 1986,

(c) paragraph 3(2) of Schedule 2 to the Timeshare Act 1992,

(d) paragraph 1 of Schedule 9 to the Data Protection Act 1998, or

(e) paragraph 1 of Schedule 3 to the Freedom of Information Act 2000,

shall be taken for the purposes of this Part to be an item subject to legal privilege if, and only if, the item would have been taken for the purposes of this Part to be an item subject to legal privilege had it been seized under the power of seizure by reference to which the power conferred by section 50 was exercised.

66.— General interpretation of Part 2.

(1) In this Part—

"appropriate judicial authority" has the meaning given by section 64;

"documents" includes information recorded in any form;

"item subject to legal privilege" shall be construed in accordance with section 65;

"marine installation" has the meaning given by section 262 of the Marine and Coastal Access Act 2009;

"premises" includes any vehicle, stall or moveable structure (including an offshore installation or other marine installation) and any other place whatever, whether or not occupied as land;

"offshore installation" has the same meaning as in the Mineral Workings (Offshore Installations) Act 1971 (c. 61);

"return", in relation to seized property, shall be construed in accordance with section 58, and cognate expressions shall be construed accordingly;

"seize", and cognate expressions, shall be construed in accordance with section 63(1) and subsection (5) below;

"seized property", in relation to any exercise of a power of seizure, means (subject to subsection (5)) anything seized in exercise of that power; and

"vehicle" includes any vessel, aircraft or hovercraft.

(2) In this Part references, in relation to a time when seized property is in any person's possession in consequence of a seizure ("the relevant time"), to something for which the person making the seizure had power to search shall be construed—

(a) where the seizure was made on the occasion of a search carried out on the authority of a warrant, as including anything of the description of things the presence or suspected presence of which provided grounds for the issue of the warrant;

(b) where the property was seized in the course of a search on the occasion of which it would have been lawful for the person carrying out the search to seize anything which on that occasion was believed by him to be, or appeared to him to be, of a particular description, as including—

(i) anything which at the relevant time is believed by the person in possession of the seized property, or (as the case may be) appears to him, to be of that description; and

(ii) anything which is in fact of that description;

(c) where the property was seized in the course of a search on the occasion of which it would have been lawful for the person carrying out the search to seize anything which there were on that occasion reasonable grounds for believing was of a particular description, as including—

(i) anything which there are at the relevant time reasonable grounds for believing is of that description; and

(ii) anything which is in fact of that description;

(d) where the property was seized in the course of a search to which neither paragraph (b) nor paragraph (c) applies, as including anything which is of a description of things which, on the occasion of the search, it would have been lawful for the person carrying it out to seize otherwise than under section 50 and 51; and

(e) where the property was seized on the occasion of a search authorised under section 82 of the Terrorism Act 2000 (c. 11) (seizure of items suspected to have been, or to be intended to be, used in commission of certain offences), as including anything—

(i) which is or has been, or is or was intended to be, used in the commission of an offence such as is mentioned in subsection (3)(a) or (b) of that section; or

(ii) which at the relevant time the person who is in possession of the seized property reasonably suspects is something falling within sub-paragraph (i).

(3) For the purpose of determining in accordance with subsection (2), in relation to any time, whether or to what extent property seized on the occasion of a search authorised under section 9 of the Official Secrets Act 1911 (c. 28) (seizure of evidence of offences under that Act having been or being about to be committed) is something for which the person making the seizure had power to search, subsection (1) of that section shall be construed—

(a) as if the reference in that subsection to evidence of an offence under that Act being about to be committed were a reference to evidence of such an offence having been, at the time of the seizure, about to be committed; and

(b) as if the reference in that subsection to reasonable ground for suspecting that such an offence is about to be committed were a reference to reasonable ground for suspecting that at the time of the seizure such an offence was about to be committed.

(4) References in subsection (2) to a search include references to any activities authorised by virtue of any of the following—

(b) section 29(1) of the Fair Trading Act 1973 (c. 41) (power to enter premises and to inspect and seize goods and documents);

(h) section 29 of the Consumer Protection Act 1987 (c. 43) (powers of search etc.);

(j) section 32(5) of the Food Safety Act 1990 (c. 16) (power to inspect records relating to a food business);

(ja) paragraph 5 of Schedule 3B to the Human Fertilisation and Embryology Act 1990;

(l) Article 33(6) of the Food Safety (Northern Ireland) Order 1991 (S.I. 1991 762 (N.I. 7));

(m) paragraph 3 of Schedule 2 to the Timeshare Act 1992 (c. 35) (powers of officers of enforcement authority);

(n) paragraph 2 of Schedule 5 to the Human Tissue Act 2004 (entry and inspection of licensed premises);

(o) regulation 22(4) of the General Product Safety Regulations 2005 (powers of entry and search etc);

(p) sections 26(1), 27(1), 28(1) and 29(1) of the Animal Welfare Act 2006 (inspection in connection with licences, inspection in connection with registration, inspection of farm premises and inspection relating to EU obligations);

(t) Part 4 of Schedule 5 to the Consumer Rights Act 2015.

(5) References in this Part to a power of seizure include references to each of the powers to take possession of items under—

(b) section 448(3) of the Companies Act 1985 (c. 6);

(f) section 2(5) of the Criminal Justice Act 1987 (c. 38);

(h) section 28(2)(c) of the Competition Act 1998 (c. 41); and

(i) section 176(5) of the Financial Services and Markets Act 2000 (c. 8);

and references in this Part to seizure and to seized property shall be construed accordingly.

(6) In this Part, so far as it applies to England and Wales—

(a) references to excluded material shall be construed in accordance with section 11 of the 1984 Act (meaning of “excluded material”); and

(b) references to special procedure material shall be construed in accordance with section 14 of that Act (meaning of “special procedure material”).

(7) In this Part, so far as it applies to Northern Ireland—

(a) references to excluded material shall be construed in accordance with Article 13 of the Police and Criminal Evidence (Northern Ireland) Order 1989 (S.I. 1989 1341 (N.I. 12)) (meaning of “excluded material”); and

(b) references to special procedure material shall be construed in accordance with Article 16 of that Order (meaning of "special procedure material").

(8) References in this Part to any item or material being comprised in other property include references to its being mixed with that other property.

(9) In this Part "enactment" includes an enactment contained in Northern Ireland legislation.

67.— Application to officers of Revenue and Customs.

The powers conferred by section 114(2) of the 1984 Act and Article 85(1) of the Police and Criminal Evidence (Northern Ireland) Order 1989 (application of provisions relating to police officers to officers of Revenue and Customs) shall have effect in relation to the provisions of this Part as they have effect in relation to the provisions of that Act or, as the case may be, that Order.

67A.— Application to Welsh Revenue Authority

(1) The Welsh Ministers may by regulations—

(a) direct that any provision of this Part is to apply, subject to such modifications as the regulations may specify, to investigations of offences conducted by the Welsh Revenue Authority;

(b) make provision permitting a person exercising a function conferred on the Welsh Revenue Authority by the regulations to use reasonable force in the exercise of such a function.

(2) Regulations under subsection (1) may—

(a) make provision that applies generally or only in specified cases,

(b) make different provision for different cases or circumstances, and

(c) may, in modifying a provision, in particular impose conditions on the exercise of a function.

(3) The power to make regulations under subsection (1) is exercisable by statutory instrument.

(4) A statutory instrument containing regulations under subsection (1) may not be made unless a draft of the instrument has been laid before, and approved by a resolution of, the National Assembly for Wales.

68.— Application to Scotland.

(1) In the application of this Part to Scotland—

(a) subsection (4) of section 54 and subsection (10) of section 59 shall each have effect with the omission of paragraph (c) of that subsection;

(b) section 55 and subsection (3)(c) of section 59 shall be omitted; and

(c) Schedule 1 shall have effect as if the powers specified in that Schedule did not include any power of seizure under any enactment mentioned in that Schedule, so far as it is exercisable in Scotland by a constable, except a power conferred by an enactment mentioned in subsection (2).

(2) Those enactments are—

(a) section 43(5) of the Gaming Act 1968 (c. 65);

(c) section 448(3) of the Companies Act 1985 (c. 6);

(f) section 176(5) of the Financial Services and Markets Act 2000 (c. 8); and

(g) regulation 70(7) of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

69.— Application to powers designated by order.

(1) The Secretary of State may by order—

(a) provide for any power designated by the order to be added to those specified in Schedule 1 or section 63(2);

(b) make any modification of the provisions of this Part which the Secretary of State considers appropriate in consequence of any provision made by virtue of paragraph (a);

(c) make any modification of any enactment making provision in relation to seizures, or things seized, under a power designated by an order under this subsection which the Secretary of State considers appropriate in consequence of any provision made by virtue of that paragraph.

(2) Where the power designated by the order made under subsection (1) is a power conferred in relation to Scotland, the Secretary of State shall consult the Scottish Ministers before making the order.

(2A) Where the power designated by the order made under subsection (1) is a power conferred in relation to Northern Ireland, the Secretary of State shall consult the Department of Justice in Northern Ireland before making the order.

(3) The power to make an order under subsection (1) shall be exercisable by statutory instrument; and no such order shall be made unless a draft of it has been laid before Parliament and approved by a resolution of each House.

(4) In this section “modification” includes any exclusion, extension or application.

70.— Consequential applications and amendments of enactments.

Schedule 2 (which applies enactments in relation to provision made by this Part and contains minor and consequential amendments) shall have effect.