Neutral Citation Number: [2022] UKIP Trib 6
Case No: **IPT/20/62/H**

IN THE INVESTIGATORY POWERS TRIBUNAL

Date: 30 December 2022

Before :

LORD JUSTICE EDIS
PROFESSOR GRAHAM ZELLICK CBE KC
and
MR DESMOND BROWNE CBE KC

- -

Between :

DAMIAN HILL	**Appellant**
- and -	
METROPOLITAN POLICE SERVICE & INDEPENDENT OFFICE FOR POLICE CONDUCT	**Respondent**

- -

Nicholas Yeo and Ryan Dowding (instructed by **Reynolds Dawson**) for the **Claimant**

Neil Sheldon KC and Ruby Shrimpton (instructed by **Metropolitan Police Service**) for the **First Respondent**

Andrew Bird KC (instructed by **Independent Office for Police Conduct**) for the **Second Respondent**

Julian Milford KC (instructed by **Home office**) for the **Interested Party**

Rosemary Davidson as Counsel to the Tribunal

Hearing dates : 21 and 22 June 2022

JUDGMENT

1. This is the Judgment of the Tribunal. The complainant/claimant is not anonymised and is not subject to any criminal or disciplinary proceedings arising out of the matters we will set out. We have not named other individual police officers at all where there may be some proceedings arising of these matters and their conduct is not relevant to the issues we have to decide. This judgment follows a public hearing without reporting restrictions and no party sought any.

Introduction

2. This is a complaint and a human rights claim brought by Detective Sergeant Damian Hill against the Metropolitan Police Service ("MPS") and the Independent Office for Police Conduct ("IOPC"). It relates to two episodes in respect of which the Tribunal has, or may have, jurisdiction. Those episodes occurred within a series of events about which Sergeant Hill also complains, but much of that is not within the jurisdiction of the Tribunal. It would be wrong for the Tribunal to express any view about matters which are not within its jurisdiction as other proceedings in other courts may be brought in order to address those complaints. We intend to decide only those matters which we have to decide in order to deal with the claims within our jurisdiction. Sergeant Hill complains that his data was unlawfully obtained by the MPS and IOPC in two ways: first they obtained communications data relating to his use of a mobile phone ("the communications data claim"), and secondly, they subsequently downloaded its content purportedly exercising powers under the Police and Criminal Evidence Act 1984 (PACE) ("the phone download claim"). He alleges that by doing so those bodies breached his right under Article 8 of the ECHR to a private life. For the purposes of the procedure of the Tribunal, this results in both a claim and a complaint in respect of these two acts, using the terminology of section 65(2) of the Regulation of Investigatory Powers Act 2000 (RIPA). In substance, the complaint and the human rights proceedings raise the same issue. If the complaint succeeds in demonstrating unlawfulness in the conduct (which interfered with Sergeant Hill's Article 8 rights) then it will necessarily follow that the interference was not "in accordance with law" and his human rights claim will succeed to the same extent. That is not in dispute. What is in issue is the extent of the unlawful conduct and the extent of the Tribunal's jurisdiction in respect of the downloading of the phone.

Factual context

3. The facts are set out in a Crown Court judgment which is Annex A and a chronology prepared by the IOPC for the Tribunal which is Annex B. It is necessary briefly to summarise the context in order to assist comprehension. In doing so, we refer in passing to

matters which are not within our jurisdiction but are not intending to make any findings about such things. An incident took place on 15 May 2018 when a drug dealer called Dean Francis was arrested by an Operation Trident surveillance team of the Metropolitan Police. In the course of his arrest, or immediately before it, he was injured when one of the surveillance vehicles came into contact with him, knocking him over some railings and down into the area between the street and a house. He subsequently pleaded guilty to supplying class A drugs and received a substantial prison sentence. Sergeant Hill and Detective Constable X were involved in the operation, but neither was the driver of the vehicle which collided with Mr. Francis. Detective Constable X was the driver of another vehicle and had fitted his own dashcam camera which recorded footage of the collision. That footage showed that at the point when he was knocked over the railings Mr. Francis was carrying a bag, which later turned out to contain 500g of cocaine. He was later to say that the bag which was found beside him after his fall had been put there by someone else, and that it was a coincidence that he landed close to it. The film showed that this account was false. After his arrest, Sergeant Hill became the officer in charge of the investigation into him. The incident was referred to the IOPC as a death or serious injury matter in accordance with Part 2 of and Schedule 3 to the Police Reform Act 2002. The IOPC decided to refer the investigation into the incident back to the MPS for a local investigation by the Department of Professional Standards ("DPS"). A police officer from traffic was involved and took possession of Officer B's film. This was then held by the MPS DPS. On 7 June 2018 Sergeant Hill viewed that footage which was made available to him by the DPS. He recorded the screen on his personal mobile phone as a video clip. He later explained that he did this because it was easier to view the footage in that way for his purposes as officer in charge of the investigation into Mr. Francis than it was on the standalone computer in which it was held, because the phone had different software. He later sent his video of the footage by WhatsApp to Officer B, at his request, in circumstances described in the chronology entry for that day at Annex B. The IOPC then redetermined its original decision on 6 July 2018 and established its own independent enquiry, called Operation Irwin, into the circumstances in which Mr. Francis had been injured. That resulted in the seizure of phones from three officers on 13 September 2018. These were (1) the driver of the vehicle which collided with Mr. Francis, Officer C, (2) Officer B, and (3) another officer, not Sergeant Hill. Analysis of these phones showed the existence of WhatsApp groups in which officers of the MPS (including Sergeant Hill) were communicating with each other about police business. This practice has since become

notorious, but was already a matter of concern and the MPS referred these three officers for investigation by the IOPC for possible breaches of the criminal law relating to data protection. An IOPC operation was set up, called Operation Trent, to investigate these referrals. There was no referral at this time in relation to Sergeant Hill. Notwithstanding this, the IOPC later decided to investigate him, and to seize his phone, which they did on 19 June 2019. That seizure, the Crown Court has decided, was unlawful, see the judgment at Annex A. It was done by an IOPC investigator who wrongly believed that he had the powers of seizure of a constable under PACE. In the absence of a referral by the MPS to the IOPC in respect of Sergeant Hill under the Police Reform Act 2002 this was not so. Before the seizure, and in preparation for it, the IOPC obtained communications data from Sergeant Hill's service provider as described below. Afterwards, the content of the phone was extracted by the MPS acting on behalf of the IOPC. That data was never examined and has now been destroyed. It will be apparent that there may be civil proceedings arising from the unlawful seizure of the phone, and perhaps criminal or disciplinary proceedings arising from various aspects of this sequence of events. We are concerned only with the communications data claim and, if we have jurisdiction, the phone download claim.

The allegations in outline

4. The two episodes about which complaint is made are as follows:-

   a. **The communications data claim:** On 29 March 2019, an application under section 22 of the Regulation of Investigatory Powers Act 2000 (RIPA)[1] was approved by the IOPC's 'designated person', Mike Benbow, who stated:

   "I have considered the crimes under investigation of misconduct in public office and perverting the course of justice. These are serious offences and as such the public expect that where a person employed by the state is suspected of such offences every legal method should be used to seek to prove or disprove the allegations. I have considered the actions proposed and consider them necessary to assist in this investigation. I consider them proportionate to the crimes under investigation…".

   A notice was issued requiring Hutchinson 3G to produce communications data for the period 14 May 2018 to 7 July 2018, and for 26 March 2019 for a mobile

[1] At the material time section 22 of RIPA was still in force, in a heavily amended version. It is only necessary to analyse the provision and its legislative history to a very limited extent.

number used at all times by Sergeant Hill as his personal mobile phone. The IOPC now concedes that this period was too long, and that some of the data was therefore unlawfully obtained. Sergeant Hill's case is that the application should not have been made or approved, and that the obtaining of all the data was unlawful. As will appear, we agree. There is no doubt that this complaint is within our jurisdiction.

b. **The handset download claim:** On 19 June 2019, Sergeant Hill was required to attend a meeting with the IOPC. The IOPC Policy Decision 90 records the IOPC's belief that the investigating officers who attended the meeting had the powers of a constable pursuant to section 13 of and paragraph 19(4) of Schedule 3 to the Police Reform Act 2002. It is now agreed that they did not, because there had been no referral by the MPS to the IOPC in respect of Sergeant Hill, as is required by that Act before the powers it confers become exercisable by the IOPC. It is common ground that: (a) the Complainant was informed that he would be arrested if he did not hand the device over; and (b) the mobile telephone was seized by Kieran Casserly, an IPCO officer, purporting to exercise the powers of a constable pursuant to section 19 of PACE. That seizure was unlawful, it is agreed, because he did not have the powers which he purported to exercise. The complaint about seizure is not within our jurisdiction. However, a series of events unfolded as follows:-

The decryption of the PIN on the Complainant's device and the initial download of data

i. Jack Lee, another IOPC Officer, states that, between 19 June 2019 and December 2019, *"attempts were made to access [Sergeant Hill's] mobile phone after he refused to provide the PIN"*.

ii. On 20 September 2019, Mr. Lee completed a *'National Digital Exploitation Unit Tasking Form'* stating that Sergeant Hill was being investigated in relation to data protection offences and requesting that the mobile telephone be accessed to download the data. The form stated that the device had been seized pursuant to section 19 of PACE and noted that, as the Complainant had refused to provide his PIN, *"the next course of action is to unlock it through brute force"*.

iii. On 8 October 2019, an MPS officer, DC James Lynch, took possession of Sergeant Hill's mobile phone, now known as KCA/3, and used digital media exploitation software to attempt to discover the PIN code to the device. The attempt was unsuccessful but he repeated the exercise on 2 December 2019 and discovered the PIN code which he used to unlock the device. DC Lynch *"obtained a full read of the device"* and copied it to an encrypted USB drive (KCA/3/JWL/1). DC Lynch has confirmed that he did not forensically process or view the data.

Forensic examination of the Complainant's data

iv. In December 2019, Jack Lee made a submission to the MPS Professional Standards High Tech Crime Unit requesting assistance with the examination of KCA/3 and KCA/3/JWL/1.

v. Mr. Lee also completed a 'Digital Examination Request'. The Digital Examination Request included the assertion *"this is a criminal investigation and, as such, the IOPC has the legal authority to access all information on the mobile phone"*. The request included date range parameters (15 May 2018 to 19 June 2019) *"to ensure the download is proportionate"*.

vi. The Digital Examination Request form contained a box headed 'is this action likely to result in the acquisition of confidential material or personal data?' and Mr. Lee ticked the boxes for: (a) matters subject to legal privilege; (b) confidential personal information; and (c) personal data. In a box headed 'Exhibits seized under the following power' Mr. Lee ticked *"s19. PACE 1984 exercisable by a constable lawfully on premises"*.

vii. On 30 December 2019 David Balcombe, an MPS Digital Forensic Examiner, conducted a forensic examination of KCA/3 and KCA/3/JWL/1 which resulted in multiple copies of the content of Sergeant Hill's phone. On 22 January 2020, the original exhibits and examination reports in relation to the Complainant's device were returned to the IOPC but the MPS retained a copy of the forensic extraction in case further work should be required. Mr. Lee received the product of the download on 22 January 2020 but states that he did not review any of the material received.

viii. Soon afterwards an application was issued by Sergeant Hill to the Crown Court under section 59 of PACE. This succeeded before His Honour Judge Lickley KC in a reserved ruling in which he was strongly critical of the IOPC, having heard evidence on disputed matters. He made findings of fact in relation to matters within his jurisdiction. So far as material, we accept his findings about the matters which were necessary for his decision, which concerned the seizure and retention of the mobile phone and not the obtaining of communications data which was a preparatory step to that seizure. At paragraph 69 he made a finding about the RIPA application for communications data nonetheless, to which we will return. That judgment is annexed to this ruling as Annex A, and we will not repeat its content here. We have not heard evidence, and no party has suggested that his main findings were wrong, except in one respect. Further evidence before the Tribunal shows that there is an error in paragraph 31 of that judgment which says that on 3 July 2019 Mr. Lee served a section 49 RIPA 2000 notice on DS Hill requiring disclosure of the PIN for his phone. In fact, there never was a section 49 notice. The 3 July 2019 document was a letter which asked for voluntary disclosure of the PIN and added:-

> "Please be aware that if you do not disclose the relevant information to access your phone, I may seek a disclosure notice under s.49 of the Regulation of Investigator [sic] Powers Act 2000 (RIPA) requiring the material in question to be made intelligible and accessible to me. As I am sure you are aware, failure to comply with a disclosure notice to provide the material in an intelligible form by supply keys (passwords, PINs etc) is a chargeable offence."

ix. In fact, the IOPC was advised that other methods should be tried before any section 49 notice was issued and as we have said those other methods succeeded. No such notice was ever given, nor could one ever have been lawfully issued because section 49 only allows a notice to be given where the phone has been lawfully seized. Accordingly the jurisdiction in section 65(8)(e) of RIPA is not engaged.

5. Whether the handset download claim is within our jurisdiction depends on whether the handset was part of a telecommunications system. If so, access to it was governed by the

Investigatory Powers Act 2016 ("the IPA 2016") and this Tribunal has jurisdiction to deal with the claim. Sergeant Hill contends that his handset was part of the public telecommunications system which had supplied his SIM card to enable him to connect to its network. The MPS and IOPC submit that it was not. The Home Office has filed submissions supporting Mr. Hill's position and we have received helpful submissions from Counsel to the Tribunal (CTT) which tend to the same conclusion. It is common ground that the interference with the handset by the MPS was unlawful. It was, however, done in good faith by the MPS at the behest of the IOPC which wrongly assured MPS that it had lawful authority under section 19 of PACE to request its assistance. The act of downloading the content of the phone was done by staff who were entitled to rely on this assurance and are without fault. The MPS corporately will have known that it had not referred Sergeant Hill for investigation but it is not clear from the evidence that anyone with that knowledge was aware of the request to extract data from his phone. It is thus not established that any individual fault lies with the MPS for this extraction. The issues for us on this claim are:-

a. Is it within our jurisdiction; and, if so,

b. What is the appropriate remedy.

6. Sergeant Hill makes a number of complaints about the MPS and the IOPC which are not within our jurisdiction. An example is this:-

> "On the 9 July 2019 Commander Paul Brogden of the MPS (as a result of the IOPC feedback from the 19 June 2019) placed me on restrictions that I assert breached my Article 8 Human Rights."

7. We do not intend to list all the complaints which are out of scope. We have identified those which are in scope, and will deal only with them and the facts necessary to decide both the extent of liability and remedy.

8. The phone download claim is based on the submission that the extraction of data from the mobile phone required a warrant or other lawful authority because it was interception as defined in IPA 2016. The result of that, if made out, would be that the conduct complained of took place within challengeable circumstances (within the meaning of section 65(7) of RIPA (see section 65(8)(a)), and the Tribunal is the appropriate forum for this complaint (see section 65(4) of RIPA). The Tribunal is the only appropriate tribunal for the purposes

of section 7 of the HRA 1998 (section 65(2)(a), section 65(3)(d) and section 65(5)(a) and (czd)) in respect of the ensuing human rights claim.

The communications data claim: further detail

9. Much of the factual background is set out in Judge Lickley KC's judgment at Annex A. The chronology to which he refers is not attached to this judgment, but it is incorporated in the chronology which is Annex B. We can therefore extract in summary the facts most material to the grant of the authorisation for the communications data. The purpose of the application was to check that the handset in use in May 2018 was still in use in March 2019. This was achieved by securing communications data which showed the IMEI number of the handset in use at the time of communications at those times. The IMEI number could not be obtained separately, and thus all the communications data was secured from the service provider. The IOPC said (and there is no reason to doubt this) that the data was actually used only for the purpose of confirming that the IMEI number (and thus the handset in use) had remained the same.

10. The phone was to be recovered and examined after this check had been carried out to ensure it was the right phone. This would govern the way in which it was done and, in some ways, reduce intrusion. To secure a mobile phone handset which was still in use would often only require a request to or seizure from the individual who habitually carries it. Recovery of an old handset might require a search of the home of the person, or might be judged so speculative that it would not be attempted.

11. The relevant facts for this part of the claim are set out in the Annex B chronology and begin with the meeting on 22 March 2019. The IOPC decided that it would investigate Sergeant Hill by seizing his phone because it concluded that he had sent the video footage to Officer B "for no apparent policing purpose". This seizure was not then open to it in law because of the lack of a referral of Sergeant Hill by the MPS for the reasons set out by Judge Lickley KC. Kieran Casserley was tasked with making the preparatory application for communications data. The draft he produced went through various hands before being approved by Mr. Benbow in the terms set out at [4(a)] above. No severity assessment had been carried out by the IOPC by that stage of the allegations against Sergeant Hill. This is part of the normal process following a referral, but had not taken place in this case because, no doubt, there had been no referral. Therefore, an intrusive investigative step was authorised by the IOPC designated person before the strength and gravity of the complaint

had been assessed. Judge Lickley's comments on this were very well founded and accurate. It was alarmingly cavalier.

12. The result of this failure was that the application for communications data under section 22 of RIPA was inadequate. The information which informed the severity assessment carried out on 17 May 2019 by Mr. Lee was all available to the IOPC at the time when the section 22 application was drafted and authorised. Mr. Lee later decided that the investigation should only relate to potential data protection offences and not to the more serious offences of perverting the course of justice or misconduct in public office. The decision was recorded in 'Policy Decision 78' in the following terms:

> "There were initially concerns regarding [Sergeant Hill's] prior involvement in the referral process and his status within Op Irwin. However, the evidence currently available to the IOPC does not suggest the sending of the dashcam footage is related to any wider attempt by [Sergeant Hill] to undermine a local investigation. At the point by which [Sergeant Hill] sends the dashcam footage to Officer B, officers had already provided their statements. Additionally, the evidence shows [Sergeant Hill] only sending the footage to Officer B, rather than all the officers involved in the incident – as such it does not appear to be a deliberate attempt by [Sergeant Hill] to provide information to the officers regarding the investigation. Although [Sergeant Hill] would be aware at the time when he sent the footage that there was an active investigation/potential for an IOPC independent investigation, the threshold for [Perverting the Course of Justice] is not met by this act alone"

13. The material which led Mr. Lee to conclude that Sergeant Hill should not be investigated for the offences which had been the basis of the authorisation of the communications data request was not disclosed to Mr. Benbow. He was not told that the video footage was only sent to one officer, who was the officer who had taken it on his own device. That officer was not responsible for driving his car into the person who was injured. He was not told that all relevant officers had made their statements before the video footage was disclosed to Officer B.

14. Moreover, Mr. Benbow's authorisation is specifically tailored to the seriousness of the offences under investigation. If he had been told that the evidence was not such as to warrant investigation for those offences the outcome would have been different. If he had been told that it would be unlawful for the IOPC to investigate them using PACE powers because there had been no MPS referral of Sergeant Hill's case, this also would have led

him to refuse to authorise the application. Indeed, if the decision makers present at the meeting on the 22 March had properly informed themselves about the case before deciding to apply for communications data, the application would not, or at least should not, have been made. The IOPC submits that this application was not rendered unlawful by the absence of a referral because no police powers were involved in its being made. This misses the point that the IOPC is a creature of statute and investigates matters within the framework of the Police Reform Act 2002. It is not necessary to decide whether such an application must always be unlawful if there is no properly constituted investigation in being at the time when it is made. We do however find it hard to envisage any circumstances where a lawful application could be made outside a lawfully constituted investigation. Certainly, there is nothing in the facts of this case which would justify such conduct. Our decision on this issue is based on the failures in the application to disclose relevant material to the designated person, as we shall explain. He was not told that the proposed seizure of the phone, to which the application he authorised was merely ancillary, was going to be unlawful.

15. Before it could be authorised, the designated person had to decide that the obtaining of the communications data was necessary for the investigation of serious crime. The part of the application dealing with necessity said only this:-

> "The phones of three officers were seized in a related investigation. These phones were forensically downloaded and the WhatsApp messages extracted. A contact was identified as Damian Hill from the context of messages, this contact was saved as "Damo" in the address book of all phones, with the phone number "447718912791". Communications sent from this number on 7 July 2018 were identified. The communications on this date included a video, created by filming a screen of a Metropolitan Police Service computer which was playing a video of a police incident where a male was hit by a covert police vehicle. This incident took place on 15 May 2018.
>
> "This video was sent, by the above phone number, using WhatsApp to the personal phone of [Officer B], who was involved in that incident, and is under criminal investigation by the IOPC as a result of that incident and a statement he produced about it. DI Hill was aware of the IOPC investigation at the time that he sent the video. The source of this video is currently unknown, it may have been recorded on

DI Hill's phone or sent to him by someone else. The video was recorded between 15 May 2018, and 7 July 2018 but the specific date is unknown.

"The offences being considered are potentially attempting to pervert the course of justice and/or that the officer may have misconducted himself in a public office by sharing footage of an incident for which an officer was under investigation with that officer. The IOPC is planning to seize the phone used to send the video. By accessing call data which includes the IMEI number associated with the phone number, we will be able to establish what handset DI Hill was using between the 14 May and 7 July 2018 and to check if DI Hill is still using the same handset. This will allow us to plan accordingly for that seizure."

16. This application did not, therefore, disclose the following pieces of information all of which were within the knowledge of the IOPC, or easily capable of being discovered by them:-

    a. That Sergeant Hill was the officer in charge of the investigation into the conduct of the drug dealer who had been injured. This investigation resulted in a conviction for dealing in class A drugs. The footage was relevant to his investigation because it showed that the dealer was holding the bag before he was knocked into the area of a house. His claim that he landed near the bag which had got there by some other means was, therefore, false. Sergeant Hill did recover some stills which were part of the file he prepared for the CPS which showed this. He did have a policing purpose for having and processing the footage, although the policing purpose of transmitting it to Officer B is far less obvious.

    b. That Sergeant Hill was not aware of the IOPC investigation when he made and transmitted the footage on 7 June 2018. The IOPC did not decide to conduct its own independent investigation until 6 July 2018, see chronology at Annex B.

    c. The date inserted into the application as the date when the footage was transmitted, 7 July 2018, was false. It suggested that Sergeant Hill could have been aware of the IOPC investigation when he made and transmitted the footage. If the true date of 7 June 2018 had been inserted this claim would have been seen to be untrue by anyone who knew the actual chronology. Given the number of hands through which this document went in draft over the course of a week, see chronology, this is a very surprising error. The IOPC accepts that it renders the obtaining of

communications data between 7 June and 7 July disproportionate and unlawful. However, the falsification of a key factual claim (that Sergeant Hill knew of the IOPC investigation when he transmitted the footage) has consequences beyond that. Judge Lickley KC took a charitable view of the "error". He said:-

> "69. The RIPA application was clumsy and not thought through. I am not satisfied it was drafted to mislead. It does however show laxness, a lack of attention to detail and a failure to apply the necessary care needed when drafting such a document."

As we say at 4(b)(viii) above, this finding was not essential to his decision and as we have just said, it could be regarded as charitable. When associated with another convenient dating "error" on what Judge Lickley called "the criminal letter", a pattern emerges. In that case a completely false date was inserted which would suggest that a referral had been made on a particular date when it had not been made at all at any time prior to the 19 June 2019 when Sergeant Hill's phone was unlawfully seized. We cannot find that these were innocent errors, but neither do we find that there was deliberate dishonesty. We have not heard the witnesses and are not in a position to make findings against them fairly. We therefore leave open the question of whether the fault in relation to these two documents was careless or dishonest. That this level of carelessness, if that is what it was, amounts to serious fault, at least for our purposes, is beyond doubt. This is relevant, for our purposes, only to remedy.

d. At the date of transmission to Officer B, 7 June 2018, that officer was not under criminal investigation by the IOPC "as a result of that incident and a statement he produced about it", and Sergeant Hill was not aware that he was. In fact, Officer B was the driver of a vehicle which was not the one which caused injury to the drug dealer. As at 7 June, the IOPC had decided that the investigation into the incident should be conducted by the DPS of the MPS. It was not until after the IOPC independent investigation was established on 6 July 2018 and had been running for some time that it was decided that there was an indication that three officers (including Officer B) may have colluded about their statements, see the statement of Steven Foxley dated 26 January 2021. Notices were not served on the three officers under the Regulations until 13 September 2018.

e. By the time of the transmission to Officer B, not only he but other relevant officers had made their witness statements.

f. The transmission was made only to Officer B, who was the officer who had caused it to be created, and not to any other officer. In particular, it was not transmitted to the occupants of the vehicle which had caused the injury.

g. The IOPC had not received a referral in respect of Sergeant Hill from the MPS and had not conducted a severity assessment in respect of his alleged conduct. It had no statutory basis for its investigation. Whether or not that meant that the whole conduct of the IOPC at that point was unlawful is not something we have to decide, because the position should have been made clear to the designated person, Mr. Benbow, and was not.

17. In *News Group Newspapers Limited v Commissioner of Police for the Metropolis* (IPT/14/176/H) the Tribunal considered the operation of section 22 of RIPA and held:

> (a) an applicant for authorisation under RIPA has a duty to include in the application the necessary material to enable the authorising officer to be satisfied that the statutory conditions are met, and must also make full and accurate disclosure, including disclosure of anything that might militate against the grant of an authorisation (para. 81, applying *Chatwani* IPT/15/84/88/CH at para. (15);
>
> (b) the lawfulness of the authorisation(s) to obtain communications data must be judged on the basis of the information known to the investigation team at the time when the authorisations were issued (para. 34);
>
> (c) the belief of the designated person as to necessity and proportionality under section 21(1) and (5) must be an honest and reasonable belief (paras. 74 and 89); and
>
> (d) whether or not Convention rights have been breached is an objective question which does not depend on the procedural propriety of the decision-making process or the adequacy of the reasoning of the relevant designated person (para. 65, applying *Belfast City Council v Miss Behavin' Limited* [2007] 1 WLR 1420).

18. The IOPC submissions refer to the fact that Sergeant Hill was under investigation in relation to an offence under section 170 of the Data Protection Act 2018 following the severity assessment, and that this could have been a proper basis for the section 22 application. While it might have been possible to make the application on the basis of this offence pursuant to the serious crime definition in section 25 of RIPA (because it is an offence which involves, as an integral part of it, the sending of a communication, and

perhaps also a breach of a person's privacy) both the necessity and proportionality requirements would have been much more finely balanced given that: (a) the IOPC already had the evidence that Sergeant Hill had sent the footage via Whatsapp and it was not necessary to prove that it was he who filmed it in order to make out an offence under section 170; and (b) an offence under section 170 carries only a non-custodial penalty. Sergeant Hill sets out in his witness statement various other difficulties in proving the data protection offence. We do not need to decide whether he is right about that although if the application had been made on this basis, proper disclosure of the strength of the case in relation to this offence would have been required. The seriousness of the offences which were cited in the section 22 application was a material factor in the granting of the authorisation and the designated person noted the public interest in ensuring that, where a person employed by the state is suspected of such offences, *"every legal method should be used to seek to prove or disprove the allegations"*. We are bound by the decision of the Divisional Court in the search warrant case of *R (Mills) v. Sussex Police* [2014] EWHC 2523 (Admin) in which Elias LJ analysed the authorities and concluded at [49]:-

> "In my judgment, the court should state that the warrant has been unlawfully obtained on the basis that the judge might well have refused to issue it had there been full and proper disclosure."

19. In fact, this passage led the court not only to conclude that the warrant had been unlawfully obtained but also that the right remedy was to quash it.

20. Mr. Benbow is no longer employed by the IOPC and has not given evidence or, so far as we can see, contributed to any document which is before us except the authorisation. We do not therefore know what difference it would have made to him if he had known the things listed at paragraph [17] above. The test, however, is an objective one. We are able to draw our own conclusions about what a decision maker acting reasonably would have done if given all the missing information identified above. We have concluded that any reasonable decision maker given all the information which he should have had would probably have decided to refuse to authorise the section 22 request. It follows that we must conclude that the authorisation might well have been refused if there had been proper disclosure.

21. Accordingly, the communications data claim succeeds against the IOPC. We will deal with remedies in the last section of this ruling.

The handset download claim

22. The issue for this Tribunal is whether it has jurisdiction in respect of the downloading of Sergeant Hill's phone. It is accepted that this was an unlawful act, but the IOPC and MPS submit that this Tribunal does not have jurisdiction to grant a remedy and Sergeant Hill must seek redress through the civil courts. This question has proved extremely difficult. The Tribunal certainly has jurisdiction (in summary of very complex statutory provisions) if the download required a warrant under Part 5 of the Investigatory Powers Act 2016. This depends on whether the download was an "interception" as defined by section 4 of IPA 2016. The download included communications stored on the handset before or after transmission and would amount to an "interception" if the communications stored on the handset were "stored in or by the system" at the time of extraction. This is the effect of s.4(4)(b) of IPA 2016. We did not hear argument based on what the words "or by" might add to the word "in" in that statutory phrase and express no view on that question. The issue we were asked to determine was whether, at the time of the download (which was an interference with the system or "wireless telegraphy apparatus used for making transmissions to or from apparatus that is part of the system", see section 4(3)) the communications were "stored in or by the system" or not.

23. It is not satisfactory that an issue with potentially far reaching implications falls to be decided when there is no substantive dispute. The submissions we received at and before the hearing did not fully address those implications and this caused the Tribunal to seek further assistance by way of written submissions after a first draft of this judgment had been written.

24. The request issued by the Tribunal in September 2022 was as follows:-

> "In the course of preparing the judgment, the Tribunal has decided to seek further written submissions from the Home Office, the complainant and CTT on the point made at paragraphs 24 and 34-36 of the IOPC submissions of 11 March 2022, and also referred to in the MPS written submissions. This concerns the submission that Parliament cannot have intended that the handset should be part of a public telecommunications system because otherwise downloading communications stored on it with no other authority than the consent of the user would be a criminal offence and its product inadmissible. The Tribunal noted that reliance was placed on Chapter 3 of the Police, Crime, Sentencing and Courts Act 2022 but that it had not heard from the Home Office as to what the purpose of these provisions is."

25. Sergeant Hill's original case was as follows:-

> "3. The circumstances of the conduct complained of were such that it would not have been appropriate for it to take place without a warrant under the *Investigatory*

Powers Act 2016 (**IPA 2016**), in particular, a targeted equipment interference warrant under Part 5 (**TEIW**), or at least without proper consideration having been given to whether such authority should be sought.
4. Accordingly, the conduct complained of took place within *challengeable circumstances* (within the meaning of section 65(7) of *RIPA 2000* (section 65(8)(a)), and the Tribunal is the *appropriate forum* for his complaint (section 65(4) of *RIPA 2000*).
5. It is submitted that, in the absence of such authority, the conduct complained of was a violation of his rights under the Convention, in particular Article 8."

26. We have concluded that this handset, an iPhone 7 smartphone, was not part of a telecommunications system for the purposes of the IPA 2016 at the time when it was downloaded by MPS at the request of the IOPC. This is because at that time it was not connected to the public telecommunications system of which it had formerly been a part. We do not need to decide whether that was a public or a private system, although it was almost certainly the former. That means that the basis on which it is suggested by Sergeant Hill that the Tribunal has jurisdiction over this claim is not made out. Warrantry authorising interceptions as defined in section 4 of the IPA 2016 is not required where no such interception is to take place. On our finding that the handset was not part of the telecommunications system at the time of the download, the download was not an interception as defined.

27. In submissions received after the Tribunal's request for further assistance, the possibility was canvassed that the Tribunal may have jurisdiction because the downloading required a Directed Surveillance Authorisation (DSA) as covert surveillance under Part II of RIPA 2000. A further possibility may be that although a TEIW is not required for the download of a disconnected handset, it may nevertheless be available to render such conduct lawful notwithstanding the provisions of the Computer Misuse Act 1990. It might be argued that in conducting the download without having such a warrant or authorisation in place the MPS and IOPC committed an act which was within the jurisdiction of this Tribunal by virtue of section 65(4) and (7)(b) of IPA. No such arguments have been deployed before us in fully reasoned form and we consider that in the facts of this case we do not need to resolve them. This is because this claim is, in truth, a claim about misuse of a PACE power. The IOPC acted as they did because they wrongly thought they were acting lawfully under section 19 of PACE. It would be artificial to determine that they should have given "proper consideration to whether [a TEIW or DSA] should be sought", simply for the purpose of clothing this Tribunal with jurisdiction to give a remedy for an admitted wrong. Their flawed analysis of the PACE powers available to them meant that it never occurred to them that they might need some other authority. This was a mistake, but it was

a mistake about PACE and not about the IPA 2016. It is very clear that this Tribunal has no jurisdiction in relation to PACE and that disputes about that Act are for the courts to resolve. The Tribunal has decided in the case of *KJF v. Surrey Police* (IPT/20/02/C), published on the same day as this decision. that if the seizure of a mobile-phone is lawful under PACE by virtue of a search warrant, no further authorisation is required to recover its stored data. The same answer would follow in the case of a seizure under section 19 of PACE. The issue here, therefore, is whether this download was lawful under PACE or not which is not a matter for us. There is, of course, no dispute about the substance of that issue. We do not know what negotiations there have been between the IOPC and MPS and Sergeant Hill about his various claims, but it appears to us that it would not be a sensible use of public resources for any further litigation to take place about this claim, and we would hope that a settlement can be achieved.

28. Having summarised our conclusions, we will now set out our reasoning in full because of the importance of the question of when and whether a mobile phone is part of a telecommunications system so that acquiring communications from it requires warrantry under IPA 2016.

The proper approach

29. We deal with this issue as a matter of statutory construction of the scheme in Parts 1, 2 and 5 of the IPA 2016 which establish a code for the interception of communications. That code is designed to function alongside other provisions in the IPA 2016 which regulate the obtaining of other kinds of material in other circumstances. Although many of the relevant provisions resemble predecessors in RIPA, and some have their origins as far back as the Interception of Communications Act 1985, we consider that these earlier statutory schemes do not provide any useful assistance in the construction of the IPA 2016. Much of the IPA 2016 scheme is entirely new. Whether a handset is, or is not, part of a telecommunications system for the purposes of conduct regulated by a statute is matter of the construction of that statute.

30. For ease of reference, the principal relevant provisions of the IPA 2016 are set out below. In general, however, the effect of the Act is to render unlawful any interception of communications which is not specifically rendered lawful by the IPA 2016 or some other provision. Part 2 of the Act contains a system of warrants which may render interception lawful. This system is new. It replaces the earlier system established by RIPA. Other provisions of the IPA 2016 deal with TEIWs (Part 5) and Bulk Warrants (Part 6) neither of

which were dealt with at all in RIPA, perhaps because their use had not been avowed by the state when RIPA was enacted. Section 56 contains a provision which excludes the product of interception from evidence, but that is subject to exceptions contained in Schedule 3. Where communications have been lawfully obtained while stored in or by the system then they may be put into evidence, unless that interception occurred under the authority of one of the three kinds of warrant listed in section 15(1) of IPA 2016, in which case they are not admissible. It appears that interception of stored communications may lawfully occur under those provisions (inadmissible in evidence), and under section 44(2) of IPA 2016 or Part 5 of IPA 2016 (admissible in evidence). Section 44(2) deals with interception as a form of surveillance where it takes place with consent of either the sender or the intended recipient of a communication. As we have said we are not concerned with interception as defined in that Act.

31. Because of the widespread use of downloads from mobile phones in evidence in criminal trials it is important to be as clear as possible about the legal basis on which that extraction of data is done. There is some level of uncertainty about this, which is perhaps surprising. In response to our request at [24] above, the Home Office referred us to the Explanatory Notes for the Police, Crime, Sentencing and Courts Act 2022. These summarise the purpose of the new provision contained in section 37 of that Act which allows extraction of information from an electronic device with the consent of a user. The Notes refer to some of the uncertainty which existed, and still exists on respect of conduct before the 2022 Act was brought into force in November 2022. They say this:-

> "49. In June 2020, the Information Commissioner's Office published a report on police practice in England and Wales around the extraction and analysis of data from mobile phones and other electronic communication devices of victims, witnesses and suspects during a criminal investigation. The report identified inconsistencies in the approach taken by police forces to extract digital data and the complex legal framework that governs this practice. It recommended clarifying the lawful basis for data extraction and introducing a code of practice to guide this activity in order to increase consistency and ensure that any data taken is strictly necessary for the purpose of the investigation.
> "50. Chapter 3 of Part 2 introduces a specific legal basis for the extraction of information from complainants', witnesses' and others' digital devices. This will be a non-coercive power based on the agreement of the routine user of the device. It will be applicable to specified law enforcement and regulatory agencies, such as the police, who extract information to support investigations or to protect vulnerable people from harm. This will provide a nationally consistent legal basis for the purpose of preventing, detecting, investigating or prosecuting criminal offences and for safeguarding and preventing serious harm."

32. Parliament does not appear to have dealt with the provisions of section 44(2) of IPA 2016 or to have explained how the two different statutory schemes operate together. We do not have to decide that. The purpose of referring to the new Act is to explain the difficult context in which our decision as to jurisdiction arises.

The jurisdictional question: was the handset part of the system?

33. Mobile phone extraction is commonly done under powers conferred by PACE, and in that case the exclusionary rule in section 56 of IPA 2016 does not apply because of section 6(1)(c)(ii) of and paragraph 2(1)(a) of Schedule 3 to IPA 2016.
34. The clear statutory purpose of the regime is to create a system whereby:-

    a. All intercept activity is to be controlled by a legal system which ensures that its use conforms to law, and is conducted under independent judicial oversight. This is designed to protect the rights of those affected by it, while allowing the security services, and other agencies who may engage in intercept activity, effective tools for intelligence gathering and the acquisition of relevant evidence in investigations.

    b. The product of interception in the commonly understood sense of phone tapping or monitoring messages in real time while the conversation or chat is ongoing is excluded from use in evidence. This is a policy choice by Parliament to preserve the value of the use of the technique for intelligence purposes. It is a clear and striking exception to the common law rule of evidence that in criminal proceedings relevant evidence is admissible, subject to some exclusionary rules and an overarching discretion to exclude evidence under section 78 of PACE. In our judgment, this exclusionary rule should be confined to the clear words of the Act. It does not exist for the protection of anyone or anything other than the value of intercept as an intelligence gathering tool for the security services and others who are entitled to use it. It provides an obvious windfall benefit to those who benefit from the exclusion of probative evidence of criminality, but that is not its purpose. This policy can be found set out in many public documents. We will cite only one, the document which gave rise to RIPA. This was *Interception of Communications in the United Kingdom, A Consultation Paper* Cm 4368, June 1999, which said at 8.3:-

> "The main counter-argument, for retention of the prohibition on evidential use, is that exposure of interception capabilities will educate criminals and

terrorists who will then use greater counter interception measures than they presently do. This would mean that any advantage gained by repeal would be short lived and would make interception operations more difficult in the longer term."

c. The same policy argument does not, it would seem, apply to interception by the recovery of stored messages from the telecommunications system. Provided their acquisition brings them within Schedule 3 to the Act, they may be deployed in evidence.

The Investigatory Powers Act 2016

35. We will set out some of the key provisions of the IPA 2016 with parts which are not relevant to the present issue omitted. This case concerns an extraction of data from a handset which was admittedly unlawful, and which was carried out when the handset had been seized and was in "airplane mode", and incapable of transmitting or receiving communications. The SIM card was removed and the phone switched on in a "Faraday environment". That was all designed to prevent it from communicating by any means. A communication whose content was made available by the extraction would commonly be one which was stored on the handset after transmission. If the handset was part of the system the Tribunal has jurisdiction in respect of the unlawful extraction of all such communications. We do not know what was recovered from the phone, because it was never examined. We are sure that some of the recovered material comprised communications stored on the handset after transmission to or from it by means of a public telecommunications system. That is what might engage the interception regime, and the jurisdiction of this Tribunal. We are not concerned with what may lawfully have been done if a TEIW had been obtained under Part 5 of IPA 2016 because no such warrant was obtained. We do note that a Part 5 warrant could permit the obtaining of stored communications and their use in evidence, which provides some support for the proposition that the policy of IPA 2016 is that this technique for extraction of material does not require the protection from public view which is accorded to the interception of communications in the course of transmission. Otherwise, nothing in this decision has any relevance to Part 5.

36. **Section 3** deals with unlawful intercepts:-

3 Offence of unlawful interception

(1) A person commits an offence if—

(a) the person intentionally intercepts a communication in the course of its transmission by means of—

(i) a public telecommunication system,

(ii) a private telecommunication system, or

(iii) a public postal service,

(b) the interception is carried out in the United Kingdom, and

(c) the person does not have lawful authority to carry out the interception.

(2) But it is not an offence under subsection (1) for a person to intercept a communication in the course of its transmission by means of a private telecommunication system if the person—

(a) is a person with a right to control the operation or use of the system, or

(b) has the express or implied consent of such a person to carry out the interception.

(3) Sections 4 and 5 contain provision about—

(a) the meaning of "interception",……

.

(4) Section 6 contains provision about when a person has lawful authority to carry out an interception.

(5) For the meaning of the terms used in subsection (1)(a)(i) to (iii), see sections 261 and 262.

37. **Section 4** is an important provision which defines some terms used in section 3. Other relevant terms are defined in section 261. Section 5 deals with interception of broadcasts and is not material. It is because of section 4 that it matters whether the handset is part of the system or not. If so, its extraction involved interfering with it, which would be a "relevant act". The effect of the download was to extract communications which were stored on it, and to make them available. This means that the relevant act was done at a relevant time. At the time of the interference with the handset, the material on the handset

included communications which had been transmitted by the system, and were stored on it. Section 4(4)(b) means that interference with them constitutes interception if the handset where they were stored was part of the system.

4 Definition of "interception" etc.

Interception in relation to telecommunication systems

(1) For the purposes of this Act, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if—

(a) the person does a relevant act in relation to the system, and

(b) the effect of the relevant act is to make any content of the communication available, at a relevant time, to a person who is not the sender or intended recipient of the communication.

For the meaning of "content" in relation to a communication, see section 261(6).

(2) In this section "relevant act", in relation to a telecommunication system, means—

(a) modifying, or interfering with, the system or its operation;

(b) monitoring transmissions made by means of the system;

(c) monitoring transmissions made by wireless telegraphy to or from apparatus that is part of the system.

(3) For the purposes of this section references to modifying a telecommunication system include references to attaching any apparatus to, or otherwise modifying or interfering with—

(a) any part of the system, or

(b) any wireless telegraphy apparatus used for making transmissions to or from apparatus that is part of the system.

(4) In this section "relevant time", in relation to a communication transmitted by means of a telecommunication system, means—

(a) any time while the communication is being transmitted, and

(b) any time when the communication is stored in or by the system (whether before or after its transmission).

(5) For the purposes of this section, the cases in which any content of a communication is to be taken to be made available to a person at a relevant time include any case in which any of the communication is diverted or recorded at a relevant time so as to make any content of the communication available to a person after that time.

(6) In this section "wireless telegraphy" and "wireless telegraphy apparatus" have the same meaning as in the Wireless Telegraphy Act 2006 (see sections 116 and 117 of that Act).

38. **Section 6** deals with the meaning of lawful authority. The MPS believed that they were acting lawfully because powers existed under PACE, as they had been assured by IOPC. This would mean, if true, that section 6(1)(c)(ii) would apply.

6 Definition of "lawful authority"

(1) For the purposes of this Act, a person has lawful authority to carry out an interception if, and only if—

(a) the interception is carried out in accordance with—

(i) a targeted interception warrant or mutual assistance warrant under Chapter 1 of Part 2, or

(ii) a bulk interception warrant under Chapter 1 of Part 6,

(b) the interception is authorised by any of sections 44 to 52, or

(c) in the case of a communication stored in or by a telecommunication system, the interception—

(i) is carried out in accordance with a targeted equipment interference warrant under Part 5 or a bulk equipment interference warrant under Chapter 3 of Part 6,

(ii) 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, or

(iii) is carried out in accordance with a court order made for that purpose.

(2) Conduct which has lawful authority for the purposes of this Act by virtue of subsection (1)(a) or (b) is to be treated as lawful for all other purposes.

(3) Any other conduct which—

(a) is carried out in accordance with a warrant under Chapter 1 of Part 2 or a bulk interception warrant, or

(b) is authorised by any of sections 44 to 52,

is to be treated as lawful for all purposes.

39. It is unnecessary to set out **section 56** in full, but in part it provides:-

56 Exclusion of matters from legal proceedings etc.

(1) No evidence may be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings or Inquiries Act proceedings which (in any manner)—

(a) discloses, in circumstances from which its origin in interception-related conduct may be inferred—

(i) any content of an intercepted communication, or

(ii) any secondary data obtained from a communication, or

(b) tends to suggest that any interception-related conduct has or may have occurred or may be going to occur.

This is subject to Schedule 3 (exceptions).

40. **Schedule 3** contains the exceptions and only paragraph 2 is relevant for present purposes, because it provides that the exercise of a power rendered lawful by section 6(1)(c) does not result in the product being inadmissible in legal proceedings:-

Disclosures of lawfully intercepted communications

2 (1) Section 56(1)(a) does not prohibit the disclosure of any content of a communication, or any secondary data obtained from a communication, if the interception of that communication was lawful by virtue of any of the following provisions—

(a) sections 6(1)(c) and 44 to 52;

(b) sections 1(5)(c), 3 and 4 of the Regulation of Investigatory Powers Act 2000;

(c) section 1(2)(b) and (3) of the Interception of Communications Act 1985.

(2) Where any disclosure is proposed to be, or has been, made on the grounds that it is authorised by sub-paragraph (1), section 56(1) does not prohibit the doing of anything in, or for the purposes of, so much of any proceedings as relates to the question whether that disclosure is or was so authorised.

41. **Section 261** provides some "Telecommunications Definitions" for the purposes of the whole Act. In part, it provides that a telecommunications system includes any apparatus comprised in it, see sub-section (13). That might be regarded as a statement of the obvious, because if apparatus is *comprised in* a system it might be thought that the statement that the system *included it* is a different way of saying the same thing. To put it another way, if the Act had said "a system includes what it includes" it would not have borne a radically different meaning as a matter of English language. It is probably best to treat this parenthesis as a recognition by Parliament that apparatus may be included as part of a system even though it is not physically connected to it. In this way it reinforces the definition of "apparatus" in section 263(1).

Communication

(2) "Communication", in relation to a telecommunications operator, telecommunications service or telecommunication system, 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.

……..

Content of a communication

(6) "Content", in relation to a communication and a telecommunications operator, telecommunications service or telecommunication system, means any element of the communication, or any data attached to or logically associated with the communication, which reveals anything of what might reasonably be considered to be the meaning (if any) of the communication, but—

(a) any meaning arising from the fact of the communication or from any data relating to the transmission of the communication is to be disregarded, and

(b) anything which is systems data is not content.

…….

(8) "Public telecommunications service" means any telecommunications service which is offered or provided to the public, or a substantial section of the public, in any one or more parts of the United Kingdom.

(9) "Public telecommunication system" means a telecommunication system located in the United Kingdom—

(a) by means of which any public telecommunications service is provided, or

(b) which consists of parts of any other telecommunication system by means of which any such service is provided.

(10) "Telecommunications operator" means a person who—

(a) offers or provides a telecommunications service to persons in the United Kingdom, or

(b) controls or provides a telecommunication system which is (wholly or partly)—

(i)in the United Kingdom, or

(ii)controlled from the United Kingdom.

(11) "Telecommunications service" means any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service).

(12) For the purposes of subsection (11), the cases in which a service is to be taken to consist in the provision of access to, and of facilities for making use of, a telecommunication system include any case where a service consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system.

(13) "Telecommunication system" means a system (including the apparatus comprised in it) that exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electromagnetic energy.

(14) "Private telecommunication system" means any telecommunication system which—

(a) is not a public telecommunication system,

(b) is attached, directly or indirectly, to a public telecommunication system (whether or not for the purposes of the communication in question), and

(c) includes apparatus which is both located in the United Kingdom and used (with or without other apparatus) for making the attachment to that public telecommunication system.

42. **Section 263** contains general definitions, only one of which it is necessary to set out:-

263 General definitions

(1) In this Act—

"apparatus" includes any equipment, machinery or device (whether physical or logical) and any wire or cable,

Discussion

43. We now turn to the reasons for our decision on the issue as to jurisdiction which the parties dealt with at the hearing. Was the mobile phone handset (or at least the part where communications were stored) part of the telecommunications system at the time of the download? As we have indicated, we have decided that the answer is No.

44. We consider that the right approach to this case is to decide whether Sergeant Hill's handset was apparatus which formed part of the telecommunications system, or whether it was "wireless telegraphy apparatus used for making transmissions to or from apparatus that is part of the system" by reference to the IPA 2016. That dichotomy is created by section 4(3) of the Act, and is operative for our purposes because of section 4(4)(b). Section 4(4)(b) extends the definition of interception to cover messages which are stored in or by the system. The equivalent RIPA provisions are not identical, and section 2(7) of RIPA (which extended the definition of "in the course of transmission" so that stored messages were captured) is not replicated in the IPA 2016. A broadly similar *effect* may be achieved by section 4(5) which does not depend on the concept of storage, but which extends the meaning of "making content available to a person" to cover the situation formerly dealt with by section 2(7) of RIPA. In the IPA 2016 there is no extended definition of "stored

on the system". The statutory provisions appear to be intended to have a similar effect, but they achieve that effect by a different route.

45. In this case the natural meaning of the words used does not assist in answering the question. In plain language a mobile phone handset could rationally be described as part of the telecommunications system to which the user connects via the SIM card. It could equally well be described as "wireless telegraphy apparatus used for making transmissions to or from apparatus that is part of the system". Which definition is chosen determines whether extracting the content of communications stored on the handset constitutes interception of communications or not. In our judgment the answer to the question comes from a close analysis of the statute within which the relevant terms are used to see which construction best serves the statutory purpose and fits best into the highly complex statutory scheme created by the IPA 2016. It is almost so obvious that it does not need to be said that this process is unlikely to be assisted by analysis of the previous statutory schemes which the IPA 2016 replaced. That analysis is itself a highly complex task and, if it is not relevant, one which serves only to confuse.

46. On this approach it is unnecessary to consider authority, because there is no relevant authority on the IPA 2016. The provision just identified, section 4(5) of IPA 2016, appears to have been designed to replace the effect of section 2(7) of RIPA as interpreted by the Court of Appeal Criminal Division in *R v. Coulson* [2013] EWCA Crim 1026. A different statutory device is used with a similar result. One purpose of this seems to have been to create a new code which avoids the need to consider decisions under previous legislation. This is not unprecedented in the legislative history of the three statutory schemes which have been created by Parliament (the Interception of Communications Act 1985, RIPA and the IPA 2016). Changes have often been driven by decisions of the UK or Strasbourg courts. We are grateful to the immense industry of those who have compiled our bundle of authorities which runs to 727 pages. We have considered all those materials, but do not find any one of them of decisive value in answering the question before us.

47. We should say something about the decision of the Court of Appeal Criminal Division in *R. v. A, B, D and C* [2021] EWCA Crim 128. In that case the Court of Appeal upheld a judge's finding of fact about messages intercepted by French law enforcement agencies and made available to UK law enforcement agencies for use as evidence in criminal investigations and proceedings. The judge had found that these were extracted while stored in the handsets and not while being transmitted. This meant that either they were

admissible because the handset was not part of the system and so there was no interception, or because they were extracted while stored on the handset in the system under warrantry which rendered the product lawful. In *A, B, D & C* it was not necessary to decide whether the handset of a mobile phone was part of the telecommunications system. At paragraph 18, the Lord Chief Justice, giving the judgment of the court, said this:-

> "We have reservations about whether handsets do ordinarily form part of the "system", given the nature of modern mobile phones which have many functions. In particular, section 4(3) extends the definition of an act of interception to include interference with any wireless telegraphy apparatus used for making transmissions to or from apparatus that is part of the system. Before us it was suggested that this would include mobile phone handsets. This extension would be unnecessary if the wireless telegraphy apparatus is part of the system. The extension of "relevant act" so that it extends to interference with handsets may be contrasted with the lack of any such extension in relation to the definition of the system for the purposes of considering the "relevant time". It would suggest that unless specifically provided otherwise, handsets are not part of "the system". Section 4(3) would not be necessary at all if the agreed position of the parties before us is right. This issue was not argued by the parties, and we will approach this appeal on the agreed basis that in respect of the EncroChat system the handsets are part of "the system". Whether that is right or not in general, it is possible to see how it could be true of this particular system in view of the findings of the judge about its nature, in paragraph 4 of his ruling set out above at our para 11. We do not decide the point, but proceed on the basis of the agreement between the parties reached in respect of this particular system."

48. It is not surprising that the court expressed reservations about accepting an agreement as to the law when it had not heard argument about it. Courts, not parties, construe statutes authoritatively, and courts are reluctant to reach decisions without argument on issues which may have unforeseen ramifications. The reasons why it entertains those reservations are obviously not intended to be binding conclusions on the point. In our judgment, the purpose of this passage was simply to highlight for future courts that the agreement reached between the parties does not have the force of law, as it would if it had been endorsed by the court.

49. The decision in *A, B, D & C* is authoritative and binding in its clear endorsement of the approach described above at [45]-[46] as the right approach to determination of issues of statutory construction arising under the IPA 2016.

50. We begin the analysis by making the obvious point that the IPA 2016 is concerned with the interception of *communications which have been or are being transmitted*. This is the effect of section 4(1) and (4). Section 4(4)(b) then extends the scope of "intercept", as a term used in the statute, to include communications stored in or by the system whether before or after transmission. The "relevant time" in respect of such communications is either while they are being transmitted or while they are stored in that way.

51. This is the answer to one concern expressed by the Court of Appeal in *A, B, D & C.* The court referred to the "many functions" of a modern mobile phone handset. This Part of the Act has nothing to say about any function which is not part of the process by which communications are transmitted. As an example, a mobile phone often has a camera and a storage area where photographs are held. Taking a photograph and storing it (without transmitting it) is not an activity which involves a "communication". Such photographs can be extracted without any engagement of the powers to intercept communications, because they are not communications. There are other protections against unlawful access to computers, and the IPA 2016 created a new scheme of warrantry to cover that situation. When the user sends a photograph (or video footage) by a communication system (in the present case using WhatsApp) a communication is created and transmitted, and the interception regime is engaged in respect of that process. That photograph having by then become a "communication", making its content available to a person other than the intended recipient will be an act of interception, if it is stored on the handset and if the handset is part of the telecommunications system.

52. The question, therefore, is not whether the whole operation of the mobile phone handset is part of a telecommunications system, but whether the function which operates to create, transmit, receive, and store communications is part of a telecommunications system.

53. In our judgment, section 4(4) of the IPA 2016 is at the heart of this question. The act of interception is a result of a person doing a relevant act at a relevant time. Section 4(3), which involves the dichotomy between, on the one hand, part of the system and, on the other, "wireless telegraphy apparatus used for making transmissions to or from apparatus that is part of the system" relates to the relevant act and not the relevant time. It contemplates that there may be apparatus which is part of the system, and other apparatus

which is not. It simply provides that it will be a relevant act to interfere with either type of apparatus if the effect of the interference is to make any content of the communication available, at a relevant time, to a person who is not the sender or intended recipient of the communication, see section 4(1). Section 4(3) has nothing to say about what the relevant time is, which is the subject of section 4(4).

54. We have helpful technical material before us from experts and from Ofcom. Ofcom responded to a request for assistance from the Tribunal for assistance about how telecommunications systems work, and we are extremely grateful. This case concerns a standard smartphone, normally connected to a telecommunications system by a SIM card supplied by the operator of that system or, sometimes, by another operator licensed by that operator to supply services using its system. The following passage from Ofcom's Note explains matters:-

> 10. There are currently four Mobile Network Operators (MNOs) in the UK (Vodafone, 02/Telefonica, EE and Three) which operate the mobile phone network used by the general public. They operate their own networks of cell towers in the UK. While some MNOs share the use of some masts, cellular coverage varies between MNOs where masts are installed separately covering differing geographic areas, and also depending on the physical characteristics of the frequency band over which that MNO operates.
>
> 11. There are also a number of Mobile Virtual Network Operators ("MVNOs") who contract with the MNOs for the resale of mobile services (e.g. Virgin Mobile, Tesco). These MVNOs do not have their own cell towers or base stations, and use the cellular network of the MNOs from whom they have bought capacity in order to sell mobile phone services as a "white label" product. This means that although the customer has a contract with an MVNO, they are in effect using the "parent" MNO's cellular network. Some MVNOs do have some physical equipment such as elements of the core network or transmission network, which connect to the mobile phone and landline networks (e.g. Virgin Mobile). MNOs and MVNOs offer a large number of different mobile phone call and data packages to the public. These include monthly contracts which include a certain number of minutes, text messages and data on payment of a monthly sum, and pay-as-you-go contracts where the consumer pays in advance for a certain amount of voice calls, text messages or data.

> 12. A mobile phone contains a few key pieces of technology which enable a user to make and receive calls, send and receive text messages and access the internet. These include a transmitter and receiver, and a SIM card which contains the user's ID and authentication keys. SIM cards are activated on the network by the MNOs and MVNOs when customers conclude contracts. They link the user, their phone number, and their home network. Each SIM card has a unique value known as the "IMSI" which identifies it to its MNO (or "parent" MNO if the user has a contract with an MVNO). When the handset is switched on, it sends a signal to the closest mobile phone cell tower operated by its MNO or "parent" MNO. The handset's SIM card is issued an authentication challenge by the MNO. The SIM then uses its authentication key and a specific algorithm to generate a response which is sent back to the MNO. The MNO in turn verifies that this response matches the response they were expecting from their authentication database. Only after successful authentication can the handset start making and receiving calls, sending and receiving text messages and connect to the internet or other data services.

55. Where the plain words of the provisions do not provide an obvious answer to the classification of a mobile phone handset for the purposes of the IPA 2016, the Explanatory Notes published when the Bill which became the IPA 2016 was introduced into Parliament may be of value. It is clearly established that Explanatory Notes are a legitimate aid to construction in that they may illustrate the context of a statute and the mischief at which it is aimed. *Bennion, Bailey and Norbury on Statutory Interpretation* 8th Edition paragraph 24.14 sets out the proper approach, and we will follow it. We would add that this is an area where Explanatory Notes are likely to be particularly helpful because the legislation is very complex and will have been considered by many agencies of the UK Government before being introduced. It is reasonable to assume that the Notes will have been the subject of careful consultation with those agencies where a high level of expertise about investigatory powers resides. Having said that, however, it is of course true that the task of the Tribunal is to construe the statute and not the Explanatory Notes. If, as is submitted by the IOPC, the Explanatory Notes do not accurately describe what Parliament enacted, then the words used by Parliament prevail. That much is obvious. However, here the position is nuanced and this cannot be firmly asserted. That is why recourse to the Notes is valuable.

56. The Explanatory Notes contain these paragraphs, under the heading "Section 4: Definition of "interception" etc.":-

39. This section defines interception and sets out when interception is regarded as taking place in the United Kingdom.

40. Subsections (1) to (5) set out what constitutes intercepting a communication in the course of its transmission by a telecommunications system. There are three elements. Firstly, the person must perform a "relevant act", which is defined in subsection (2) and includes modifying or interfering with the system. Secondly, the consequence of the relevant act must be to make the content of the communication available to a person who is not the sender or intended recipient. Thirdly, the content must be made available at a "relevant time", which means a time while the communication is being transmitted or any time when the communication is stored in or by the system.

41. The definition of a relevant time makes it clear that interception includes obtaining stored communications, such as messages stored on phones, tablets and other individual devices whether before or after they are sent.

Example: An email which has been sent and is stored on an email server or a voicemail message which has been stored on a telecommunications system to be retrieved later. This would also include an email which had not been sent by an individual but was stored on a server (e.g. a draft email).

57. The IOPC submits that paragraph 41

> "…..does not accurately reflect what Parliament enacted: the Act does not refer to communications stored "on phones, tablets and other individual devices". If this had been Parliament's intention it would have said so, or it would have referred, as it does elsewhere, to "apparatus". The Act refers only to communications "stored in or by the system". The Explanatory Note to s.261 does not refer to individual devices as being part of the "system". There is no justification in the Act for the assumption that "phones, tablets and other individual devices" will be "the system" or even "part of the system", particularly when they are offline and unable to communicate or attach to a "system"."

58. Counsel to the Tribunal invites the Tribunal to note that paragraph 41 of the Explanatory Notes was expressly cited by a Home Office Minister during Parliamentary debates in 2019 relating to a proposed (and subsequently enacted) amendment to section 52 of the

IPA 2016. This was during the debate on what became the Crime (Overseas Production Orders) Act 2019. This is admissible because a situation where a statute requires the court to determine whether a mobile phone handset is part of a telecommunications system, but does not by clear words provide the answer, involves the kind of ambiguity contemplated in *Pepper v. Hart* [1993] AC 593. The statement relied on is a statement of a Minister promoting a Bill. The Bill concerned is not the Act which the Tribunal is required to construe, but a Bill which amended that Act. It amended section 52 of the IPA 2016. The Minister of State at the Home Office explained the existing meaning of that provision as follows:-

> "As I said on Report, Section 52 can authorise obtaining stored as well as intercepted communications. Section 52 should be read alongside Section 4 of the IP Act, which outlines the definition of "interception" and related terms. According to that section, "interception" refers to the interception of a communication, "in the course of its transmission by means of a public telecommunication system or a public postal service". A person intercepts a communication in the course of its transmission if the effect is to access any content of the communication "at a relevant time". It is the meaning of "relevant time" that is significant. It can mean a time when the communication is transmitted but it can also mean, as Section 4(4) of the IP Act says, "any time when the communication is stored in or by the system (whether before or after its transmission)".It is clear that where, as in Section 52, the IP Act refers to the "interception of a communication in the course of its transmission" this includes accessing stored communications from the relevant telecommunications system, such as messages stored on phones, tablets or other devices, whether before or after they are sent. By way of an example, this would include an email that has been sent and is stored on an email server or a voicemail message that has been stored on a telecommunications system to be retrieved later. It would also include an unsent, draft email that is stored on a server. I hope that this explains it adequately to the noble Baroness but I would also direct her to the Explanatory Notes for Section 4 of the Investigatory Powers Act. To briefly sum up, I hope that I have made it clear that Section 52 of the IPA not only covers material intercepted in the course of transmission but can authorise obtaining stored communications as well."

59. We consider that paragraph 41 of the Explanatory Notes is not a sufficient basis on which to answer the question. The passage is not very clear and does not explain why the "phones, tablets or other devices" are part of the system, rather than apparatus used for connecting to the system. In other words although they appear to provide an answer to the question there is no explanation or justification of how that answer is derived from the statute. We give the Note some weight in identifying the mischief at which the provision is aimed, and rely on it as some support for the proposition that a mobile phone handset is part of the telecommunications system when it is connected to it, and in a position to transmit communications through it.

60. It is perhaps worth noting that the Explanatory Note is unclear or incomplete as an aid to construction in one further respect. The example suggests that a draft email which had not been sent but which was stored on a server would be protected from unlawful interception by section 3 of the IPA 2016 Act. Section 3 protects only "communications". A draft email which has not been sent may or may not be a "communication". We do not need to decide this question and do not do so.

61. Further, we consider that although the clear words of the IPA 2016 do not provide a conclusive answer to the question, they provide a significant steer in the same direction as the Explanatory Note. The key word used is "system". The question is whether the handset, when used in the way described in the Ofcom Note at its paragraph 12, is part of that "system". "Telecommunications system" is defined in section 261(13) of the IPA 2016 which we repeat here for ease of comprehension:-

> "Telecommunication system" means a system (including the apparatus comprised in it) that exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electromagnetic energy.

62. The word "facilitating" in the sense of "making things easier" does not really cover what a telecommunications system does. With such a system, the transmission of communications by means involving the use of electrical or electromagnetic energy is possible. Without one it is not. There are no degrees of ease with which it might happen. The system either works or it does not. If it works, it "facilitates" communication, but in a slightly different sense. The system does not make this transmission easier than it would otherwise be: it *achieves* it. Once it is understood that the word facilitating is to be read in this sense, the answer to our problem becomes a little clearer. What use is a system of the

kind we are considering without handsets? The vast complex of different networks operating together described by Ofcom would not achieve anything for a person wishing to communicate with another if both parties did not have a handset. The rest of the infrastructure would not be "facilitating" communication between them: it would not be happening at all. A system which exists for the purpose of *achieving* the transmission of communications must comprise everything which is necessary for that purpose. The fact that apparatus is not physically connected to it does not mean that it is not part of the system, see the general definition of "apparatus" in section 263(1) at paragraph [44] above. It follows that a part of the system which may be connected to it in this way may also be disconnected from it.

63. A handset converts the voice into "electrical or electromagnetic energy" and transmits it. At the other end, it receives the transmission and converts into voice again. Without that no communication by voice call can take place. The contribution of the handset to the success of the "system" is fundamental.

64. The connection of the handset to the system is through its SIM card, at least in the mode of operation currently under consideration. Other types of system operate with a less close connection between the device and the system which may require different answers in their cases. An example is a laptop which accesses the internet through public wifi, and is able to facilitate voicecalls by Zoom, Teams or some other similar software. The mobile phone network is not involved at all. This is an important point when considering the "redundancy argument" which concerned the Court of Appeal in *R v. A, B, D & C* when considering section 4(3). Section 4(3) is not redundant if the mobile phone handset is part of the system as described in paragraph 12 of the Ofcom Note. There are many other systems now in existence (and no doubt will be further developments during the life of the IPA 2016) where the provision in section 4(3)(b) may be material. We have evidence from Ofcom on this subject which was not before the Court of Appeal and accordingly are less troubled by the argument based on section 4(3).

65. The word "system" is not the same as "network". "Network" is not a word used in IPA 2016 but the expression "telecommunications service" is used. They are not synonymous but may overlap in meaning. A "system" may include a large number of networks, or "services", many of which are not accessed when an individual communication is transmitted. Each MNO has access to the networks of all the other MNOs, and to the landline network, and the system will route the call to the network which enables the

recipient to receive it. The distinction in meaning in section 261 of IPA 2016 between "telecommunications system" and "telecommunications service" confirms that the word "system" connotes a broader concept which may incorporate a number of different "telecommunications services".

66. We therefore conclude that a mobile phone handset when operating in the way described in paragraph 12 of the Ofcom Note is part of the telecommunications system, and that unlawful interception of communications stored on it does fall within the jurisdiction of this Tribunal. However, when it is disconnected from the system and not capable of communicating through it, it is not sensible to describe is as remaining part of the system. Thus, at the point of the download in this case, when it was in airplane mode, without a SIM card and in Faraday conditions, it was not part of the system. For that reason, no intercept was involved because the "relevant act" did not occur at a "relevant time". The communications which were made available by the act of downloading were not, at the time when that occurred, stored in or by the system. They were stored in a handset which had been part of the system, but no longer was. By the time of the download it had been disabled following its seizure to prevent it from making or receiving any further communications to or from the system. This is why the download in the present case did not result in the extraction of communications stored in or by the system. This approach protects "live handsets" which are in use by the user from interception otherwise than as authorised by the IPA warranty regime. Once they have been disabled, they can be lawfully accessed without engaging the IPA regime using other statutory powers, such as section 19 of PACE.

67. This is a clear case, where the download was done by a MPS examiner in forensic conditions designed to isolate the handset from the telecommunications system. We say nothing about other circumstances which may arise where a handset is temporarily not in communication with the system for other reasons. Those cases will have to be considered when they arise.

68. We do not accept the submission that a mobile phone handset is, on its own, a private telecommunications system which becomes attached to a public telecommunications system via its SIM card. There is no hint that Parliament intended that this should be the result and it would have significant consequences which are not catered for in the Act. The Act imposes obligations on the operators of telecommunications systems, see section 261(10)(b), and we are unable to work through the precise consequences of a finding that

every user of a mobile phone is an operator of a private telecommunications system. We are, however, quite confident that Parliament would only bring such a state of affairs into existence after careful thought and by the use of very clear language. The absence of any reference to this suggested consequence of the IPA 2016 in the Explanatory Notes, referred to above, confirms our view that this was not the intention of Parliament.

Conclusion

69. We therefore conclude that Sergeant Hill is entitled to a remedy from this Tribunal in respect of the unlawful obtaining of his communications data further to the authorisation granted by Mr. Benbow on 28 March 2019. That authorisation is now quashed and therefore the conduct carried out under its terms is not "lawful for all purposes" as would otherwise be the result of section 21(2) of RIPA as it was at the material time.

70. We cannot grant a remedy in relation to the unlawful downloading of the data from his mobile phone handset stored on the handset because the Tribunal has no jurisdiction in this respect.

71. We direct that Sergeant Hill should file and serve any submissions and evidence on which he wishes to rely in respect of the remedies which should be granted to him, in addition to the quashing order made at [68] above. This should include the terms of any declaration(s) he seeks. We have his submissions on remedy already but grant the parties an opportunity to finalise their position on remedy in the light of this decision. We will allow 28 days from the date when this decision is sent to his solicitors by the Tribunal staff.

72. The IOPC and MPS should have the opportunity to respond if so advised by submitting any further representations or evidence on which they propose to rely in the light of this decision, in particular in relation to the relevance to the quantification of such compensation as is payable of the serious culpability of the IOPC. Material should be lodged within 21 days of the expiry of the time allowed to Sergeant Hill under paragraph [70] above.

73. The Tribunal will then decide on remedies on the papers without a further hearing.

74. We specify, in accordance with s. 67A(2) of RIPA, that the relevant appellate court is the Court of Appeal in England & Wales.

IN THE CROWN COURT AT THE CENTRAL CRIMINAL COURT

IN THE MATTER OF AN APPLICATION UNDER SECTION 59 OF THE CRIMINAL JUSTICE AND POLICE ACT 2001

AND IN THE MATTER OF

DS Damian Hill **Applicant**

V

Independent Office for Police Conduct **Respondent**

HHJ Nigel Lickley QC

Mr Nicholas Yeo for the Applicant

Mr Andrew Bird for the respondent

This decision is to be read in conjunction with my earlier ruling dated the 3/9/20. As set out in that decision I have now heard the relevant evidence and submissions from counsel. I heard evidence on the 21st, 22nd, 23rd and 24th September 2020 and oral argument on the afternoon of the 9th and 10th December 2020. References to documents in the respondent's bundle are prefixed [R].

History and background

1. The Applicant is a serving Police Officer of the rank of Detective Sergeant with the Metropolitan police service (MPS). He has 19 years' experience and on the 15/5/18 was working on Operation Clan William an MPS investigation into class A drug dealing. His unit was involved in the surveillance of a suspect X. On that day X was seen by police and attempted to escape. He ran into the path of a police vehicle driven by Officer C and there was a collision. X was thrown over some railings into a lower area below. He was injured. A bag containing 500g of cocaine was found in the lower area with X.

He alleged that he did not have the package and that it must have been there already and so by coincidence he landed next to it. X was arrested

2. Motor car dash camera footage from one of the police vehicles driven by Officer B showed the moment that X went over the railings. The device used was the personal property of Officer B. The footage showed the incident and importantly that X had the package before he went over the railings. Therefore, the film was important and used in the prosecution of X. It disproved his initial account. After X's arrest the Applicant became the officer in charge of the investigation. He and his colleagues were required to gather the evidence to be used in the prosecution. There was a parallel investigation into the collision between X and the police car. The footage was relevant to that investigation too.

3. Eventually X pleaded guilty to possession with intent to supply cocaine and heroin. He was sentenced to 2 years 4 months imprisonment.

4. On the 7/6/2018 the Applicant maintains that he obtained a copy of the footage for the purposes of the investigation from DC Bowden of the DPS (Directorate of Professional Standards). The Applicant tried to view the footage using a work computer however there were technical issues when he tried to freeze the film to show that the package was in the possession of X at the relevant time. He therefore filmed the footage on his iPhone7 and was able to see what he was looking for. The following morning, he resolved the issue with the computer that had been causing problems and he was able to produce stills. The stills were submitted to the CPS.

5. On the 7th June Officer B and the Applicant exchanged text messages[1] . Officer B asked the Applicant to send to him the footage he had recorded. The Applicant did so. It is said by the Applicant that he did so for a policing purpose because Officer B no longer had a copy having given his copy to the traffic officer investigating the collision. Officer B thereafter forwarded the footage to a family member. The applicant says he did not know that was to happen and would not have supplied the footage if he had. The IOPC have the messages from the download of Officer B's phone.

[1] Witness statement - Hill 5/5/2000 Paragraph 14.

6. At the time despite the use of personal phones and WhatsApp to send work related policing messages being unauthorised there was nevertheless a widespread use of WhatsApp by officers. Groups were formed by teams working together so that communication was improved. The Applicant asserts that the MPS impliedly consented to the use of WhatsApp because it was widespread and known to be so used by senior officers without dissent. Unfortunately, some had used WhatsApp to send police and data sensitive material to persons outside the MPS and so not for policing purposes. The investigation of which this case is part revealed over 50 officers using WhatsApp to send information. Fortunately, the vast majority did so for legitimate policing purposes.

7. On the 19/6/19 IOPC investigators purporting to be exercising the powers of constables met with the Applicant and recovered from him his personal mobile phone (ex KCA/3). The Applicant seeks the return of his phone and applies by virtue of S.59 Criminal Justice and Police Act 2001 (CJPA). He says the phone contains personal information. The IOPC accept the investigators concerned unlawfully seized the phone as they were not authorised to act as police constables at the time. Therefore, the phone falls to be returned subject to the cross application made by the respondent pursuant to S.59(6) of the Act. In short, the Applicant says the transmission of the footage via his phone was for a legitimate policing purpose and cannot constitute an indictable offence. The respondent disagrees. The respondent seeks to have the download of the phone examined to show if there were other messages to or from Officer B around the time of the sending of the footage to disprove or support the policing purpose suggestion. The Applicant responds by saying the IOPC have the messages from the download of Officer B's phone. The IOPC do not seek to use the download to investigate any other as yet unknown activity.

8. As set out in my earlier decision the law allows the respondent to examine and rely upon the content of the material for the purposes of their cross application despite it being obtained unlawfully. In this case the phone content has been downloaded however the respondent has not accessed the content by agreement. At this preliminary stage I decided that I should hear evidence as to the way in which the phone came to be seized to determine if this was such a '*rare'* case as described by Hickinbottom J (as he

then was) in *Chatwani*[2] and determine if the failings leading up to the seizure were of the type described in the case law where the respondent is to be denied the benefit of the product from the seized material for the purposes of their cross application. I have to determine the degree and level of fault in accordance with the established law and the facts of this case. I have to consider, as part of that determination, if there was bad faith on the part of the IOPC. That said no similar case has been determined. The case law largely concerns search warrants, the applications for them and Judicial review claims that followed seizures. In the cases where the conduct was regarded as sufficiently serious and concerning to prevent the party holding the material to retain and use it the facts of each case are specific and can only provide general guidance as to how serious the failings are and need to be to prevent continued access and use of material obtained unlawfully.

9. The reason why the investigators who met with the Applicant and took his phone were not authorised to do so and did not have the '*powers and privileges of constables'* is because the formal process of referring a '*conduct matter'* had not been complied with by the IOPC. The respondents agree that is the position and that the phone was seized unlawfully. The correct referral process had been completed in relation to three police officers, officer A, Officer B and Officer C but not in relation to the Applicant. In short, the respondent's case is that it was assumed that because the three other officers had been correctly referred and that the Applicants case was part of that wider investigation a separate referral was not necessary. That was wrong and has been accepted by Mr Bird as '*incompetent'*. It is that failure that is central to my decision at this stage. I am not determining the S.59(6) cross application. That will follow.

The legal framework

10. The IOPC (Independent Office for Police Conduct) and its predecessor IPCC (Independent Police Complaints Commission) are creatures of statute. Their powers are derived from the Police Reform Act 2002 (PRA). Part 2 of the Act sets out how they are to deal with the 3 main areas of their remit, namely to handle complaints, "conduct matters" and "DSI matters" (Death or Serious Injury). Schedule 3, enacted by

[2] [2015] EWCA 1238 Admin

s.13, sets out provisions for the carrying out of investigations into each of these 3 areas. This case involves a "*Conduct Matter*" as defined in S.12(2).

11. A "*conduct matter*" means a matter other than a complaint or death and serious injury matter in which there is "*an indication (whether from the circumstances or otherwise) that a person serving with the police may have— (a) committed a criminal offence; or (b) behaved in a manner which would justify the bringing of disciplinary proceedings."* (section 12(2)). A "*recordable conduct matter*" is defined in section 29.

12. The relevant legislation to be considered is the PRA 2002 as it was in October 2018, prior to the amendments enacted by the Policing and Crime Act 2017 which did not come into force until 1st February 2020.

13. Schedule 3 to the PRA 2002 governs the process by which responsibility for an investigation is allocated between the relevant police service and the IOPC, and the circumstances in which members of the IOPC staff acquire the powers of a constable. I shall refer to that as *'the referral process'*.

The Referral Process

14. Where conduct comes to the attention of IOPC before it comes to the attention of the relevant police service (for example where, as here, the conduct is discovered in the course of another investigation of which the IOPC is already seised) the IOPC may continue its investigation (see para 13(5)) but there are five stages involved before investigators of the IOPC become entitled to exercise the powers of a constable in relation to the investigation into that additional conduct. The five stages are;

(i) Notification of the conduct to the police service by the IOPC; The IOPC has the power, where appropriate, to direct the relevant police service to record a matter and refer it to the IOPC (under paragraph 11(5) and paragraph 13(1)(c)). However, that power is not relevant in this case, rather the IOPC simply notified the police service of the conduct for it to consider making a voluntary referral.

(ii) Decision by the Police service: Once that happens a decision by the police service is necessary to record the conduct and refer the matter back to the IOPC; Whether

or not the IOPC notifies the police service of conduct, the police service may voluntarily refer the matter in any case where, by reason of the gravity of the matter or any exceptional circumstances, it considers that it would be appropriate to do so (paragraph 13(2)).

(iii) IOPC decision to investigate; Once referred back to the IOPC a decision is necessary by the IOPC that the matter should be investigated; If the police service refers a matter to the IOPC, the IOPC must determine whether or not it is necessary for the matter to be investigated. The duties of the Director General (DG) are set out in paragraph 14(1).

(iv) Type of investigation. If the police service refers a matter and the IOPC determines that it is necessary for the matter to be investigated, the IOPC must, having regard to the seriousness of the case and the public interest, determine the form which the investigation should take (paragraph 15), by reference to subparagraphs 15(4) - (4C). There are three options (a) an investigation by the appropriate authority on its own behalf (b) an investigation by that authority under the direction of the Director General or (c) an investigation by the Commission.

(v) If, under paragraph 15, the IOPC determines that the investigation is to take the form of an investigation conducted by the IOPC itself, the Director General (DG) must designate a person to take charge of the investigation and such members of the office's staff as are required by the Director General to assist that person (paragraph 19).

(vi) In practice, the decision-maker in the police service is the "appropriate authority", normally a delegate of the chief officer of police within the directorate of professional standards. The decision-maker in the IOPC is a delegate of the DG, in practice an assessment manager within the IOPC assessment unit. The lead investigator and persons to assist him will have been designated, as such, by the DG (paragraph 19).

15. Therefore, in this case as an example and as I shall explain, IOPC Investigator Mr Jack Lee had the powers and privileges of a constable in respect of the officer A investigation because the following four decisions had been taken: Gareth Smith of the MPS decided to refer Officer A's conduct (about which he had been notified by Investigator Brewster

of the IOPC) to the IOPC (JL/3). He did so voluntarily and only in respect of Officer A. He gave his referral rationale in an attached document. Harpreet Sahota of the IOPC determined that the officer A matter must be investigated. He gave his rationale in the text alongside the grey box marked "Assessment" [JL/4 at R58-59]. Harpreet Sahota determined that the Officer A matter shall be independently investigated (that is to say investigated by the IOPC not the MPS). He gave his rationale in the text alongside the grey box marked "MOI decision" [R58-59]. Mr Lee was assigned as the lead investigator by Cath Hall [R55]. As a result, the case was given a reference number 2018/110313.

16. Importantly in those circumstances, the persons so designated "*shall, for the purposes of the carrying out of the investigation and all purposes connected with it, have all those powers and privileges (*of a constable*) throughout England and Wales…."* under paragraph 19(4). It is only in these circumstances that the powers and privileges of constable are bestowed upon the IOPC. That is said by Mr Yeo to be significant. He submits the vesting of such powers in individuals requires the process to be completed for good reason and is not to be taken lightly. Unless and until the '*referral process'* is completed those important powers are not so bestowed. That did not happen in this case.

The facts of this case

17. From the agreed chronology, the following are the essential facts and events. I have not set out all events for the purposes of this decision. The agreed chronology should be read as part of this judgement. The chronology sets out the references to the associated documents.

18. In May 2018 the Applicant was aware from emails that there was to be a local investigation into the collision involving X. A formal complaint was made to the IOPC by X's solicitor on the 4/6/18. On the 7/6/18 the Applicant sent the footage to Officer B. In July 2018 the IOPC began an independent investigation into the X collision known as Operation Irwin. As part of that investigation in September 2018 the phones of Officers A, Officer B and Officer C were seized. The phones were examined. It was

at this time that the widespread use of WhatsApp by officers was discovered. After this date the referral process for officers A, Officer B and Officer C was followed correctly.

Officer A

19. In summary; the IOPC notified the MPS of potential data breaches by officer A. A conduct matter was recorded by the MPS on the 5/10/18. The IOPC received a formal referral of a conduct matter on the 15/10/18. That referral referred to other officers being involved in data breaches but they are not named on the referral. The IOPC assessment unit determined that the matter should be the subject of an independent investigation and Mr Lee was appointed as the lead investigator. The case was given the Perito number (internal case management system) of 2018/110313. Mr Sahota in his decision assessment stated [JL/4 R57] said '*There is an indication that the matter concerns a large number of members of the MPS some whose identity has been confirmed but they are not the subject of this referral'.* That detailed assessment is an important part of the referral process. Of note is the comment by Mr Sahota that although there was a wider pool of suspects other officers were not the subject of the referral. There is no suggestion that a blanket or wider referral was made or even contemplated by Mr Sahota. Separate consideration was needed despite the numbers of officers involved or suspected.

Officer C

20. The IOPC notified the MPS of potential data breaches on the 18/10/18. A formal referral back to the IOPC was received on the 24/10/18. The assessment unit determined that the potential data breaches be the subject of an independent investigation on the 29/10/18. A Perito number was given of 2018/110784 and linked to 2018/110313. Mr Mr Lee was appointed as the lead investigator.

Officer B

21. The IOPC notified the MPS of inappropriate content found on the phone of Officer B on the 9/10/18. The MPS formally referred the conduct matter back to the IOPC on the 18/10/18. On the 24/10/18 the IOPC notified the MPS of potential data breaches by

Officer B to DS Hill on the 7/6/18. The referral from the 18/10/18 was assessed and it was determined that the matter be the subject of an independent investigation. That referral was given the Perito number 2018/110539 and linked to 2018/110313. The potential data breaches were referred back to the IOPC on the 25/10/18. That matter was assessed and determined to be the subject of an independent investigation on the 30/10/18. A second Perito number of 2018/110829 was given to this separate investigation and linked to 2018/110313. All cases (Officers A, Officer C and Officer B) were then linked together under number 2018/110313 and called Operation Trent. Mr Lee was the lead investigator for all three officers and the four cases referred.

22. On the 14/12/18 the IOPC settled their terms of reference for the investigation. They were general and wide to cover the inappropriate use of WhatsApp. Individual officers were not named. From December into 2019 work commenced into the downloading of phones. On the 6th February Kieron Casserly produced a spreadsheet (ex. KC/2) setting out the information shared by over 50 officers. Preparation of investigator reports for each officer began at this time. This work involved placing the individual cases into categories (described in evidence as buckets) given the conduct revealed. On the 22/3/19 the IOPC decided that a proportionate investigation was merited. Only those officers who appeared to have shared operational material for non-policing purposes would be the subject of a formal investigation. Others would be dealt with by '*learning recommendations'*. By the end of March 2019 53 officers had been identified. On the 26th March Kieron Casserly completed a RIPA application for access to the phone / data records for DS Hill's personal phone. That was done to see if the phone was still active and thus worthy of recovery.

23. On the 4/4/19 a meeting took place with the senior IOPC staff members who have given evidence in this case namely Graham Beesley - Operations Manager (now interim Regional Director of the IOPC), Stephen Foxley - Operation Team Leader and Mr Lee. A lawyer Mr Gayer was also present. On 30/4/19 the IOPC decided to serve formal notices of investigation on DS Hill, Officer C and Officer B. The IOPC decided not to serve Officer A. Mr Lee drafted a severity assessment (normally prepared after referral and determination) for DS Hill dated the 17/5/19. His decision to do so [JL/9 R68] notes

that he had been in discussion with *'legal'* and '*DM*' (decision maker Mr Beesley) and he decided to focus on the sending of the footage to Officer B. That severity assessment and those for Officer C and Officer B were agreed by the MPS on the 21/5/19. The MPS did not point out that no conduct matter had been recorded by them and that no referral from them had been submitted to the IOPC in relation to DS Hill.

24. On the 22/5/19 Mr Lee decided to request the personal phone from DS Hill either by consent after serving notices of investigation and criminal letters or by arrest. His policy decision number 89 refers to DS Hill as a suspect in the investigation. His policy decision number 90 on the same day refers to his belief that arrest was not appropriate in order to obtain the phone. However, he went on to conclude that when DS Hill was served with the notice of investigation and criminal letter if he refused to hand over the phone or did not have it on him then arrest would be considered under S.13 PRA paragraph 19(4) of schedule 3 as he would have the powers of a constable. He would also be able to arrest DS Hill under PACE S.24(2) and search him.

25. Attempts were made to serve DS Hill with the notice of alleged breach of standards of professional behaviour (a Regulation 16 notice) and a criminal letter setting out potential offences under S.55 DPA 1998 and S.170(1)(a) DPA 2018 (JL/17 and JL/18). That letter sets out that an interview under caution will be arranged. The letter contains a caution in the usual terms. A provisional strategy was drafted by the IOPC (JL/12) to serve DS Hill on the 10/6/19. That strategy sets out the intention that after service of the two letters DS Hill would be asked to hand over his phone. If he refused or did not have it on him arrest will be considered. Mr Lee again stated erroneously that he had the powers of a constable. Custody was to be considered if a search of outer clothing was unsuccessful with a custody sergeant authorising a search in custody albeit that was regarded as unlikely.

26. The criminal letter is an important document. I repeat there was no significant action in relation to the above cases on the 23/10/18. However, that was the date that appeared on the letter served on DS Hill (ex. JL/18) on the 19/6/19. That letter stated '*IOPC investigation into the inappropriate use of computer systems by officers within the*

MPS' and '*On the 23rd October the MPS referred this matter to the IOPC. After considering the circumstances the IOPC decided to conduct an independent investigation'*. The case reference number was given as 2018/110313. There had been no referral and no determination that there be an independent investigation as prescribed by the referral process.

27. A decision to serve DS Hill at home was changed, due to concerns surrounding the health of DS Hill's partner, to arranging a meeting at Jubilee House in London on the 18th June. Originally Mr Lee and Steven Foxley were to attend on the 18/6/19 however DS Hill was not at Jubilee House to be seen. The next day Mr Lee was to be occupied with serving notices / letters and interviews of Officer C and Officer B. Therefore, Investigators Casserly, Alexis and PS Kirby were instructed to deal with the matter on the 19/6/19. The IOPC had been eager to ensure DS Hill was unaware the IOPC would be attending to '*ensure the integrity of the investigation'* [JL/15 R76]. In other words that DS Hill was able to delete any material if given advanced notice. The note ended with '*there is no guarantee that this method will work'.* The aim seems to have been to obtain DS Hill's phone before Officer C and Officer B were served. Senior officers of the MPS had been involved in arranging the meeting and keeping the real purpose from DS Hill. DS Hill was to be told the IOPC wanted to see him by DCI Gosling once he was in the room ready for the meeting.

28. In short DS Hill was asked to attend at Jubilee House for the meeting. He said DI Durham called him and asked him to attend a meeting. DS Hill said he was told the IOPC wanted to see him. In his evidence however, DI Durham was unsure if he told DS Hill that the IOPC wanted to see him. DS Hill therefore, according to him, knew of the meeting's purpose and assumed it was to do with the arrest of X. He did not take his phone to the meeting and instead placed it into a disused electrical cabinet in the basement carpark. When in the room he was informed that the IOPC wanted to speak to him and the investigators and PS Kirby entered. The notice and the letter were read to DS Hill and copies were given to him. He was asked for his phone and said he did not have his phone on him (there is an issue about what was said). DS Hill says he was then told he would be arrested and told his home would be searched. That is not

disputed. The meeting paused with the investigators leaving the room. When they returned DS Hill took Kieron Casserly to the carpark and handed over his phone. DS Hill was asked for the PIN number and refused to give it. Later he admitted sending the film to Officer B. At no time was DS Hill given legal advice.

29. It should be made clear the IOPC investigators and PS Kirby who attended on the 19/6/19 are not at fault. They all gave evidence and told me, and I accept, that they believed the correct referral process had been completed and that as a result the IOPC investigators had the powers etc. of constables. PS Kirby said that because there was a severity assessment for DS Hill that had been sent to her Inspector she believed the correct referral process had been completed. The errors and failings were made by those above them in terms of rank / status within the IOPC.

30. In addition, on the same day – 19/6/19 Officer C and Officer B were also served with Regulation 16 notices and criminal letters. Before that they had not been aware they had been under investigation other than in relation to Operation Irwin. Their phones had been seized as part of that operation.

31. Following that on the 3/7/19 Mr Lee served a S.49 RIPA 2000 notice on DS Hill requesting the PIN number for his phone. DS Hill was interviewed under caution on the 29/7/19 and he was provided with pre-interview disclosure. At interview DS Hill provided a prepared statement.

32. On the 17/2/20 DS Hill applied for the return of his phone pursuant to S.59(2) CJPA 2001. The IOPC responded on the 2/3/20**.** On the 20/4/20 Mr Lee brought to the attention of his senior members of staff the lack of a referral in relation to DS Hill. A retrospective recording of a conduct matter was made and referred by the MPS on the 11/5/20. The IOPC assessment unit determined that an independent investigation would be carried out on the 13/5/20. On the 16/6/20 the IOPC conceded that DS Hill's phone was unlawfully seized.

Preliminary matters

33. I need only refer to the evidence central to the failure to refer the case of DS Hill in this judgement. There is a discrete issue concerning what was said at the meeting on the 19/6/19 and whether or not when asked where the phone was he said it was '*at home'*. The IOPC investigators and PS Kirby all gave evidence that he said that. DS Hill and the two senior officers in the room at the time DCI Gosling and DI Durham said he did not. The contemporaneous notes of the meeting compiled by OTL Alexis and DI Durham do not refer to the comment. It is agreed by counsel that I need not determine that issue at this stage. I agree, it does not, it seems to me, impact my assessment of the decision I have to reach at this time.

34. In addition, there has been some debate about the burden and the standard of proof to apply. Mr Yeo concedes that he has to prove bad faith. Otherwise he contends that as the cross application is the only live issue – unlawful seizure having been conceded and therefore the Applicant's S.59(2) application succeeds it is for the respondent to prove the case to the civil standard. That is right in relation to the cross-application. At this stage Mr Bird agrees but submits that the decision I have to make is in effect a case management decision and no strict burden or standard of proof applies. In my judgement in order to satisfy myself that the respondent should not have the benefit of the material for the purposes of their cross application and that submission is made by the Applicant it is for him to show the failure is of a type and nature that means the respondent loses the normal right to have the material to support the cross-application. Thus, in my judgement, the Applicant bears the burden to show the conduct is of such a type and nature to the civil standard.

The evidence

35. At the start of the hearing I asked why there was no evidence submitted by the IOPC from Messrs Beesley or Foxley given the important role that had clearly played in this case and that others referred to them. That was rectified and witness statements were served. They were called to give evidence.

36. Mr Lee[3]. Having set out the history and the referrals of the other officers at paragraph 13 in error he states that the 23/10/18 was a day when conduct matters were referred to the IOPC in relation to Officer C and Officer B. He said at Paragraph 16 that it was his understanding that his role was to investigate the actions of each officer named in Operation Trent. He refers to meetings with Mr Beesley and Mr Foxley that continued into early 2019. He said that based on the evidential position after the detailed review of the phone downloads three officers met the criteria for formal investigation. They were DS Hill, Officer C and Officer B. He said at paragraph 22 *'I did not direct the MPS to record and then refer a separate conduct matter against DS Hill to the IOPC because I believed his conduct had been captured in the initial referral in October 2018. I have since learnt that this belief was mistaken'.* He mistakenly believed that the IOPC investigators who met DS Hill had the powers etc. of constables and therefore had the power to arrest and / or seize his phone under S.19 PACE.

37. In evidence before me he said that IOPC investigations are predicated on the referral process. He told me how the process worked and that he had been trained. He said he was advised by Messrs Beesley and Foxley that he was conducting an investigation into the use of WhatsApp rather than specifically the actions of officer A. He confirmed that in December 2018 neither Officer C not Officer B knew that they were being investigated for Data breaches. Their phones had been seized as part of Operation Irwin and possibly perverting the course of justice. The downloads however were being used for another purpose. He said they did not want the two officers to know because they might tell other officers and thereby hamper the investigation. He said he thought a referral included all of the officers in the WhatsApp group. He repeated several times that he did not think there had to be a separate referral for DS Hill.

38. He was unable to explain at all the date on the criminal letter erroneously suggesting the 23/10/18 referral. He said it was wrong and a '*mistake'.* He said the letter was a template investigators fill in. He said he could have expanded the wording to refer to his understanding of the situation and accepted anyone reading the letter would get the wrong impression. He denied cutting corners and that that '*nothing was deliberate'.* He

[3] Witness statement dated 10/9/20

said the referral dates on the letters for the other officers were correct and that he got the information from Perito. He said he could not recall why he put the referral date as the 23/10/18 for DS Hill. He denied choosing a date around the time of the other two letters. He accepted the letter would mislead IOPC investigators into thinking they had the remit to investigate DS Hill.

39. He agreed that the decision of Mr Sahota [JL/4] in relation to Officer A was an important document and without such a document the IOPC cannot start an investigation into an officer. He said the referral process was well known, however for this investigation he was under the impression the conduct had been captured and therefor he did not need a specific conduct referral for DS Hill. He said he was heavily supervised and was having meetings twice a week with Messrs Beesley and Foxley and no one identified that a specific conduct referral was required. He said the issue was not discussed. He said his case supervisor (Foxley) was of the same view. He agreed that the referral process involved stages that had to be met before a case proceeds.

40. He said later that when he picked up the investigation he believed that a referral had already happened but that he did not realise each officer had to be specifically named. He said he did not know each officer had to have a specific referral. He said the Perito case management system had a '*subject tab'*. He said the system would show the date of a referral. The linking of the referred cases under the original number was done by the assessment unit at the direction of either Messrs Beesley or Foxley. He said his belief was that the earlier referrals had captured DS Hill. He said if it had been any of the other fifty-three officers who had merited investigation he would have followed the same process. He agreed that if the officers attempted to arrest DS Hill and they did not have the power to do so it would be an assault. He said if he had discovered the error prior to the 18/6/19 it would have been rectified and that was a '*straightforward process'*.

41. Graham Beesley[4] the Operations manager at the time told me that the Lead Investigator is responsible for delivering and carrying out the investigation. The Team Leader (Foxley) is responsible for supervising the Lead investigator. He said he was the Decision Maker. He described his role to draft the terms of reference with the Lead Investigator and make sure the investigation met those. Finally, he would read the final report and decide if there was a breach of professional standards or a criminal offence. He was referred to the minutes of a meeting on the 4/4/19 [R114-132]. He said in his witness statement that because a severity assessment was discussed at this meeting he assumed a conduct referral had been received from the MPS. During that meeting, there was discussion about DS Hill's case and the meeting agreed to hold another meeting to discuss '*logistics and tactics in relation to arrest and interviews'*. The seizure of the phone, a search of the home address and DS Hill's arrest were also discussed. He said he believed there had been a referral for DS Hill. He thought that because DS Hill was talked about as a '*subject'* and there was to be a severity assessment. He said his reaction was one of '*disappointment'* when the error was brought to his attention. He described the error in his witness statement as a '*technical oversight'*.

42. He said there was significant training in place for staff in 2018 and 2019 to make sure the referral process was followed. He then said there was a '*confused picture'* when there were multiple suspects and there was a large criminal investigation. He said there was a '*view'* that when one or two suspects were properly recorded and a further suspect came to the attention of the team it was not clear whether or not that individual needed to be recorded by the MPS. He said it was thought the powers etc. of a constable attached to the independent investigation and if an additional suspect was identified the powers were extended to that individual. He said he had learnt that over the years and it was '*ingrained'*. He added at one point '*but clearly there has to be a conduct referral'*. He then said that he too was confused about the system. He clarified his belief at the time in 2018 by saying '*I believed two things. If there was a single referral we couldn't arrest but if there were multiple suspects and we had a referral we could identify other suspects and deal with that suspect'*. He said he believed there were two processes. He had never seen a request for a conduct matter to be recorded form [JL/3]. He said he did not read delegation decisions such as that made by Mr Sahota for officer

[4] Witness statement dated 21/9/20

A [R56]. He said he took comfort from the fact that each investigation had a lawyer attached to it and therefore he knew he was acting correctly. He said he could not remember any conversations where a lawyer had said they were acting incorrectly.

43. He was asked about the criminal letter. He said the use of the date and the reference to an investigation was '*incredibly unfortunate but I cannot believe someone has falsified a document like that there must have been a level of confusion'.* He said, *'no member of my staff would ever do that'* and *'if my staff did that that must be what they believed'.*

44. Mr Bird has suggested in his closing submissions that Mr Beesly had learnt of the incorrect belief and process after these events. That is clearly not the case. Mr Beesly was a person in a senior position, in charge of others and who had a completely wrong and incorrect understanding of the referral system. His admissions and ignorance of the proper referral process is of considerable concern. His false understanding appears to have been widespread among staff and commonly believed to be correct.

45. Stephen Foxley[5] gave evidence. He had been a police officer for 30 years. In his witness statement, he said that when the phone was recovered from DS Hill on the 19/6/18 he had no reason to consider that anything was wrong with the way in which they had conducted the investigation. He was of the opinion that the investigators had the powers etc. of constables. He said in his evidence that DS Hill was included in the other referrals for the officers involved in the WhatsApp investigation. He said it was a '*group referral'.* He accepted it was his responsibility to check that a referral had been made. He said that when an officer was served with a notice or letter the referral was not disclosed and there was no way that an officer could check to see if a proper referral had been made. He assumed no other investigations in his then five years at the IOPC had been conducted without a referral. He said the date on the criminal letter of the 23/10/18 '*looks like he has taken something from between the dates he has seen.'* He denied that, to avoid officers being tipped off and thereby destroying evidence, that he

[5] Witness statement dated 21/9/20

and Mr Lee had decided not to ask the MPS to refer the case. He said '*The IOPC don't do tricks'.*

46. Kieron Casserley was acting in the clear understanding and belief that the correct referral process had been followed prior to the 19/6/19. He said his understanding was the IOPC had decided to conduct a criminal investigation following a referral from the MPS. That meant the Decision Maker had assessed or taken legal advice and decided to conduct the investigation. He said he was of that belief given the briefing sheet he received from Mr Lee the day before. Prior to that he had been in numerous meetings where criminal offences were considered and discussed about DS Hill hence he *'automatically assumed that they would go through that process'.*

47. What the evidence suggests is that at no time in any meeting was the issue of the referral of DS Hill's case discussed. There appears to be total silence on the matter with some believing one thing and others a different thing. At no point was the confusion described by Mr Beesley ever clarified by a lawyer. That is in my judgement a very concerning state of affairs. The minutes of the meeting of the 4/4/19 have been heavily redacted and I have not been provided with the legal advice given if any was.

Case law

48. A number of authorities have been referred to. I concentrate in this judgement with the most relevant. That said I have considered all of them. Many do not relate to the S.59 jurisdiction. That said principles have emerged that are relevant to my decision at this stage.

49. The decisions in *HMRC v Cheema and others* and *R (Van der Pijl) v Kingston Cr Ct (no 2) [2013] EWCA 3040* make it clear that for the purposes of the cross application the content of the seized material can normally be considered and relied upon by the party holding the material.

50. In *El-Kurd v Winchester Crown Court [2011] EWCA 1853 (Admin)* SOCA obtained a search warrant for businesses. After seizure of documents SOCA discovered that there had been a failure to indicate on the face of the warrant the nature of the investigation which it was issued to facilitate. That was required by PACE 1984[6]. Accordingly, SOCA concluded that the warrant was unlawful. SOCA then applied for a further warrant to seize and retain the same material. SOCA applied under S.59 CJPA 2001 to retain the property retained under the first warrant. Judicial review was sought of the decision of the Crown Court to authorise retention. The court decided that the S.59 jurisdiction conferred upon the judge a discretionary power to authorise retention. However, in exercising that discretion the court will be astute and subject to the most rigorous examination the circumstances leading up to and surrounding the illegality of the initial seizure. There was, in the case, no suggestion of bad faith or any lax approach in the drawing up and execution of the first warrant. The application was dismissed. Stadlen J said '*any suggestion of bad faith or even that the police or other agency adopted a less than rigorous and scrupulous approach to the drawing up and execution of the initial warrant is likely to weigh heavily against the exercise of the discretion in favour of authorising retention.'*

51. In *Kouyoumjian v Hammersmith Magistrates Court [2014] EWHC 4028 (Admin)* search warrants were obtained pursuant to S.8 PACE 1984 in relation to drugs offences. The warrants were challenged by Judicial Review seeking inter alia return of all material seized. There was a pending S.59 application in the Crown Court for retention. The court considered six factors suggested by counsel for the Applicants as relevant to the decision to order delivery of the materials. There was no authority on the point. The factors were if the court had been misled, if so the reasons for the misleading, the conduct of the authority, the basis upon which they seek to retain the material and what the material is and finally the prospects of the S.59 application. The court considered those factors although did not expressly approve them. The court concluded that it (and the Crown Court) had been misled in relation to the change in the original purpose of the investigation into drugs offences to one concerning financial matters. The court stressed the duty of candour owed to the court when applying for an order to retain under S.59 CJPA 2001.

[6] As modified by POCA 2002

52. In *Chatwani [2015] EWCA Admin 1283* the issue was narrowed down. Again search warrants were obtained. Judicial Review was sought. The NCA conceded that the warrants were unlawful, should be quashed and the entries and seizures declared unlawful. The court was tasked with deciding if the NCA could retain the material pending a proposed S.59 application to retain. The case concerned what were described as innovative and audacious methods by the NCA. The plan was that when the warrants were executed in a deliberately boisterous way covert surveillance devices would be deployed at a business address and at the homes of the suspects. After questioning it was hoped they would react to their arrests and evidence would be obtained that would assist in their prosecution. The court considered the relevant principles governing the granting of a search warrant including the duty on the Applicant to put before the court the necessary material to enable the court to satisfy itself that the statutory conditions for the warrant are met. The court referred to the duty of candour when applications are made without notice. The court rejected the suggestion there was bad faith however Hickinbottom J said [P.111] *'the failings of the NCA resulted from ignorance on the part of the officers involved, coupled with a systemic failing which resulted in the fundamentally misconceived approach to these warrants being pursued and not being stopped.*'

53. Later His Lordship said that each case will be fact-dependant and quoted Stadlen J in *El Kurd* and at [P.135] '*There may be circumstances in which it is appropriate to deny the agency of all benefit of the illegal search irrespective of the nature and content of the documents seized. Those circumstances are likely to focus on the agency's own conduct. If it has acted in bad faith that is likely to be a compelling reason for not allowing it to retain any benefit from the exercise. However bad faith is not a prerequisite: the agency's conduct……may drive this court to give the subjects of the warrants relief to deny the agency of all benefit of the unlawful search. I stress that the circumstances in which the court is likely to make such a finding will be rare.'*

54. At [P.141-2] The Learned Judge said '*I am unpersuaded that the NCA officers acted in bad faith. However, they acted with patent and egregious disregard for, or indifference to the constitutional safeguards within the statutory scheme within which they were*

operating. The individual officers, I accept, were operating out of ignorance: but that ignorance was deep, it ran to inspector level, it related to the fundamentals of the scheme being operated and there were no systemic checks to ensure warrants were not issued without even consideration of the requirements of sections 15 and 16 of PACE. Given the system then in place, it was almost inevitable that an application for a warrant would be grossly deficient..'. He added that the case did not concern relatively minor errors and *'the errors were grave and went to the very root of the statutory scheme'.*

55. Davis LJ added that agencies like the NCA would be well advised to take legal advice in advance of such applications. He added *'...laxness in this context cannot readily be tolerated when one compares and contrasts the very careful preparation routinely given to , and close scrutiny undertaken by the courts of applications made without notice for search orders in civil cases'* [P.149]

56. In *R (Windsor & Hare) v Bristol Cr Ct [2011] EWCH 1899* HMRC had undertaken not to copy material and had acted in contempt of court in doing so.

57. Finally, in *Brook and others v Chief Constable of Lancashire Police [2018] EWHC 2024 (Admin)* Leggatt LJ (as he then was) was also considering judicial review of two decisions to issue search warrants. He concluded that the evidence did not indicate that any misrepresentation or failure to disclose information had taken place. The second warrant was declared unlawful because it was issued on the basis of a plainly material error of fact and the magistrate may have come to a different conclusion. In relation to the retention of material seized for the S.59 application His lordship said there was no basis for alleging the police acted in bad faith. However, he found the failure to disclose a note of a conversation that had been requested at the outset of the proceedings was a matter of '*great seriousness'*. He found that was an act that was untenable, a wrong position to adopt and was inconsistent with the duty of candour. The warrants were quashed and permission to retain the material for the S.59 hearing was refused. The court ordered that the seized material be returned and all copies were to be destroyed.

58. Submissions: I have considered the oral and written submissions of counsel. Mr Yeo submits that the factors I should take into account in refusing the respondent from having the benefit of the material for the purposes of their cross application are in summary:

- Bad faith. He says the level of incompetence and misunderstanding as stated by the IOPC staff 'begs incredulity'. He says the disconnect is not tenable. He submits the crime letter with the false date and Mr Lee's inability to explain it means there is no innocent reason. He says a trick was played with a date that fits the other referrals and because a subject would not ordinarily have the actual referral disclosed no one would ever know. Avoiding tipping off is suggested as the reason.

- Overall conduct. The IOPC's purpose is to hold to account those who have the powers etc. of constables. Such powers are only vested in investigators when the correct referral process has been completed. He submits there has been a fundamental breach of police powers by purporting to exercise the powers etc. of constables when unauthorised to do so. He says the ignorance was endemic and extended to senior officers. He submits there was in existence according to the evidence a '*non-statutory process with no bounds*'. He asks why have a statutory process if you can add suspects at will? He says there was (i) a lack of safeguards namely training, and supervision (ii) there was laxness in the RIPA application and there was no proper consideration as to why the Applicant had sent the film to Officer B (iii) the seizure was fundamentally unlawful accompanied by the threat of arrest and search of the Applicant's home (iv) it was disproportionate. Finally, he says there are poor prospects of the final application and that it took the IOPC until 2/7/20 to admit that the seizure was unlawful when the absence of a referral had been discovered in April 2020.

59. Mr Bird for the IOPC concedes that the seizure was unlawful because there was no separate referral for DS Hill. He categorises the error as "a 'lack of diligence', an 'oversight and 'incompetence' ". He says there is no bad faith, no abuse of power and no deliberate flouting of the rules. He refers to the case law as a guide to the type of conduct that would be sufficient in such a case to deny use. Mr Bird says there is no

motive to act in bad faith or to cut corners because the correct process could very easily have been adopted. He says there has been no deliberate disregard of the scheme, the court has not been misled and there has been no contempt of court therefore the conduct is not so bad and does not meet the test for refusal to use and rely upon etc. He invites me to accept the apologies and explanations of the IOPC and to categorise what went wrong as a '*simple oversight'* that was easily remedied.

60. In his response to the Applicant's submissions he adds that the statutory structure is not straightforward and thus something might be overlooked. He reminds me that a departure from the normal course i.e. use of content for the application will be in rare cases.

61. I have been asked to consider the overall prospects of success as a factor at this stage by Mr Yeo. Assuming it is a relevant factor I do not consider it necessary to come to any view and to take that into consideration given the findings I have made.

Decision

62. It is not necessary for me to resolve every issue raised. I have to decide if the conduct of the IOPC does fall into the rare category of cases where they should be denied the benefit of the material, in this case a phone download, for the purposes of their cross application. For the following reasons and applying the relevant law I am so satisfied that this is such a rare case.

63. It is agreed that all of the correct steps were taken in the cases of officer A, Officer C and Officer B. Their cases were given unique reference numbers initially then all three were grouped together under the Perito reference number for officer A. No such number was ever allocated to the case of DS Hill because no referral was made. None of the required steps and stages set out above were undertaken and completed in his case. A severity assessment was made suggesting to others that the correct procedure had been followed.

64. It is the absence of the correct decisions and procedure being followed in the case of the Applicant that led to the admitted unlawful seizure of the phone. Because of the failure to follow the correct procedure the IOPC officers who went to the meeting on the 19/6/19 did not have the powers and privileges of a constable. They had no right to ask for the phone, to take it, to say that the Applicant would be arrested for non-compliance or to say there would be a search of DS Hill's home. They believed they did have those powers because they were working on the assumption that the process of referral had been completed in the way that it should. Senior members of staff either knew that the process had not been followed or assumed that it had.

The Criminal letter and the reference to the referral dated 23/10/18

65. Mr Lee drafted this letter from a template. He chose the date of the referral as the 23/10/18. He has not been able to explain that choice of date. It was ether deliberate in the sense that he knew there was no referral and made up a date to fit in with the other dates in which case he was doing more than cutting corners or there is some other explanation that has not been provided. I can only conclude that I have not been told the full facts. That is concerning. The letter is false and misleading. It was designed to demonstrate that a referral had been made and that a criminal investigation had commenced. Any reader of that letter would believe that the correct referral process had been completed and would be misled and deceived. No reader would contemplate that there had been a total disregard for the procedure set out in the legislation. The effect on the recipient cannot be underestimated. To describe this as an oversight is some way off the mark.

66. I regard the letter as significant and important. I note Mr Bird suggested the letter was not in fact requited by law and that the IOPC were entitled to carry on with their investigation. Those facts are correct. The date chosen however, gives a semblance of reality and credibility to the letter and to the referral process falling as it does around the time the other officers were the subject of referral and assessment. Without that process being completed in the correct manner the IOPC officers had no right to (i) purport to act as constables (ii) ask for DS Hill's phone or (iii) suggest that he might be arrested.

67. The criminal letter, I find, therefore supported and legitimised the presence of the IOPC officers in requesting that DS Hill hand over his phone and supported their status as having the powers and privileges of constables. In addition, Mr Lee, even if he had forgotten the fact that DS Hill had not been referred would have discovered that fact on drafting this letter because the date had no relevance to any referral and assessment. He would also have had to add the Perito number and although at that time the cases of the three officers had been linked under one number the absence of DS Hill in that process would have become apparent. To add a false date to the letter cannot be explained by confusion.

The RIPA application

68. Kieron Casserley compiled the application. He said in evidence that when he did so because he had been told there was an investigation into DS Hill by Mr Lee and that he was aware that DS Hill was a '*subject'*. He had included potential offences of perverting the course of justice and misconduct in public office because he had been at meetings with Messrs Beesley, Foxley and Lee. He had not looked at or become aware that the severity assessment for DS Hill did not suggest those offences were made out. He said Mr Foxley checked the application.

69. The RIPA application was clumsy and not thought through. I am not satisfied it was drafted to mislead. It does show however show laxness, a lack of attention to detail and a failure to apply the necessary care needed when drafting such a document.

The severity assessment

70. This is to be completed as soon as reasonably practicable after the appointment of a Lead investigator. That means and suggests the referral process had been completed. In this case there was no referral and yet Mr Lee completed a severity assessment.

71. I am not satisfied there was bad faith that is deliberate avoidance of the correct process to gain a tactical advantage. That said some aspects of this case are particularly concerning. There was at the time a belief in an alternative system that had no basis in fact or law. There was therefore a disregard of the statutory scheme.

72. The whole purpose of the referral regime is that an individual case is assessed and investigated following the correct process. Each case differs from another hence the need for separate consideration. How then can it be that three senior members of staff at the IOPC with many years' experience believed there was a separate '*group referral'* process in place that avoided the need for individual assessment and scrutiny? Their thought that DS Hill was captured by the referral of others flies in the face of the required thorough and specific consideration of each officer that must have been known to them, taught by them and reinforced through continuing training. If they had any doubt they should have sought legal advice. They did not. They assumed they were right. That shows not only incompetence as Mr Bird accepts but incompetence to a high degree. The consequence of their complete failure to grasp the essentials of the referral system was to grant to junior members of staff the powers and privileges of police officers who may have arrested DS Hill, detained him in a police station and searched his home without any lawful justification at all.

73. It is no answer to say the IOPC could have got it right in a few moments or say or that no real harm has been done. Poor performance and behaviour and conduct of this type should not be tolerated. High standards are expected and required. In this case there has been a very significant failing in terms of understanding, training and implementation of the rules and standards. This is a case where the conduct of the IOPC in relation to the seizure of the phone from DS Hill can be categorised as egregious that is outstandingly bad or shocking. The facts of this case demonstrate and reveal a number of significant and alarming failings on the part of the IOPC.

74. In detail the failings are: First, there was ignorance at a high level of the correct legal position. Messrs Beesley, Foxley and Lee with many years' experience and holding

senior positions somehow got to believe there was an alternative basis for investigating police officers that was not only contrary to the legislation but removed any of the necessary checks and balances put in place by Parliament. I find it very difficult to understand how such a mentality came to exist. I can only assume that it was as described namely '*ingrained*' and that the faulty understanding had existed for many years and had not been either identified and remedied or had simply been assumed to be correct.

75. Second, there has been a failure on many levels: (i) There has obviously been a failure in training to ensure the legitimate way to proceed was understood and that it could not be bypassed by another, (ii) There has been a failure in oversight and supervision. In this case the errors are those of senior staff not junior investigators acting on a whim. (iii) There has been a failure to obtain proper legal advice. I am struck by the fact that despite a lawyer being present at meetings and in particular on the 4/4/19 that the issue was not canvassed and corrected. Finally, (iv) there was no system in place to check that the correct procedure had been followed. That may be because it never occurred to anyone that an investigation would be commenced when the correct process had not been followed. These failings can rightly be categorised as systemic.

76. The conduct cannot be described as a simple oversight or incompetence. The failings go to the very heart of the investigation process and the very reason the IOPC exists. There appears to have been a cavalier attitude to the correct process and the law bordering on the arrogant in the sense that available legal advice was not sought. I add of course the failings are on the part of the IOPC, a body established to enforce high standards in the police service. The facts of this case demonstrate and reveal a number of significant and alarming failings on the part of the IOPC. The conduct goes beyond laxity.

77. Poor performance, ignorance, incompetence and system failures of the type exposed by this case cannot be accepted. To order otherwise would be to condone what I regard as unacceptable behaviour that falls into the same category of conduct as identified in *Chatwani* and the other cases. There was, I find, to a significant degree a less than

rigorous and scrupulous approach to the seizure of the applicant's phone given the failings outlined in this case.

78. I therefore deny the respondent the right to use the downloaded material for the purposes of their cross application.

79. I invite counsel to draft the appropriate orders that follow my decision

HHJ Nigel Lickley QC

Central Criminal Court

23/12/20.

INVESTIGATORY POWERS TRIBUNAL

ANNEX B TO JUDGMENT

IPT/20/62/CH

CHRONOLOGY

Date	Event
15 May 2018	Dean Francis is seriously injured when he is hit by a police vehicle (driven by Officer C) during a surveillance operation carried out by a Trident Unit of the Metropolitan Police ("MPS"). Footage of the incident is captured on the personal dash camera belonging to Officer B that was mounted in another police vehicle, not involved in any collision with Dean Francis. The incident is referred to the Independent Office for Police Conduct ("IOPC") as a "death or serious injury matter" ("DST") in accordance with Part 2 and schedule 3 of the Police Reform Act 2002. The IOPC decides that it was necessary to investigate the incident and refer it back to the MPS for a local investigation to be carried out by the MPS Department for Professional Standards ("MPS DPS").
19 May 2018	DS Hill is made aware that there would be a local DPS and traffic investigation into the collision.
31May2018	Email sent from Bhatt Murphy (solicitors for Mr Francis); forwarded to and by DS Hill
4 June 2018	Bhatt Murphy make a complaint to IOPC on behalf of Mr Francis
7 June 2018	DS Hill views footage of the incident (captured on Officer B's personal dash camera) on the 15 May in the office in Wimbledon on a stand-alone computer having obtained a copy from the MPS DPS. DS Hill captures the footage on his personal mobile phone by using the video function to video the screen of the stand-alone computer At 1711 DS Hill sends the footage via WhatsApp to Officer B's mobile phone. Officer B was off duty at the time.

Date	Event
7 June 2018	WhatsApp messages (from Officer B's phone) show: 1528 Officer B asks DS Hill (by WhatsApp) to send "that thing" 1628 Officer B: "Damo any chance of that Vid please" 1711 video sent 1711 Officer B: "Cheers fella appreciate it!!" Officer B forwards the footage to his brother.
6 July 2018	Having considered the complaint made on behalf of Mr Francis and the level of injury sustained, the IOPC (in accordance with paragraph 15, schedule 3, PRA) redetermine the original decision that there should be a local investigation and, instead, decide to conduct an independent investigation into the circumstances surrounding the injury of Dean Francis. This IOPC investigation is called **Operation Irwin.** Operation Irwin is a criminal investigation into the actions of the officers involved in the incident with Dean Francis. This includes allegations of causing serious injury by dangerous driving and perverting the course of justice by colluding in the making of subsequent statements.
13 September 2018	As part of Operation Irwin, work issued and personal mobile telephones are seized from: • Officer A • Officer B • Officer C .The lawfulness or otherwise of these seizures has not been in issue before the IPT. Work begins on forensically downloading and analysing the content.
October 2018	As a result of the ongoing analysis of the content of the seized mobile phones IOPC investigator Nathifa Brewster notifies the (MPS) of potential data breaches by Officers A, B, and C. This includes the sharing via WhatsApp of surveillance and other material including images of individuals against PNC numbers, surveillance videos and photographs, pictures of seized drugs, firearms, cash and operational targets. It is also identified that there are a number of WhatsApp groups that appear to include other officers within the same Trident unit (including DS Hill). Officer B was also identified as having pornographic material on his work issued phone. "By the end of October 2018, the MPS has formally referred the conduct of Officers A, B, and C to the IOPC and the IOPC has decided to begin a second independent investigation (linked to Operation Irwin) into the use of WhatsApp by the Trident Unit". NOTE: This extract is quoted from the chronology prepared by the IOPC for the IPT proceedings. This is called **Operation Trent** (and is still ongoing) Jack Lee is designated as lead investigator. He is supervised by Operations Team Leader (OTL) Steven Foxley.

Date	Event
14 December 2018	IOPC Terms of Reference for Operation Trent are settled.
December 2018	IOPC investigators begin work on a detailed analysis of the mobile phone downloads.
6 February 2019	IOPC investigator Kieran Casserly completes a spreadsheet of all the information shared by WhatsApp by over 50 officers. Work subsequently begins on completing IRs (Investigator Reports) for a number of officers (including DS Hill) to set out what has been shared, with whom and when.
March 2019	Based on the detailed analysis completed to date, the IOPC decides (in consultation with the MPS) to conduct an investigation. Only those officers that appear to have shared operational material for a non-policing purpose would be made subject to a formal investigation. IOPC decides that "cultural issues" around the use of WhatsApp for sharing policing material for a policing purpose are to be dealt with via learning recommendations. A separate learning report relating to the use of WhatsApp to share operational material is subsequently produced by the IOPC in November 2020.
22 March 2019	Meeting held at the IOPC to review the results of the analysis in relation to the individual officers identified to date. Officers identified as being subject to further investigation are: • Officer B • Officer C • DS Hill The decision to make DS Hill a subject of the investigation is based only on the evidence obtained from Officer B's phone that DS Hill made a recording of the footage of the incident involving Dean Francis and sent it to him for “no apparent policing purpose” (which Officer B subsequently forwarded to his brother, although there was no evidence that DS Hill knew or intended that this would be done). It was decided that it was necessary to seize DS Hill's mobile phone. Kieran Casserly is tasked with making an application for communications data relating to DS Hill's mobile phone. This is with a view to ensuring that, given the passage of time, the correct handset is targeted.
22 March 2019	Kieran Casserly sends draft application for communications data to Bruce McDonald (RIPA SPOC in the IOPC Intelligence Unit) to obtain feedback and advice.
26 March 2019	Kieran Casserley makes amendments to the application in line with advice from Bruce McDonald and sends it to OTL Steven Foxley to review.

Date	Event
27 March 2019	Application approved by OTL Steven Foxley. **om Bruce**
28 March 2019	Application under section 22 RIPA authorised by Mike Benbow (at the time IOPC Director for Hillsborough)
End of March - April 2019	Review of all phone data completed (53 separate officers identified by this point).
2 April 2019	Call data received by IOPC Intel Unit from Hutchison 3G. Bruce McDonald raises some further enquiries about the data with Hutchison 3G.
4 April 2019	Meeting held at the IOPC to discuss progress of Ops Irwin and Trent.
30 April 2019	Hutchison call data sent by Bruce McDonald to Kieran Casserly.
1 May 2019	Jack Lee decides to draft a severity assessment for DS Hill. This is part of the procedure under schedule 3 PRA for serving a formal notice of investigation on an officer. It requires the investigator to make an assessment of the seriousness of the alleged conduct. This is done is consultation with the MPS.
8 May 2019	Jack Lee completes severity assessment for DS Hill at the level of Gross Misconduct. It is also decided that DS Hill will be criminally investigated for a potential breach of the DPA only.
17 May 2019	Date on Severity Assessment for DS Hill
21 May 2019	Severity assessments at the level of Gross Misconduct for potential data breaches by Officer B, Officer C, and DS Hill are agreed with the MPS.
22 May 2018	Jack Lee makes the following formal policy decisions: P89 - to request personal mobile phone from DS Hill - either by consent or by arrest P90 - not to arrest initially to obtain phone
End ofMay-18 June 2019	Various unsuccessful attempts made to make arrangements to serve DS Hill with a formal notice of a misconduct investigation and a letter setting out the parallel criminal allegations.
10 June 2019	IOPC Provisional Strategy document for DS Hill
18 June 2019	Jack Lee decides to arrange for DS Hill to be called into a meeting at Jubilee House
18 June 2019	Jack Lee designates IOPC Investigator Kieran Casserly and OTL Correne Alexis to serve DS Hill on Wednesday 19 June 2019. They are provided with a briefing pack.
19 June 2019	Regulation 16 notices and criminal letters served on DS Hill, and Officers B and C.

Date	Event
	Seizure of DS Hill's phone by Kieran Casserly, purportedly under section 19 of PACE. DS Hill declines to provide the PIN. NOTE: DS Hill was not the subject of a separate referral to the IOPC at this point in time. The absence of a formal referral for DS Hill was a key issue in the subsequent litigation under section 59 Criminal Justice and Police Act 2001 referred to in DS Hill's complaint. The IOPC conceded during the litigation that the absence of a referral meant that, under the statutory scheme in the Police Reform Act 2002, the investigators in Operation Trent did not have the powers and privileges of a constable at the time that DS Hill's mobile phone was seized on 19 June 2019. Accordingly, that seizure was unlawful.
3 July 2019	Further regulation 16 Notice served on DS Hill alleging that he hid his phone and lied to IOPC investigators about its whereabouts on 19 June 2019.
19 June 2019- December 2019	Continuing attempts to access DS Hill's mobile phone. DS Hill provided with regular updates.
December 2019	Access gained to DS Hill's phone.
6 January 2020	Jack Lee drafts Digital Examination Request for MPS High Tech Crime Unit to produce proportionate download of DS Hill's phone within specific parameters.
22 January 2020	Forensic download of DS Hill's phone received. In light of ongoing correspondence with solicitors for DS Hill the download was not reviewed.
1 February 2020	IOPC receives pre-action letter from Reynolds Dawson solicitor's on behalf of DS Hill regarding proceedings under section 59 Criminal Justice and Police Act 2001
10 February 2020	IOPC responds to pre-action letter.
17 February 2020	DS Hill files an application under section 59 Criminal Justice and Police Act 200l for his phone to be returned.
2 March 2020	IOPC file response to DS Hill's application
End of March - early April 2020	Jack Lee carries out an administrative review of Operation Trent.
20 April 2020	Jack Lee brings the absence of a referral for DS Hill to attention of OTL Steve Foxley
1 May 2020	Following enquiry by the IOPC MPS confirm that there was no separate conduct matter recorded or referred for DS Hill.
11 May 2020	Recording of a conduct matter and referral to the IOPC by the MPS of a for DS Hill
19 May 2020	DS Hill makes complaint to the Investigatory Powers Tribunal
21 May 2020	Further advice sought regarding the legal consequences of there having been no referral for DS Hill at the time of the mobile phone seizure.
12 June 2020	Advice received

16 June 2020	Decision taken by IOPC Operations Manager Graham Beesley to concede that DS Hill's phone was unlawfully seized. Decision taken to proceed with cross-application under section 59 Criminal Justice and Police Act 2001 to retain phone notwithstanding unlawful seizure on the basis that it is relevant evidence of a criminal offence.
16 June - 2 July 2020	Work undertaken to amend IOPC response to DS Hill's application under section 59 Criminal Justice and Police Act 2001 and draft a letter to the legal representatives of DS Hill (Reynolds Dawson) explaining the basis of the concession.
3 September 2020	HHJ Lickley KC decides to hold a preliminary hearing to determine whether the conduct of the IOPC in unlawfully seizing DS Hill's phone is such that the IOPC should not have the benefit of reviewing the contents of the phone for the purposes of its cross-application.
21-24 September 2020	Preliminary hearing before HHJ Lickley KC The fact that an application was made under RIPA in respect of DS Hill's phone is disclosed to DS Hill, as is a copy of the application.
9-10 December 2020	HHJ Lickley KC hears further oral submissions from the parties on the preliminary issue.
23 December 2020	HHJ Lickley KC hands down ruling on the preliminary issue. IOPC should not have the benefit of viewing the contents ofDS Hill's phone The ruling is initially in private but it is subsequently agreed on 6 January 2021 that the ruling can be made in open court providing the names of the officers still under investigation are anonymised. The RIPA application is directly referred to in the ruling at paragraphs 68 and 69. IOPC withdraws its cross-application under section 59 Criminal Justice and Police Act 2001.
6-7 January 2021	Phone returned to DS Hill and downloaded contents destroyed in accordance with the Court's order.