The Law Commission

Working Paper No. 110

Computer Misuse

HER MAJESTY'S STATIONERY OFFICE

The Law Commission was set up by section 1 of the Law Commissions Act 1965 for the purpose of promoting the reform of the law.

The Law Commissioners are:

The Honourable Mr. Justice Beldam, *Chairman*
Mr. Trevor M. Aldridge
Mr. Brian Davenport, Q.C.
Professor Julian Farrand
Professor Brenda Hoggett

The Secretary of the Law Commission is Mr. Michael Collon and its offices are at Conquest House, 37-38 John Street, Theobalds Road, London, WC1N 2BQ.

This working paper, completed on 11 August 1988, is circulated for comment and criticism only. It does not represent the final views of the Law Commission.

The Law Commission would be grateful for comments before 28 February 1989. All correspondence should be addressed to:

Mr M N Farmer
Law Commission
Conquest House
37-38 John Street
Theobalds Road
London WC1N 2BQ

(Tel: 01-242 0861 Ext. 231
Fax: 01-242 1885)

It may be helpful for the Law Commission, either in discussion with others concerned or in any subsequent recommendations, to be able to refer to and attribute comments submitted in response to this working paper. Whilst any request to treat all, or part, of a response in confidence will, of course, be respected, if no such request is made the Law Commission will assume that the response is not intended to be confidential.

The Law Commission

Working Paper No. 110

Computer Misuse

LONDON

HER MAJESTY'S STATIONERY OFFICE

© *Crown copyright 1988*
First published 1988

ISBN 0 11 730192 2

THE LAW COMMISSION

WORKING PAPER NO. 110

COMPUTER MISUSE

TABLE OF CONTENTS

THE LAW COMMISSION

WORKING PAPER NO. 110

COMPUTER MISUSE

SUMMARY

In this Working Paper, the Law Commission examines a range of activities which might be said to constitute computer misuse, and considers the application of the criminal law in England and Wales to them. The paper concludes that, in general, the present scheme of criminal offences is sufficient to deal with the forms of computer misuse identified. The Commission's provisional view is that a comprehensive computer crime statute is neither necessary nor appropriate here. Only one form of computer misuse might be said to require the creation of a "computer crime": the obtaining of unauthorised access to a computer by "hacking". The paper sets out the arguments for and against the criminalization of such conduct, and considers a range of options for a new offence. The Commission asks whether hacking should be criminalized and, if so, whether it should be an offence along the lines of one of the four options suggested. The purpose of this paper is to obtain the views of the public on the matters considered in it.

THE LAW COMMISSION

WORKING PAPER NO. 110

COMPUTER MISUSE

PART I
INTRODUCTION

A. BACKGROUND

1.1 Computers now play an important part in our everyday lives. This technological development, upon which society is becoming ever more dependent in hundreds of different ways, has without doubt produced substantial benefits for us all. However, alongside these benefits lies the disadvantage that computers and computer systems are vulnerable to all manner of misuse. The consequences of such misuse may be very serious. While in some respects the law has already come to terms with the computer, and has been adapted or shown itself capable of being adapted to take account of it, in other respects it has not. This has led to calls for the law, in particular the criminal law, to be amended and strengthened to ensure that problems arising from the misuse of computers can be more effectively dealt with.

1.2 It is the purpose of this working paper to examine the applicability and effectiveness of the existing law of England and Wales in dealing with instances of computer misuse; and to seek the views of interested persons on what, if any, reform of the criminal law is required.

1.3 Our work on this subject began as part of our review of the common law offence of conspiracy to defraud.[1] However, in relation to computer misuse we confined ourselves there to looking at the issue of computer fraud, by which we meant the dishonest manipulation of a computer in order to obtain money, property or some other advantage of value.[2] It was clear to us that the possible legal implications of the misuse of computers extended well beyond the confines of fraud; and that a wider review was called for which would enable us to examine the effectiveness of our law, both criminal and civil, in relation to conduct involving the misuse of computers and computer systems generally. We therefore embarked on the present study.[3]

1.4 Computer misuse is a subject which has lately received widespread coverage in the media. References to the dangers arising from computer-related frauds, from "hacking" into computer systems by unauthorised persons, from logic bombs, computer viruses and other sinister-sounding devices have become commonplace. For example, in July 1988 it was reported that a potential computer fraud involving the fraudulent transfer of £32 million from a Swiss bank had been thwarted by the police.[4] We note also the recent attention in the press given to the

---

1. We published a consultation paper on this subject last year: Conspiracy to Defraud (1987), Working Paper No. 104. We hope to publish a final report in 1989.

2. See ibid., paras. 4.9 - 4.14 and 10.3 - 10.9.

3. Our progress was delayed so that we could await and take account of the outcome of the Court of Appeal's decision in R v. Gold and Schifreen [1988] Q.B. 1116 (C.A.), a case concerning the question whether computer hacking could amount to the crime of forgery under the Forgery and Counterfeiting Act 1981. The case subsequently went to the House of Lords [1988] 2 W.L.R. 984 (H.L.): see further paras. 3.14 - 3.22 below.

4. The Independent, 6 July 1988.

so-called "Brain" virus which, according to reports,[5] was spreading among IBM-compatible personal computers by means of "infected" disks. The "virus" - a specially written program designed both to replicate itself and to cause damage - was reported as having erased and damaged data files on infected machines. A similar virus apparently infected certain "Amiga" disks in 1987.[6] The authors of the computer programs responsible for the damage appear not to have been located.

B. "COMPUTER CRIME"

1.5 Discussion of computer misuse often reflects concern about the effects of "computer crime". This is a term that we have avoided in this paper, because it appears to us to prejudge the conduct in question.[7] The general criminal law in England and Wales contains no specific offences aimed at computers, but it is of course possible, for example, to steal or unlawfully damage a computer, or to use computers to commit traditional offences. It is also true that activities which are generally lawful, albeit unauthorised, do not become unlawful simply because a computer is involved. For example, as we explain below,[8] it is not a crime to use someone else's lawnmower without their permission, so long as it is returned undamaged. By analogy, it is not an offence to make unauthorised use of a computer.

---

5. See e.g. Sunday Times, 3 April 1988.

6. The Guardian, 19 November 1987.

7. "Computer crime" is also a concept the scope of which is not easy to define: see the discussion in C. Tapper, "'Computer Crime': Scotch Mist?", [1987] Crim.L.R. 4, at pp.5-8.

8. See para. 2.14.

1.6 In considering the question whether the criminal law should be extended to prohibit certain kinds of computer misuse, one important factor will be whether similar activities not involving a computer (but which might be thought analogous) are at present illegal.[9] For example, it is not an offence to obtain unauthorised access to information, and this is a relevant but not necessarily decisive factor in deciding whether "hacking" into a computer should be a crime. If it is felt that hacking (or any other form of computer misuse) should be criminalized, then it is crucial to identify the special harm which such an offence would seek to counter. Such an offence would then accurately be called a "computer crime", because it could only be committed with the aid of a computer.

C. PREPARATION AND STRUCTURE OF THE PAPER

1.7 Our examination of computer misuse has been undertaken against a background of national and international concern about the problem of computer misuse. It has attracted considerable professional interest both here and abroad. In the United Kingdom many large companies and corporations have sought to address the problem within their own organisations. Professional bodies representing, for example, accountants and auditors have set up committees to examine computer misuse. The Audit Commission for Local Authorities in England and Wales published surveys of computer fraud and abuse in 1981, 1984 and 1987. The Scottish Law Commission has recently carried out a review of computer misuse and recommended new legislation.[10] Outside the United Kingdom, following a campaign by the American Bar Association, the USA have introduced federal legislation on

---

9. Some general guidelines relevant to the creation of new criminal offences are considered in para. 1.11 below.

10. See para. 1.8 below.

computer crime. Within Europe the subject is under review by, among others, the Commission of the European Communities and the Council of Europe, and new legislation has recently come into force in Sweden and France. The scope for international co-operation has been examined by the OECD. Further afield, the whole subject has been reviewed by, among others, the Law Reform Commission of Tasmania, and is currently under review in the Commonwealth of Australia and Hong Kong.[11]

1.8 We have derived considerable help in preparing this paper from a number of sources, including many of those just mentioned. We should especially mention in this context the work carried out by the Scottish Law Commission. In 1984 the Commission was asked by the Law Society of Scotland to consider "the applicability and effectiveness of the criminal law of Scotland in relation to the use and abuse of computers, computer systems and other data storing, data processing and telecommunications systems..." Its Consultative Memorandum on this topic was published in March 1986[12] and contained a full analysis of the nature of the problem and of the legal issues involved. This was followed last year by the publication of its final Report.[13] The Commission's main recommendation was for the creation of a specific offence to cover the obtaining of unauthorised access to a computer. We shall be referring to this recommendation, and other aspects of the Scottish Law Commission's review, in more detail later in this paper.

1.9 In Part II, we outline the factual background to the main categories of computer misuse. In Part III, we

---

11. See further Appendix A below.

12. Computer Crime (1986) Consultative Memorandum No. 68.

13. Report on Computer Crime (1987), Scot. Law Com. No. 106.

examine the extent to which the activities described in Part II are at present affected by the existing criminal and civil law in England and Wales. Then in Part IV we turn to consider whether there is a need for a comprehensive computer crime statute, or whether a more limited approach to reform would be satisfactory. Part V sets out our provisional proposal for the reform of the law relating to offences involving the "deception" of a computer. In Part VI we present the arguments for and against the criminalization of hacking and, without reaching a provisional conclusion on that matter, we also discuss the form that a new offence might take. In Part VII we consider the aspects of territorial jurisdiction raised by the paper. Part VIII summarises the main points for consultation. In Appendix A we summarise the approaches to law reform on this subject in other jurisdictions. In Appendix B we raise the question of whether there should be a duty to disclose incidents of computer misuse.

1.10 In this paper we are dealing only with the substantive law relating to computer misuse. We note that the Police and Criminal Evidence Act 1984 makes special provision to deal with computer evidence,[14] but aspects of evidence and procedure are outside the scope of this paper.

D. GUIDELINES FOR THE CREATION OF NEW CRIMINAL OFFENCES

1.11 In our discussion we have taken into account the views expressed by the Home Office, in a consultation document a few years ago,[15] in relation to some guiding principles kept in mind by successive Governments in

---

14. Sect. 69 and Sch. 3, part II.

15. Trespass in Residential Premises (1982), paras. 18 - 20. See also Hansard (H.C.), 21 December 1984, Vol.70, col.365 (written answers).

proposing to Parliament the creation of new criminal offences. These are in summary, first, that the behaviour in question is so serious that it goes beyond what it is proper to deal with on the basis of compensation as between one individual and another and concerns the public interest in general. Secondly, criminal sanctions should be reserved for dealing with undesirable behaviour for which other, less drastic means of control would be ineffective, impracticable or insufficient. This helps to maintain public respect for the criminal law. Thirdly, a new offence should be enforceable. It must therefore be clear in its scope and effect.

E. TERMINOLOGY

1.12 The Scottish Law Commission's Consultative Memorandum on Computer Crime contained a useful summary of the history of the computer and a description of its operations.[16] In this paper we have consciously avoided the use of technical terms wherever possible, but some explanation is desirable at this stage.

1.13 A computer[17] is a device for storing and processing data, by which is meant information of any kind. The data can be stored on magnetic tape or a disk and it is possible to retrieve, alter or add to this information quickly and simply. Furthermore, the computer is able, in response to a set of logical instructions, to sort that data and extract information from it which otherwise would not be apparent. To take one example, if the data in a computer consisted of the personnel files of all the employees in a business, the

---

16. Computer Crime (1986) Consultative Memorandum No. 68, paras. 2.1 - 2.27.

17. For the difficulties in producing an exhaustive definition of a computer, see para. 6.23 below.

computer could be programmed to produce, in response to a single instruction, a list of all the employees above a certain age, or who had worked for the business for more than a certain number of years, or who earned more than a given sum of wages or salary.

1.14 A computer system, of whatever size, consists of three main elements: hardware, system software and application software. In simple terms, the hardware is the visible computer; for example, the cabinet containing the Central Processing Units (C.P.U.'s) which perform the calculations necessary to run the computer, and which are stored on "microchips", the screen or terminal (often a visual display unit - V.D.U.) from which the information can be read, the disks or tapes on which data is stored, and the keyboard by means of which instructions may be entered. Application and system software are the sets of logical instructions (computer programs) which make the computer work. Application software controls the actual tasks required, such as word-processing, stock control or data storage. System software (the operating system) acts as an interpretor between the keyboard and the C.P.U.. In this paper, when we refer to information in a computer, this generally refers both to the data stored, and to the computer programs which regulate the processing of such data.

1.15 Although all computer systems are based on the C.P.U., the size and power of the machine varies from the largest "mainframe", through the minicomputer and down to the basic microcomputer (or personal computer) and now the portable "lap-top" computer. Minicomputers and mainframes usually support several users (sometimes several hundred or more). Each computer terminal can be connected to the central computer, and a network of computer terminals may be linked together within one building, or scattered about the country or overseas and connected through the public

telecommunication system. The usefulness of many computer systems depends on users being able to contact the central computer from remote locations.[18] This brings us to the problem of obtaining access to a computer.

1.16 It is clear from the preceding paragraph that it is not necessary to be physically next to a computer in order to use it. In this paper, therefore, when we use the phrase "obtaining access to a computer" we do not mean the obtaining of physical access thereto.[19] Most computers, other perhaps than those used at home, are protected by some kind of security device, often in the form of a personal identification number and a password, which a user must correctly enter before being allowed to "log on" (obtain access to) the computer. Particular sections of the computer can be further protected with additional passwords. Such security measures are desirable not only where, in relation to computer systems accessible through the public telecommunications system, it is necessary to prevent those without authority from obtaining any access to the system, but also in situations where it is considered that certain users should only be permitted access to certain sections of the computer's stored data.[20]

---

18. This is commonly done by means of a computer terminal, a telephone and a "modem" (a modulator/demodulator device) which connects the terminal to the public telecommunications system and thence to the central computer.

19. The same idea is contained in the verb, "to access" a computer.

20. Additional and more sophisticated security devices are also available, such as "encryption" devices (which scramble signals sent between distant computers) and "dial back" systems (which ensure that access can only take place through an authorised user's telephone). An important recent development is a new kind of microchip which electronically labels every piece of data in a computer system, allowing only authorised users to gain access to it: The Times, 2 August 1988.

PART II

TYPES OF COMPUTER MISUSE

2.1 In this part of the paper we outline the factual background to the main categories of computer misuse.[1] No list could possibly be exhaustive and equally conduct will often fall into more than one of the categories. However, we intend to provide examples of behaviour which might be thought to involve the use of a computer for an unauthorised purpose, or by an unauthorised person (or indeed both), to which reference may be made in our later discussions of the extent to which such activities are at present affected by the criminal law in England and Wales, and the possible need for reform of that law.[2] The activities covered are categorised in this part as follows:

A. Computer fraud

B. Unauthorised obtaining of information from a computer -

1. Computer "hacking"
2. Eavesdropping on a computer
3. Making unauthorised use of computers for personal benefit

---

1. For ease of explanation, a slightly different presentation of the categories is adopted here to that followed later in the paper.

2. It should be remembered that some of the activities discussed in this section are simply examples of conduct which, were a computer not involved, would not be prohibited by the criminal law. See paras. 1.5 - 1.6 above.

C. Unauthorised alteration or destruction of information stored on a computer

D. Denying access to an authorised user

E. Unauthorised removal of information stored on a computer.

A. COMPUTER FRAUD

2.2 By computer fraud we mean conduct which involves the manipulation of a computer, by whatever method, in order dishonestly to obtain money, property or some other advantage of value, or to cause loss. We recognise that attempting to draw a neat boundary around a concept as nebulous as computer-related fraud is an impossible and somewhat barren task. In a society in which computers increasingly deal with financial transactions, many types of behaviour which the criminal law has in the past dealt with under the heads of theft and fraud will nowadays involve a computer system. Labelling all frauds in which information is processed at some stage by a computer as "computer frauds" takes us no further and tends to confuse the issue of whether computers create any new problems for the criminal law.

2.3 Perhaps the most helpful way for present purposes in which to look at computer fraud is that adopted by the Audit Commission of England and Wales: it divided this category of conduct into "input frauds", "output frauds" and "program frauds".

1. Input frauds

2.4 This kind of fraud can be defined as dishonestly entering false data into a computer, or dishonestly

suppressing or amending data as it is keyed in. The Audit Commission's survey[3] found that input fraud was by far the most common type of fraud identified by respondents, probably because it does not require a sophisticated understanding of the computer system. The frauds reported took place in a range of computer systems dealing with purchases and claims, sales and debtors, and the payroll.[4] Two examples may be given.

2.5 A wages clerk[5] operating a payroll system in local government made false entries on timesheets for about 20 manual employees over a lengthy period of time. The extra payments were later split 50/50 between the wages clerk and the particular manual employees. The fraud went on undetected for three years and losses amounted to £54,500. When it was eventually discovered, sixteen people were charged and convicted of conspiracy to defraud; sentences ranged between imprisonment and fines.

2.6 A clerk[6] in a housing benefits department prepared and input fraudulent claims in respect of his brother-in-law. These claims led to £12,000 being paid directly into building society accounts. The clerk transferred to another office and repeated the scheme. The fraud was discovered after an internal audit and the clerk dismissed and prosecuted on twenty counts of theft.[7]

---

3. Survey of Computer Fraud and Abuse, 3rd triennial Report (1987), p.14. This Report is referred to hereafter as "Audit Commission".

4. Ibid., p.15.

5. Ibid., Appendix A, Case 2.

6. Ibid., Appendix A, Case 29.

7. The Report does not reveal the outcome of the case.

2. Output frauds

2.7 Output frauds involve the suppression or alteration of data which emerges from a computer. In the one case reported to the Audit Commission,[8] a finance officer responsible for the collection and control of rents misappropriated funds from these accounts and suppressed the computer balance reports which would have revealed the discrepancies. He was detected when he began altering input data as well. He was prosecuted[9] and sentenced to four years' imprisonment.

3. Program frauds

2.8 The Audit Commission said that, while there was a feeling that a "true" computer fraud must involve the dishonest alteration of a computer program, in practice the evidence suggested that relatively few such frauds actually occur.[10] The Commission noted that few program frauds may be detected because of the skill of the programmers in covering up the fraud, but considered that -[11]

> "... it seems unlikely that the quality of management throughout the international business world is so lacking that regular acts would continue to go unnoticed."

The programmer does have the opportunity to add instructions to a program which will only be activated when a "trigger" occurs,[12] but most computer users are not programmers and

---

8. Appendix A, Case 39.

9. The report does not give details of the charges.

10. Audit Commission, p.16.

11. Ibid.

12. This problem will be discussed further in relation to "computer viruses", para. 2.16 below.

are merely responding to the options which are provided by the computer system. In everyday use it is the ordinary user who has the greater opportunity dishonestly to manipulate a computer by altering the data which is keyed in.

2.9 In an example of a program fraud given by the Audit Commission,[13] two programmers designed a stock accounting system containing a hidden routine which on presentation of a certain password would suppress the volume of sales and thus reduce the liability to VAT payment. No further details are given.

B. UNAUTHORISED OBTAINING OF INFORMATION FROM A COMPUTER

2.10 There are three distinct aspects to this activity. The first is "hacking": the obtaining of unauthorised access to a computer; secondly, there is passive "eavesdropping" on information kept in a computer; and thirdly, there is the situation where computer facilities belonging to another are used for a purpose which causes no direct loss to the owner or legitimate users but which bestows a benefit on the perpetrator.

1. Computer "hacking"

2.11 The activities of computer "hackers" have attracted considerable media attention in recent years. Typically in such reports, the hacker uses a comparatively simple micro-computer coupled to a "modem", which allows him to access the "target" computer via the telephone system. Sometimes, the hacker will already know a password which will let him into the computer system. Otherwise a password will be found by trial and error, perhaps using a program

---

13. Audit Commission, p.17.

which rapidly generates many permutations of letters and numbers: eventually, one will be found which the target computer recognises as a legitimate password.

2.12 Although the computer enthusiast at home is the stereotypical hacker, most of the hacking cases reported to the Audit Commission[14] involved employees obtaining unauthorised access to information stored on their employer's computer. Such cases draw attention to the need for computer systems to be adequately protected by passwords which are regularly changed and the need for controls which record the operations performed on the computer.

2. Eavesdropping on a computer

2.13 The second aspect of the unauthorised obtaining of information involves various forms of passive "eavesdropping". This does not entail the obtaining of access to a computer and does not allow the eavesdropper to control what information is obtained, in the way that a hacker can instruct the machine to display the desired material. The activities envisaged range from the simple reading of information on a screen or print-out, or the removal of print-out with information on it, to more complex techniques of electronic interception. Examples of such methods include "bugging" a telephone wire along which the data is being transmitted, perhaps to another computer or to a remote terminal, and eavesdropping on the electro-magnetic field radiated by a computer screen or the cables leading to the screen: in favourable conditions this radiation can be used to re-create the screen display.

---

14. Cases 71 - 102.

3. Making unauthorised use of computer facilities for personal benefit

2.14 The third aspect of the unauthorised obtaining of access to a computer is where computer facilities belonging to another person are used for a purpose which causes no direct loss to the owner or legitimate users but which bestows a benefit on the perpetrator. In general, the unauthorised use of another's property is not a criminal offence, unless it amounts to theft or criminal damage.[15] In the context of computers, a person who is authorised to use a computer for certain purposes may make illicit use of it for personal, and unauthorised, purposes. The benefit may be as trivial as producing personal letters on a word processor or as serious as providing computer services to outside clients at substantial profit.[16] Where a "mainframe" computer is used it may be the case that even quite substantial operations of this kind will make only imperceptible demands on the processing and data storage capacity of the computer involved, although in certain circumstances a noticeable strain may be placed upon either. The situation may be different where a smaller computer is used. The illicit user of a "micro-computer" or "personal computer" could, by supplying his own disks or tapes (which are the principal way information is stored by such computers), use the machine without impinging on other users

---

15. A common example given is the person who borrows a neighbour's lawnmower without permission. If the lawnmower is returned undamaged, no offence is committed.

16. The Audit Commission noted (p.4) the large number of reported incidents of unauthorised private work, and recognized that a distinction should be drawn between,

> "... instances of 'playing' with the computer and those activities which affect working patterns or are deliberately deceitful."

except, of course, to the extent that such machines can usually only be used by one person at a time.

2.15 A related form of conduct, and one more likely to constitute a criminal offence, is the unauthorised use of commercially provided services. These are usually accessed via the public telecommunications network. Many of these are "data-bases" - such as LEXIS[17] and POLIS[18] - while others provide active services, such as electronic mailboxes or facilities for the processing of data. If a person were able to access such a system without authority, it would be quite possible to use the services it provides without paying for them.

C. UNAUTHORISED ALTERATION OR DESTRUCTION OF INFORMATION STORED ON A COMPUTER

2.16 The alteration of a computer program would usually involve overcoming a number of levels of security or at least having knowledge of special procedures, but it is possible in principle. Other than financial gain,[19] the consequences might include any or all of the following -

(a) the program ceases to run;

(b) the program runs in such a way as to impair the performance of the job it is meant to do or even to impair the running of other programs: for example, a person may introduce a program which by replicating itself consumes

---

17. A computerised legal information service.

18. Parliamentary On-Line Information Service; a computerised means of obtaining access to information contained in Hansard.

19. For which see "Program frauds", paras. 2.8 - 2.9 above.

an enormous proportion of the computer's memory or processing capacity, so causing it to abort other programs or run them very slowly. Such programs are commonly known as "computer virus" programs.

(c) the program runs normally until a "trigger" event takes place. When this trigger is activated the program might cease to operate partially or completely, or run so as to damage other programs. This kind of program is sometimes called a "logic bomb".

2.17 Information in the form of data or a program may be destroyed in several ways. For example, by physically destroying the medium upon which the information is stored, such as a floppy disk; by electronically "wiping" the storage medium clean; or by "corrupting" the storage medium in such a way as to leave it physically undamaged, in that it would be capable of accepting new information, but rendering the information already on it wholly or partly unusable. Placing a powerful magnet next to a floppy disk might well have this effect.

D. DENYING ACCESS TO AN AUTHORISED USER

2.18 There are a number of ways in which a legitimate user may be denied use of computer facilities. A user or operator may be physically prevented from reaching the terminal, for example, by locking a door or obstructing his passage by picketing, or, perhaps, by a withdrawal of labour which results in there being no one available to operate the machine. We do not consider such activities further in this paper. However, unauthorised access to a computer or damage to software may have the same result -

(a) a computer can only handle a finite number of users at any one time. When all its "ports" are in use, attempts to log on will be rejected. Thus, an unauthorised user may obstruct an authorised user merely by occupying a port;

(b) an unauthorised user may, deliberately or otherwise, activate defensive mechanisms in the computer which cause it to shut down a whole or part of its system;

(c) that part of the computer's software which controls access could be altered, for example, so as to change or delete passwords in order to deny access to some or all legitimate users.

E. UNAUTHORISED REMOVAL OF INFORMATION STORED ON A COMPUTER

2.19 This may be achieved either by the physical removal of the device (such as a disk or tape) upon which information is stored, or by electronic means. In the first instance, the taker of the tape may, having copied the program or data stored on it, decide to return it in order to avoid detection. Physically removing the storage medium may not be necessary, however. After accessing the computer, the perpetrator can instruct it to copy a program into the memory of the perpetrator's computer. Certain technical questions arise concerning the extent to which a program copied from one type of computer is intelligible to, or usable by, another type. In principle, however, the remote copying of material is feasible.

PART III

THE SCOPE OF THE PRESENT LAW

3.1 In this part of the paper we shall examine the extent to which the forms of behaviour described in Part II[1] are prohibited by the criminal and civil law of England and Wales. Insofar as this section may be said to outline the scope of the law of "computer crime", the same qualifications are relevant here as were outlined above.[2] Our conclusions are contained in paragraphs 3.64 to 3.71 below.

A. COMPUTER FRAUD

3.2 Earlier,[3] we used the term "computer fraud" to mean the manipulation of a computer in order dishonestly to obtain money, property or some other advantage of value or to cause loss. There are no offences which correspond to the categories of input frauds, output frauds and program frauds because those categories relate to the manner of the commission of offences. The essence of these forms of conduct is similar to, and may be the same as, ordinary theft or fraud committed in some other way. In consequence, the existing offences of theft and fraud can be used to deal with most cases of computer fraud. The following are the main offences which fall for consideration here: theft, obtaining property by deception, false accounting and common law conspiracy to defraud.

---

1. But see para. 2.1, n.1 above.
2. See paras. 1.5 - 1.6.
3. See para. 2.2 above.

1. Theft

3.3 Section 1(1) of the Theft Act 1968 states that a person is guilty of theft -

> "if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it;..."

Theft is punishable on indictment with imprisonment for ten years.[4]

3.4 When a computer is manipulated in order dishonestly to obtain money or other property, a charge of theft or attempted theft will generally lie. Such a charge can be used, for example, in cases of input fraud where false data is entered by someone into a computer in order to obtain payments to which he or she (or another) is not entitled, for theft of money from a cash dispensing machine (ATM) using either a forged cash card or another's card, or for the theft of pre-signed computer cheques.

2. Obtaining property by deception, and other deception offences

3.5 Another possible charge, with the same maximum penalty as for theft, is obtaining property by deception contrary to the Theft Act 1968, section 15 -

> "(1) A person who by any deception dishonestly obtains property belonging to another, with the intention of permanently depriving the other of it,..."

"Deception" is defined in section 15(4) as meaning -

---

4. Theft Act 1968, s.7.

> "... any deception (whether deliberate or reckless) by words or conduct as to fact or as to law, including a deception as to the present intentions of the person using the deception or any other person."

3.6 For the purposes of this offence, the authorities seem to indicate that the deception must operate on the mind of a person. In Davies v. Flackett[5] Bridge J. doubted whether it was possible in law to deceive a machine, although he did not decide the point. However, in Moritz[6] a Crown Court judge ruled that "intent to deceive" (for the purposes of section 38 of the Finance Act 1972) required an intent to deceive a human mind and that, given the computer-assisted nature of the processing of VAT returns, there was in that case no satisfactory evidence to put to a jury that an admittedly false VAT return which had secured unwarranted repayments had been intended to "deceive" in the required sense.[7] The deception element in the offence under section 15 may therefore cause similar difficulty where a computer is manipulated in order to obtain property (for example, money) and no human mind is deceived. In these circumstances it is probable that a charge of this offence will fail. On the other hand, there are likely to be many cases of computer fraud where it will be possible to say that a person has been deceived and also that there is a causal connection between the deception and the advantage

---

5. [1973] R.T.R. 8.

6. (1981) unreported, Acton Crown Court, Judge Feinstein.

7. The gap which this case revealed has since been filled by s.12(5) of the Finance Act 1985 which amended s.39 of the Value Added Tax Act 1983 so as to define "intend to deceive" in terms of an "intent to secure that a machine will respond to the document as if it were a true document": see also para. 5.2 below.

obtained.[8] If, for example, the fraud depends upon the generation of false output from a computer which will then be acted upon by someone, the problem will not arise because the person reading the output may be deceived.

3.7 The Theft Acts contain a number of other fraud offences which require proof of deception, in particular obtaining a pecuniary advantage,[9] obtaining services,[10] evasion of liability,[11] and procuring the execution of a valuable security.[12] The fact that a computer cannot be the victim of a deception in law is a limitation on the scope of these offences too.

3. False accounting

3.8 Section 17(1) of the Theft Act 1968 creates two offences, penalising anyone who -

---

8. In Thompson [1984] 1 W.L.R. 962, for example, the defendant computer operator, while working in a bank in Kuwait, programmed the bank's computer to debit accounts belonging to customers and credit corresponding amounts to accounts in his own name. After returning to England, he wrote to the Kuwaiti bank and asked for the credit balances on those accounts to be transferred to his accounts in England. He was charged under section 15 with obtaining property from the bank by deception, in respect of the letters asking for the sums to be transferred. The Court of Appeal rejected the defence's argument that the obtaining had already taken place in Kuwait; it was the officers of the bank who read and acted upon the letters who were deceived, and not the computer in acting upon the instructions in the computer program to alter the various account balances.

9. Theft Act 1968, s.16.

10. Theft Act 1978, s.1: see para. 3.34 below.

11. Theft Act 1978, s.2.

12. Theft Act 1968, s.20(2).

"(a) destroys, defaces, conceals or falsifies any account or any record or document made or required for any accounting purpose; or

(b) in furnishing information for any purpose produces or makes use of any account, or any such record or document as aforesaid, which to his knowledge is or may be misleading, false or deceptive in a material particular;"

in each case there must be proved to be dishonesty and either an intent to gain for himself or another or to cause loss to another. Both offences are punishable on conviction on indictment with seven years' imprisonment. The falsifying of accounts may be done in order to conceal the fact that an offence, such as theft, has taken place, but it may be difficult to identify the precise nature of the crime which is being concealed. The falsifying may itself be an integral part of a fraud, for example, an act of preparation for a fraud yet to be carried out. The use of a false or deceptive account may be an attempt to commit another offence involving dishonesty. Section 17 supplements both offences of theft and deception as well as offences of forgery.

3.9 In our view, these offences are capable of covering a wide range of activities related to computers. Information held on a computer could clearly constitute a "record" for the purposes of section 17 and the principal limitation upon the application of this section to any form of tampering with computerised records, whether it be by altering input or output or by reprogramming to produce the effects mentioned in the section, is that the record in question be "made or required for any accounting purpose". However, the record need not be exclusively for such a purpose and the cases[13] suggest that the section will not be too narrowly

---

13. For example, Mallett (1978) 66 Cr.App.R. 239.

defined.

4. Conspiracy to defraud

3.10 Conspiracy to defraud is a common law offence, the essence of which is -[14]

> "... an agreement by two or more by dishonesty to deprive a person of something which is his or to which he is or would be or might be entitled [or] an agreement by two or more by dishonesty to injure some proprietary right of his..."

It is thus very broadly defined and makes possible the prosecution of a wide range of fraudulent conduct where two or more persons are involved.[15] The offence is triable only on indictment and is punishable with a maximum penalty of ten years' imprisonment.[16] Its use therefore tends to be limited to the more serious cases of fraud.

3.11 From the point of view of its usefulness in relation to cases of computer fraud, one significant feature of conspiracy to defraud is the absence of any requirement

---

14. Scott v. Metropolitan Police Commissioner [1975] A.C. 819, at p.840 per Viscount Dilhorne.

15. The offence was recently given a new lease of life by the Criminal Justice Act 1987, s.12. This provision has the effect of reversing the decision of the House of Lords in Ayres [1984] A.C. 447 and removes the limitation that a person could not be guilty of conspiracy to defraud if his conduct might also have amounted to, or involved, the commission of a statutory conspiracy contrary to s.1 of the Criminal Law Act 1977 or some other substantive offence. The common law offence is currently under review by the Commission: see (1987) Working Paper No. 104, Conspiracy to Defraud and para. 5.7 below.

16. Criminal Justice Act 1987, s.12(3).

of proof of deception or an intent to deceive.[17] The problem which we saw[18] may arise in connection with the deception offences is therefore avoided in the case of this offence. If two or more people agree by dishonest means to cause loss to another (for example, by obtaining property from them or valuable services) and their conduct involves or may involve the "deception" of a computer to achieve their objective, a charge of conspiracy to defraud could be brought against them.

B. OBTAINING UNAUTHORISED ACCESS TO A COMPUTER

3.12 The law on this subject will be treated under three heads: first, obtaining unauthorised access to a computer by "hacking"; secondly, obtaining information by eavesdropping on a computer; and thirdly, using computer time or services for unauthorised private work. These areas may not be mutually exclusive and may overlap with, for example, the discussion in the section below headed "Unauthorised alteration or erasure of data or software".[19] Finally, it should be mentioned here that the Data Protection Act 1984 provides a limited range of criminal sanctions which may, in certain circumstances, extend to persons who hold personal data obtained by hacking into a computer. Discussion of this subject is deferred until we consider the 1984 Act below.[20]

---

17. See Scott v. Metropolitan Police Commissioner [1975] A.C. 819.

18. See para. 3.6 above.

19. See paras. 3.35 - 3.40 below.

20. Paras. 3.49 - 3.60.

1. Hacking

3.13 For the purpose of examining the position in criminal law in relation to the obtaining of unauthorised access to a computer ("hacking"), five offences are considered as follows: forgery, abstraction of electricity, criminal damage, the interception of communications and the improper use of a public telecommunication system.

(a) Forgery

3.14 A recent decision of the House of Lords, which upheld the judgment of the Court of Appeal (Criminal Division), has made it clear that forgery is not an appropriate charge to deal with hacking.[21] Nevertheless, in the light of the interest aroused by this case, it seems desirable to explore the basis for the decision.

3.15 On 24 April 1986, two "hackers" who obtained access to British Telecom's "Prestel" computers, using passwords they were not entitled to use, were convicted at Southwark Crown Court of a number of offences under the Forgery and Counterfeiting Act 1981. The defendants, Robert Schifreen and Stephen Gold, appealed to the Court of Appeal (Criminal Division) and on 17 July 1987 their appeals were allowed and their convictions quashed.[22] On 31 July 1987 the Court of Appeal, on the application of the prosecution, certified that several points of law of general public importance were involved in its decision to allow the appeals, but refused leave to appeal to the House of Lords. On 16 November, the House of Lords gave leave to appeal. The case was argued

---

21. R v. Gold and Schifreen [1988] 2 W.L.R. 984 (H.L.).

22. R v. Gold and Schifreen [1988] Q.B. 1116.

before the House of Lords on 4 and 5 February 1988 and on the 21 April the House unanimously agreed that the appeal should be dismissed; the main speech was delivered by Lord Brandon.

3.16 To understand the nature of the charges against Gold and Schifreen it is necessary to examine the operations which go on within the Prestel computers when a user attempts to access them. Each user of Prestel has his or her own micro-computer, with a keyboard and a monitor (like a television screen). First, the user is connected to the computer via the public telephone system. Once connected, the Prestel computer displays on the user's monitor a "logging frame", which requests the user to type into the keyboard his or her "customer identification number" (or C.I.N.). When the user does this, the number is passed down the telephone line in the form of electronic impulses to the Prestel computer where it passes into an area of the computer called the "user segment". The user segment is itself divided into three areas: the input buffer, the control area, and the output buffer. The user's C.I.N. is received in the input buffer, from where it is immediately passed into the control area, where it is retained for so long as it takes for the computer to compare it with its store of valid C.I.N.'s. If it achieves a match, the computer proceeds to request from the user a password which is compared with its store of valid passwords in a similar manner. If the password is also matched, access is allowed; otherwise the computer denies access. When this procedure is completed, the record of the C.I.N. and the password as entered by the user is deleted from the user segment.

3.17 It was common ground at the trial that Gold and Schifreen had each gained access to the Prestel computers on numerous occasions using the C.I.N.'s and passwords of others without their permission. They had obtained information to which they were not entitled, altered data

stored on the network and caused charges to be made to account holders without their knowledge or consent. However, Lord Brandon said that -[23]

> "The [defendants'] object in carrying on these activities was not so much to gain any profit for themselves as to demonstrate their skill as 'hackers'."

3.18 The defendants were convicted on an indictment which contained nine specimen counts of forgery, five against Schifreen and four against Gold, alleging that the respondent concerned had, on certain dates in respect of a particular computer,

> "... made a false instrument namely a device on or in which information is recorded or stored by electronic means with the intention of using it to induce the Prestel Computer to accept it as genuine and by reason of so accepting it to do an act to the prejudice of British Telecommunications Plc."

Section 1 of the Forgery and Counterfeiting Act 1981 provides that -

> "A person is guilty of forgery if he makes a false instrument, with the intention that he or another shall use it to induce somebody to accept it as genuine, and by reason of so accepting it to do or not to do some act to his own or any other person's detriment".

3.19 It is possible that some confusion arose at the trial as to whether it was the electronic impulses sent by the user to the Prestel computer, or the user segment of the Prestel computer itself, which was relied upon by the prosecution as constituting the "false instrument" made by the accused. The matter was apparently not dealt with specifically at the trial during the technical evidence

---

23. [1988] 2 W.L.R. 984, 987.

presented by the prosecutor. During final submissions at the close of the Crown's case the trial judge asked prosecuting counsel what the instrument was, and he replied "the user segment".[24]

3.20 An "instrument" is defined by section 8(1) of the 1981 Act, which (so far as is relevant) reads as follows -

> "... in this Part of this Act 'instrument' means...
>
> (d) any disc, tape, soundtrack or other device on or in which information is recorded or stored by mechanical, electronic or other means."

Before the House of Lords, it was conceded by the Crown that electronic impulses could not be an "instrument" for the purposes of the Act.[25] This left the argument that the user segment was an instrument for these purposes. The case for the Crown was explained by Lord Brandon in the course of his speech as follows -[26]

> "The relevant instrument was the control area of the user segment of the relevant Prestel computer whilst it had recorded and/or stored within it the electronic impulses purporting to be a C.I.N. and a password. That control area of the user segment consisted of semi-conductor chips and/or magnetic cores, either or both of which are devices 'on or in which information is recorded or stored by... electronic means' within the meaning of section 8(1)(d) of the Act. Such an instrument was made by each respondent when he keyed into the control area of the user segment through a telephone line the electronic impulses which constituted the C.I.N. and the password."

---

24. Ibid., p.988.

25. Ibid., p.990.

26. Ibid.

3.21 Lord Brandon rejected the Crown's argument on the ground that, in order to meet the definition of an instrument in section 8(1)(d) of the 1981 Act, information must be "recorded" or "stored" on or in a disk, tape, soundtrack or other device. To give effect to the everyday meaning of "recorded" or "stored", the information must be held first, for an appreciable time and, secondly, with the object of subsequent retrieval or recovery. Furthermore, this natural reading was the intended meaning of the Act in relation to information stored or recorded on a disc, tape or soundtrack. His Lordship accepted the case for Gold and Schifreen that -[27]

> "The process relied on by the Crown involved no more than the C.I.N. and the password being held momentarily in the control area of the user segment while the checking of them was carried out, and then being totally and irretrievably expunged. The process did not, therefore, amount to the recording or storage of the C.I.N. and the password within the meaning of section 8(1)(d)."

Having concluded that the respondents had not made an instrument as defined in section 8(1) of the 1981 Act, it was unnecessary for Lord Brandon to consider whether, if they had done so, the instruments would have been "false instruments" as defined in section 9(1) of the Act. In reaching this conclusion, he said -[28]

> "Moreover, I share the view of the Court of Appeal (Criminal Division), as expressed by Lord Lane C.J., that there is no reason to regret the failure of what he aptly described as the Procrustean attempt to force the facts of the present case into the language of an Act not designed to fit them."

---

27. Ibid.

28. Ibid., p.991.

3.22 The robust rejection by the Court of Appeal (Criminal Division) and the House of Lords of forgery as an appropriate charge to deal with hackers appears to leave no possibility of the future use of this offence in such cases. Other criminal offences were not, however, considered. Nor were the courts asked to consider whether the defendants might have been liable in any civil proceedings for breach of confidence in respect of any confidential information to which they had obtained access and later revealed.[29]

(b) Abstraction of electricity

3.23 Section 13 of the Theft Act 1968 creates the offence of abstracting electricity. It provides -

> "A person who dishonestly uses without due authority, or dishonestly causes to be wasted or diverted, any electricity shall on conviction on indictment be liable to imprisonment for a term not exceeding five years."

3.24 The operation of a computer consumes electricity. Any unauthorised accessing of a computer would therefore seem to constitute the actus reus of this offence, although in some cases a jury (or magistrates) may decline to find that a hacker was "dishonest".[30]

3.25 One problem raised by charging a hacker under section 13 might be that of proving that electricity has been used. Each operation carried out by the computer uses a minute quantity of electricity and, where the computer in

---

29. See paras. 3.61 - 3.63 below.

30. The partial definition of dishonesty provided by the Theft Act 1968, s.2 does not apply to the offence under s.13 (see s.1(3)). For the general test of dishonesty see further Ghosh [1982] Q.B. 1053; E. Griew, The Theft Acts 1968 and 1978, 5th ed. (1986), paras. 2-99 - 2-114.

question is used by many users at the same time, it would probably be impossible to quantify the electricity consumed by an unauthorised user in isolation from that consumed by other, authorised users.[31] However, perhaps the major objection to such a charge being brought is its apparent artificiality: the mischief it seeks to counter, unauthorised access, is patently divorced from the substance of the charge, namely the abstraction of a trivial quantity of electricity.[32]

(c) Criminal damage

3.26 Section 1(1) of the Criminal Damage Act 1971 provides that -

> "A person who without lawful excuse destroys or damages any property belonging to another intending to destroy or damage any such property or being reckless as to whether any such property would be destroyed or damaged shall be guilty of an offence."

---

31. Attention was drawn to this problem in papers sent to us by the D.P.P.'s office in 1980 concerning a case in which an employee of a local authority had made considerable private profits by providing computer services for clients, using the local authority's computer. The D.P.P.'s office acknowledged the existence of this problem but did not regard it as an absolute bar to a charge under s.13.

32. In Hong Kong in 1984, a computer technician who, out of curiosity, gained unauthorised access to private and confidential information stored in an electronic mail box data system, was convicted of abstracting electricity worth less than one eighth of a Hong Kong cent (contrary to a Theft Ordinance provision which is, in relevant respects, the same as s.13 of the Theft Act 1968). But in view of the small amount of electricity involved, the magistrate discharged the defendant unconditionally and ordered that no conviction be recorded, adding that the prosecution should never have been brought: R v. Siu Tak-Chee (unreported), noted in "Computer Misuse", Law Reform Commission of Tasmania Report No. 47 (1986), para. 7(ii).

The offence is triable either way and is punishable on indictment with imprisonment for ten years.[33]

3.27 The applicability of a charge of criminal damage to the acts of a hacker is dependent on the resolution of two preliminary problems. First, the definition of "property" in the 1971 Act and, secondly, the meaning of "destroy or damage". The Divisional Court in Cox v. Riley[34] decided that the erasure of computer programs stored on a plastic circuit card amounted to damage of the plastic circuit card. It may be that, in cases such as Gold and Schifreen where the hacker in addition to gaining unauthorised access to a computer, intentionally or recklessly makes unauthorised alterations to stored data,[35] the hacker may be guilty of criminal damage to the medium on which the data is stored. These arguments will be considered below. It seems certain, however, that criminal damage will not be committed if the hacker merely obtains unauthorised information stored in a computer and does not attempt to alter or destroy that information nor does anything which in fact has that effect.

(d) Interception of communications

3.28 The Interception of Communications Act 1985 provides that it is a criminal offence intentionally to intercept a communication in the course of its transmission

---

33. Sect.4. Criminal damage of property valued at less than £2,000 is a summary offence, see Criminal Justice Act 1988, s.38.

34. Cox v. Riley (1986) 83 Cr.App.R. 54. The facts of this case and a discussion of its implications can be found in Section C "Unauthorised alteration or erasure of data or software", paras. 3.35 - 3.40 below.

35. Gold and Schifreen intentionally made such alterations: see [1988] 2 W.L.R. 984, 987.

by means of a public telecommunication system.[36] A telecommunication system is defined so as to include its use for the transmission of data,[37] and a public telecommunication system is defined as any system which is so designated by order of the Secretary of State.[38] The main limitation on the application of this offence to hacking is that it applies to the interception of a communication and not to the unauthorised initiation of a message to a computer system. It will therefore seldom be an appropriate charge to deal with such conduct.[39]

(e) Improper use of a public telecommunication system

3.29 Certain forms of unauthorised access activities may fall within the offence of improper use of a public telecommunication system. Section 43(1) of the Telecommunications Act 1984 provides that a person who -

> "(a) sends, by means of a public telecommunication system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or

---

36. Sect.1(1). The offence is punishable, on summary conviction, with a fine of up to £2,000, and on indictment with a fine or two years' imprisonment or both. The offence is not committed if the interception is carried out under a warrant issued by the Home Secretary or if the interceptor has reasonable grounds for believing that the person to whom or by whom the communication was sent has consented to the interception (s.1(2)). In addition, no offence is committed if the interception is for purposes connected with the provision of public telecommunication services (s.1(3)).

37. Interception of Communications Act 1985, s.10 read with the Telecommunications Act 1984, s.4(1)(c).

38. Telecommunications Act 1984, s.9(1).

39. The application of this offence to "eavesdropping" on a computer is considered in para. 3.30 below.

(b) sends by those means, for the purpose of causing annoyance, inconvenience or needless anxiety to another, a message that he knows to be false or persistently makes use for that purpose of a public telecommunication system..."

is guilty of an offence.[40] In relation to hacking, the fact that the offence is restricted to public telecommunication systems[41] means that, where such conduct takes place between terminals linked to the computer by some other method (such as a closed system of wiring within an office), this offence is not applicable.

2. Eavesdropping on a computer

3.30 The offence created by section 1 of the Interception of Communications Act 1985 covers those forms of eavesdropping on computer communications which involve "tapping" the wires along which messages are being passed. One problem which may arise, however, is the question of whether the communication in question was intercepted in the course of its transmission by means of a public telecommunication system. It is technically possible to intercept a communication at several stages in its transmission, and it may be a question of fact to decide the stage at which it enters the "public" realm.

3.31 There are also forms of eavesdropping which the Act does not cover. For example, eavesdropping on a V.D.U. screen by monitoring the radiation field which surrounds it in order to display whatever appears on the legitimate user's screen on the eavesdropper's screen. This activity would not seem to constitute any criminal offence (unless

---

40. Punishable on summary conviction with a fine not exceeding level 3 on the standard scale (£400).

41. See para. 3.28 above.

the information gained was specially protected under, for example, the Official Secrets Act 1911). Whether any civil liability could be shown is discussed further below.[42]

3.32 In our view computer eavesdropping raises the same issues as any other form of unauthorised surveillance. Such conduct does not generally involve the commission of a criminal offence, and it is beyond the scope of this paper to consider whether it should. However, we do recognise that it is possible to regard computer eavesdropping as a form of obtaining unauthorised access to a computer, even though the eavesdropper will not be able to control the information which is obtained. Later in the paper, therefore, when we examine proposals to reform the law to cover computer hacking, we shall consider the possibility that such reform might affect certain kinds of unauthorised surveillance of a computer, and try to retain a distinction between the two forms of conduct.[43]

3. Using a computer for unauthorised private purposes

3.33 The criminal law at present makes no special provision in relation to the use of another's property for unauthorised private purposes.[44] Various fraud offences might be relevant, but where the relationship between the computer user and the computer owner is one of employer and employee, as in many of the illustrations given by the Audit Commission,[45] the matter can usually be dealt with by internal disciplinary procedures, in the absence of theft or fraud.

3.34 We should perhaps mention here one further

---

42. See paras. 3.61 - 3.63.

43. See para. 6.22 below.

44. See para. 2.14 above.

45. Ibid.

limit[46] on the application of the offence of obtaining services by deception, contrary to section 1 of the Theft Act 1978, to the case[47] where an authorised user of a computer (usually an employee) uses the computer in order to perform private tasks. Obtaining services by deception will seldom be applicable because the Theft Act 1978 requires (section 1(2)) that, in addition to the service being obtained by deception, the service obtained must be provided on the understanding that it has been or will be paid for. The requirement is clearly satisfied where the deceiver gains access to a commercial computer service, such as one of the numerous on-line data bases now available.[48] However, the offence could never be committed where the computer concerned is "private", in that its owner never offers its services to others for payment. This will be the case where the computer is operated purely for the purposes of the company or organisation which owns it.[49]

C. UNAUTHORISED ALTERATION OR ERASURE OF DATA OR SOFTWARE

3.35 A recent decision of the Divisional Court concerning the application of the Criminal Damage Act 1971 to cases of damage to computer software has, it is suggested, resolved many of the questions which arise in

---

46. This limit arises independently of that presented by the present meaning of "deception"; see paras. 3.5 - 3.7 above.

47. Discussed in para. 2.14 above.

48. An agreement to make unauthorised use of a computer or computer services with intent to avoid paying for them, where the services are provided to legitimate users on a commercial basis might constitute conspiracy to defraud. See paras. 3.10 - 3.11 above.

49. A similar limitation would apply to a charge of fraudulent use of a telecommunication system, contrary to s.42 of the Telecommunications Act 1984. Sect.42 states that a person who dishonestly obtains a service provided by a licensed telecommunications system with intent to avoid payment of any charge applicable commits an offence.

this area. In essence, any interference with the operation of a computer or its software which causes loss or inconvenience to its legitimate users can probably now be charged as criminal damage. The case is that of Cox v. Riley[50] in which the defendant was convicted in the magistrates' court of criminal damage, contrary to section 1(1) of the Criminal Damage Act 1971, to a plastic circuit card which was used in a computer-operated saw owned by the defendant's employers. When the card was inserted in the machine and one of the programs selected, the program caused the saw to cut a certain shape. Without the programs on it, the card was useless (although it could be reprogrammed) and the saw operable only manually, which was very inefficient.[51] The defendant erased the programs by operating the saw's "program cancellation facility".

3.36 The defendant appealed to the Divisional Court by way of case stated. The question posed for the Court was: "Can the erasing of a program for a printed circuit card which is used to operate a computerised saw constitute damage within the meaning of the Criminal Damage Act 1971?" The Divisional Court answered the question in the affirmative and upheld the conviction. The Court held that the erasure of the programs damaged the printed circuit card;[52] the card was of no use without the programs stored

---

50. (1986) 83 Cr.App.R. 54.

51. The card was alleged to be damaged to the value of £620; presumably this was the cost of reprogramming the card.

52. The magistrates' court had also reached its decision on this basis. It would have been open to the Divisional Court to have found that it was the saw itself that was damaged, on the ground that the erasure of the program temporarily rendered it inoperable. In Fisher (1865) L.R. 1 C.C.R. 7, Pollock C.B., giving the judgment of the Court for Crown Cases Reserved, held that the temporary disabling of an agricultural steam-engine by a disgruntled employee amounted to malicious damage, because two hours labour was required to repair it. The Divisional Court considered this authority, but reached its decision on the basis that the circuit card had been deliberately damaged.

on it and reprogramming it would require, "... time and effort of a more than minimal nature."[53]

3.37 On this reasoning, a person can be convicted of damaging a computer program even though the program itself is not "property" within the meaning of section 10 of the Criminal Damage Act 1971, which states (so far as is relevant) -

> "In this Act, 'property' means property of a tangible nature..."

The program itself is intangible but, so long as the defendant is charged with causing damage to some tangible part of the computer's hardware on which the information is stored - such as a "floppy disk", or magnetic tape - then, it seems clear, he can be convicted of damage to that hardware if he deletes or alters a program.[54]

3.38 Whether damage is done with the requisite mental element is a question of fact and degree in all the circumstances. In Henderson and Batley[55] Cantley J.,

---

53. Cox v. Riley (1986) 83 Cr.App.R. 54, at p.56.

54. If the Divisional Court had based its decision on the damage done to the saw (by analogy with Fisher (1865) L.R. 1 C.C.R. 7, see para. 3.36, n.52 above), it would have limited the offence to circumstances in which the operation of the computer was impaired in some way. In cases where the operation of the computer is impaired, it would be open to the prosecution, it is suggested, to charge the offence on the basis of damage to the computer, if that were more appropriate in the circumstances.

55. Henderson and Batley (unreported) 29.11.84 (C.A.).

giving the judgment of the Court of Appeal (Criminal Division), noted that the dictionary definition of "damage" was "injury impairing value or usefulness". This definition does not suggest that damage be permanent, and the decision in Cox v. Riley seems to confirm that, if an erasure or alteration of stored data requires the expenditure of more than a minimal amount of effort in restoring the program to its original state, that is sufficient to constitute damage.[56] Our provisional view is that this reasoning is correct and in accordance with the wide meaning which damage was intended to bear.[57]

3.39 The Criminal Damage Act 1971 may also apply in certain cases where access is denied to legitimate users by alterations to the computer system. It is perhaps less clear whether the Act applies where the defendant deliberately or recklessly activates security measures in a computer which cause it to shut down, wholly or partly, or impair its operation in some other way when unauthorised acts are attempted. It is clear, however, that if a person (acting without authorisation) inadvertently causes, for example, the computer terminal on which he or she is working

---

56. Smith and Hogan suggest (Criminal Law, 6th ed. (1988), p.678) that damage is, "... some physical harm, impairment or deterioration which can be perceived by the senses." If the reasoning in Cox v. Riley is correct, this qualification should be removed. For the applicability of criminal damage to hacking, see para. 3.27 above.

57. The Law Commission considered ((1969) Working Paper No. 23, Malicious Damage, para. 17) that the offence should encompass "... destruction or damage to tangible property (in the widest sense)".

to shut down, this will not be criminal damage.[58]

3.40 There are two ways to look at the case where a defendant deliberately or recklessly activates computer security measures. The first is to say that the defendant has done no more than to cause the computer to do what its owner intended it should do when "attacked". Thus, on this argument, it is false to say that "damage" has occurred, since any loss or inconvenience which occurs must be taken to have been foreseen, and the risk of its occurrence accepted, by the owner when installing the protective measures. The alternative argument is that the computer is clearly "damaged" because its operation is impaired, albeit that that impairment has been brought about by in-built procedures. What is important, this second argument proceeds, is that the defendant deliberately initiated those procedures in order to impair the computer's operation or, at least, was reckless as to that result. We consider that, in the light of the broad meaning given to "damage" in the authorities discussed above, deliberately or recklessly impairing the operation of a computer in this way would constitute criminal damage under the present law.

D. UNAUTHORISED COPYING OF DATA OR SOFTWARE

3.41 Two aspects of this problem are dealt with here: first, the temporary physical removal of items such as tapes and disks on which data or information is stored, in order

---

58. The Audit Commission, Survey of Computer Fraud and Abuse (1987), reports one case in which three unsuccessful attempts to gain unauthorised access to a computer via a terminal resulted in the disabling of that terminal. The possibility of unauthorised access to a computer causing inadvertent damage is discussed as a possible justification for a criminal offence of hacking in paras. 6.11 and 6.18 below.

that such data or information may be copied. Secondly, the electronic copying of data or software. Both aspects fall within the law relating to intellectual property and the infringement of copyright. This area of the law, involving consideration of the complex subject of so-called "software piracy" - the unauthorised copying of computer programs - is currently before Parliament in connection with the reform of copyright law.[59] However, it is sometimes suggested that the temporary removal of a disk or tape in order to copy the information stored on it, or indeed the process of copying itself, amounts or should amount to the theft of the information. We consider these arguments briefly but conclude that such conduct does not at present constitute theft and, in view of the fact that the issues of temporary borrowing and property rights in information involve questions far beyond the subject of computer misuse, we do not consider the general arguments for reform in this paper.

1. Temporary physical removal

3.42 On the basis of a recent decision of the Court of Appeal, it seems that the unauthorised temporary borrowing of a computer tape or disk in order to copy the program stored on it does not amount to theft of the tape or disk. The case was Lloyd,[60] in which a cinema projectionist temporarily removed a number of feature films from the cinema at which he worked in order that two other defendants could copy the films onto a master video tape, so that "pirate" copies could be made and sold. Each film was only out of the cinema for a few hours; it was always returned in time for the advertised performance.

---

59. Copyright, Designs and Patents Bill 1988, discussed briefly in para. 3.48 below.

60. [1985] Q.B. 829.

3.43 The three defendants were tried and convicted of conspiring to steal feature films.[61] The Court of Appeal held that, notwithstanding section 6(1) of the Theft Act 1968,[62] a temporary "borrowing" could only be regarded as amounting to permanent deprivation if -[63]

> "... the intention is to return the 'thing' in such a changed state that it can truly be said that all its goodness or virtue had gone:"

Such a case, the Court suggested, would be the taking of torch batteries intending to return them only when their power was exhausted. In Lloyd, although the borrowing "grossly and adversely" prejudiced the commercial interests of the owners of the copyright in the film, the film itself remained unharmed and its value undiminished.[64] The Court therefore allowed the appeal and quashed the convictions.

3.44 Applying this reasoning to the temporary borrowing of a disk on which a computer program is stored, such conduct would seldom amount to theft because, if the computer program is returned, it is unlikely that the copying of the program will have removed all the virtue from it. The original would be usable and, unless the copier had flooded the market with so many copies that it was no longer

---

61. Contrary to s.1(1) of the Criminal Law Act 1977.

62. Which provides that a person temporarily borrowing an item is to be regarded as having the intention permanently to deprive its owner of it, "... if, but only if, the borrowing... is for a period and in circumstances making it equivalent to an outright taking or disposal."

63. Lloyd [1985] Q.B. 829, 836, per Lord Lane C.J..

64. Ibid., p.837.

possible to sell the program at all, the program would retain some, albeit reduced, commercial value.[65]

2. Electronic copying

(a) Unauthorised copying under the Theft Act 1968

3.45 Where there is no physical removal of the medium on which data or programs are stored, but merely an unauthorised copying, two particular elements must be proved in order to obtain a conviction for theft. First, whether the data or programs can be regarded as "property" for the purpose of theft and, secondly, whether the data or programs can be appropriated with the intention of permanently depriving the owner of them.

3.46 In Oxford v. Moss,[66] the Divisional Court ruled that information was not property for the purposes of theft.[67] The defendant, Mr Moss, a student at Liverpool University, had acquired the proof of an examination paper which he was due to sit a month later. He borrowed the paper in order to obtain advance knowledge of the questions set, hoping to return it undetected. It was contended by the prosecutor that he had stolen intangible property belonging to the University, that is to say, the confidential information contained in the question paper. The charge was dismissed by the stipendiary magistrate and, on the prosecutor's appeal by way of case stated, the Divisional Court agreed that confidential information was not a form of intangible property within the meaning of

---

65. See G. Williams, Textbook of Criminal Law, 2nd ed. (1983), p.718.

66. (1978) 68 Cr.App.R. 183. See also Professor J.C. Smith's commentary: [1978] Crim.L.R. 120.

67. By s.4(1) of the Theft Act 1968, property is defined for the purposes of theft as including, "... money and all other property, real or personal, including things in action and other intangible property."

section 4(1) of the Theft Act 1968 and therefore could not be stolen.

3.47 It is possible that a distinction could be drawn between confidential information, which cannot be stolen, and data or programs. However, the debate on whether information is capable of being property, other than in the special forms governed by intellectual property law, and the consequences which such a view would have, is a question far beyond the scope of this paper.[68] For our purposes, it is sufficient to note that, even assuming that information or data is property for the purpose of section 4(1) of the Theft Act 1968, it will seldom be the case that such a right is appropriated with the intention of permanently depriving the owner of it. Usually, the owner of the information will retain that knowledge even if someone else obtains it. Circumstances might exist where such an intention was to be found, such as where the copier erased the original information after having made the copy,[69] or where all the value of the information has gone,[70] but in general this

---

68. For a persuasively argued view that, except in a very loose sense, information is not property, see R. Grant Hammond, "Theft of Information", (1984) 100 L.Q.R. 252 - 264. In Canada it has been held that confidential information is capable of being stolen, see R v. Stewart (1983) 5 C.C.C. (3d) 481 (Ontario Court of Appeal). A contrary view is expressed by the Lord Justice-Clerk (Ross), Lord McDonald and Lord Wylie in the decision of the High Court of Scotland, Grant v. Allan 1987 S.C.C.R. 402.

69. This would probably also constitute criminal damage - see paras. 3.35 - 3.40 above. For further examples of theft of intangible property, see E. Griew, The Theft Acts 1968 and 1978, 5th ed. (1986), para. 2-83; J.C. Smith, The Law of Theft, 5th ed. (1984), para. 104.

70. On the basis of the reasoning in Lloyd [1985] Q.B. 829, para. 3.43 above. Professor Smith suggested that in Oxford v. Moss, the defendant might have been convicted of theft of the question paper, on the basis that all the value of the work put into the paper was lost when it was discovered that Mr Moss had advance notice of its contents: [1978] Crim.L.R. 120.

would not be the case.

(b) Unauthorised copying under the Copyright, Designs and Patents Bill 1988

3.48 While it seems that the unauthorised copying of computer programs will seldom constitute theft, computer programs were brought within the scope of the Copyright Act 1956 by the Copyright (Computer Software) Amendment Act 1985. However, the Copyright, Designs and Patents Bill 1988 will, if enacted, provide a complete new code to deal with rights in computer software. It is not proposed to deal with the provisions of the Bill in this paper, because any discussion may be out of date by the time of publication.[71]

E. USE OF INFORMATION HELD UNDER THE DATA PROTECTION ACT 1984

3.49 The Data Protection Act 1984 is described in the long title as -

> "An Act to regulate the use of automatically processed information relating to individuals and the provision of services in respect of such information."

For the purpose of this Working Paper it is not necessary to provide a comprehensive discussion of the 1984 Act.[72] We

---

71. The Bill is due to return to the House of Lords in October 1988.

72. In particular, our account omits discussion of exceptions to the Act. Where personal data is held for certain purposes (e.g. national security - s.27(1)), Part II of the Act (registration, supervision, appeals etc.) and ss.21 - 24 (rights of data subjects) do not apply at all. There are also partial exemptions (contained in Part IV of the Act) to the "subject access provisions" (primarily s.21) and the "non-disclosure provisions" (primarily s.5(2)(d) and s.15). For access to certain records stored manually, see Access to Personal Files Act 1987.

outline the principles on which the Act is based and look at the controls imposed by the Act on the use of data held on an individual. We deal, first, with the structure of the Act and, secondly, with the sanctions against the misuse of information by a data user and the remedies of a data subject in respect of damage caused by such misuse. Thirdly, we look at the criminal sanctions provided by the Act which may in certain circumstances apply to the hacker who obtains unauthorised access to personal data.

1. The structure of the Act

3.50 Section 1 of the Act provides definitions for certain terms used in the Act. "Data" means -[73]

> "... information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose."

"Personal data" means -[74]

> "... data consisting of information which relates to a living individual who can be identified from that information (or from that and other information in the possession of the data user), including any expression of opinion about the individual but not any indication of the intentions of the data user in respect of that individual." (emphasis added.)

---

73. Sect.1(2).

74. Sect.1(3).

The living individual who can be thus identified is the "data subject".[75] A "data user" is a person who holds data[76] and a person carries on a "computer bureau" if he provides other persons with services in respect of data.[77]

3.51 Section 4 of the Act provides that data users and persons carrying on computer bureaux must register with the Data Protection Registrar. Each entry on the register must contain[78] the name and address of the data user; a description of the personal data to be held and of the purpose or purposes for which data will be used; a description of the sources from which the user intends to obtain the data; a description of any person to whom the user may wish to disclose the data; the names of any countries outside the United Kingdom to which the user may wish to transfer the data; and one or more addresses for the receipt of requests from data subjects for access to the data.

3.52 The Registrar is responsible for compiling and supervising the register and for promoting the observance of the "data protection principles" by data users and computer bureaux.[79] These principles,[80] the crux of the Act, are set

---

75. Sect.1(4).

76. Sect.1(5), which also defines "holds".

77. Sect.1(6).

78. Sect.4(3) and subject to the other provisions of this section.

79. Sect.4 and s.36 - "General duties of Registrar".

80. Similar principles were originally recommended in the Younger Committee's Report on Privacy in 1972 (Cmnd. 5012). They were endorsed by the Lindop Committee in 1978 (Report of the Committee on Data Protection, Cmnd. 7341, para. 38.08) and subsequently stated in the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.

out in Schedule I, Part I. In respect of personal data held by a data user the Act provides that -

> "1. The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.
>
> 2. Personal data shall be held only for one or more specified and lawful purposes.
>
> 3. Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes.
>
> 4. Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes.
>
> 5. Personal data shall be accurate and, where necessary, kept up to date.
>
> 6. Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
>
> 7. An individual shall be entitled -
>
> (a) at reasonable intervals and without undue delay or expense -
>
> (i) to be informed by any data user whether he holds personal data of which that individual is the subject; and
>
> (ii) to access to any such data held by a data user; and
>
> (b) where appropriate, to have such data corrected or erased."

In addition, principle no. 8 applies to data users and to persons carrying on computer bureaux. This provides that -

> "8. Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data."

3.53 Schedule I, Part II of the Act - "Interpretation" - provides further assistance as to the meaning of the data

protection principles. Three aspects are particularly relevant here. In respect of the first principle, the Act states that, subject to information supplied under a statutory obligation,

> "1. - (1) ... in determining whether information was obtained fairly regard shall be had to the method by which it was obtained, including in particular whether any person from whom it was obtained was deceived or misled as to the purpose or purposes for which it is to be held, used or disclosed."

In respect of the third principle,

> "3. Personal data shall not be treated as used or disclosed in contravention of this principle unless -
>
> (a) used otherwise than for a purpose of a description registered under this Act in relation to the data; or
>
> (b) disclosed otherwise than to a person of a description so registered."

In respect of the eighth principle, regard shall be had -

> "6(a) to the nature of the personal data and the harm that would result from such access, alteration, disclosure, loss or destruction as are mentioned in this principle; and
>
> (b) to the place where the personal data are stored, to security measures programmed into the relevant equipment and to measures taken for ensuring the reliability of staff having access to the data."

2. Enforcement of the Act

3.54 As already noted, it is the function of the Registrar to "promote the observance of the data protection principles" by data users and persons carrying on computer

bureaux.[81] There are no direct criminal sanctions for offending against the principles,[82] but a number of offences prohibit the knowing or reckless holding or use of personal data contrary to the entry in the register,[83] and the Registrar has a number of supervisory powers which are backed by the criminal law. Furthermore, the data subject has rights of inspection and, where appropriate, compensation and rectification in respect of personal data. However, the Act does not provide for a criminal offence of obtaining unauthorised access to personal data.[84]

3.55 Now that the Act is in force,[85] it is a criminal offence[86] to hold personal data unless registered with the Registrar. Furthermore, the Registrar must refuse to register an applicant if he is satisfied that the applicant is likely to contravene any of the data protection principles.[87] If the Registrar is satisfied that a

---

81. Sect.36. For the Registrar's powers of entry and inspection in relation to his supervisory function, see s.16, Sch.4.

82. The Lindop Committee recommended (para. 19.91) that it should be a criminal offence (triable either way and more serious than that of failing to register) for any user to be in breach of the Code of Practice.

83. Sect.5(2).

84. See paras. 3.58 - 3.60 below.

85. The Data Protection Act 1984 (Appointed Day) Order 1985 (SI 1985/1055) provided that applications for Registration might be made from 11 November 1985. This is the "appointed day" for the purposes of s.42(1) of the Act; s.42 deals with the commencement of the Act in terms of this appointed day.

86. See s.5(1). The offence is triable either-way and punishable on indictment with a fine or, on summary conviction to a fine not exceeding the statutory maximum (£2,000) - s.19.

87. Sect.7(2). It is an offence contrary to s.6(6) of the Act knowingly or recklessly to furnish the Registrar with information which is false or misleading in a material respect in connection with an application for registration.

registered person has contravened a data protection principle he may serve him with an "enforcement notice"[88] (ordering him to comply with the principle) or a "de-registration notice"[89] (where the Registrar is satisfied that an enforcement notice would be ineffective). The Registrar also possesses the final sanction of instituting proceedings for an offence[90] under, where appropriate, section 5 (the unregistered holding of personal data), or section 10 (failure to comply with an enforcement notice).

3.56 The individual data subject is entitled, broadly speaking, first, to be informed by a data user whether the latter holds any personal data relating to him; and, secondly, to be supplied by the data user with a copy of that personal data.[91] If the data are incorrect or misleading as to any matter of fact and the data subject thereby suffers damage or distress, he shall be entitled to compensation from the data user.[92] Furthermore, the data subject is entitled to compensation for any damage or

---

88. Sect.10.

89. Sect.11.

90. See s.19 - "Prosecutions and penalties". Proceedings for an offence under the Act may only be instituted by the Registrar or with the consent of the Director of Public Prosecutions.

91. See further s.21 - "Rights of access to personal data".

92. Sect.22 - "Compensation for inaccuracy". It shall be a defence in any such proceedings for the data user to prove that he had taken such care as in all the circumstances was reasonably required to ensure the accuracy of the data at the material time - s.22(3).

distress suffered by reason of the unauthorised loss, destruction, disclosure of or access to such data.[93]

3.57 There is as yet little experience of the operation of the Data Protection Act 1984 and the practical impact of the data protection principles. The collection and use of information regulated by the Act is constrained by, in particular, the first three principles and the requirement that every data user must state the purpose for which the information is held in the relevant entry on the register. The further definition of the first principle in Schedule I, Part II makes it clear that a person collecting data must not mislead as to the purpose for which that information is to be held. In general, therefore, the Act provides the opportunity for, and imposes a certain responsibility on the data subject to check the information held in relation to him or her. If that information is obtained or used unfairly by a registered data user there is the possibility of compensation and, in the event of continuing breaches, a criminal sanction instituted by the Registrar. If an unregistered user obtains personal data this may also be a criminal offence.[94]

---

93. Sect.23 - "Compensation for loss or unauthorised disclosure". It shall be a defence in any such proceedings for the data user to prove that he had taken such care as in all the circumstances was reasonably required to prevent the loss, destruction, disclosure or access in question - s.23(3). The eighth data protection principle imposes a duty on both data users and persons carrying on computer bureaux to ensure that adequate security measures are taken against unauthorised access to, or alteration, disclosure, or destruction of personal data (see paras. 3.52 and 3.53 above). For the data subject's right to have inaccurate information rectified or erased, see s.24.

94. Contrary to s.5(1). See paras. 3.58 - 3.60 below.

3. The Data Protection Act 1984 and hacking

3.58 While it is true to say that the 1984 Act does not expressly prohibit the obtaining of unauthorised access to personal data, such conduct may fall within the scheme of criminal offences created by the Act.

3.59 If a person, who is not registered under the 1984 Act, obtains access to personal data stored on another computer, records that information as data on his own computer and intends to extract the information constituting that data (for example, by displaying it on a V.D.U. screen) by reference to the data subject, that person may commit the offence of holding personal data without having registered as a data user.[95] If on similar facts the hacker is registered under the Act, it is likely that an offence is committed under section 5(2) of the Act, such as knowingly or recklessly obtaining personal data from a source which is not described in the entry,[96] or knowingly or recklessly holding personal data of any description other than that

---

95. Contrary to s.5(1) of the 1984 Act and assuming that the general exemptions to the Act do not apply. An important exemption in this instance would be s.33(1) which provides that, "Personal data held by an individual and concerned only with the management of his personal, family or household affairs or held by him only for recreational purposes are exempt from [the registration requirements and the provisions (ss.21-24) dealing with the data subject's rights]...." The offences created by s.5 are triable either way and punishable on indictment with a fine or on summary conviction with a fine not exceeding the statutory maximum.

96. Contrary to s.5(2)(c).

specified in the entry.[97]

3.60 We are not aware of any prosecutions under section 5 of the 1984 Act in relation to the unauthorised obtaining of access to personal data. We note that the offence makes no distinction between the authorised and unauthorised obtaining of information, and also that it does not punish the obtaining of access to personal data, but the holding of such information. It would therefore be incorrect to describe section 5 as a "hacking" offence; it may provide a limited and complex criminal sanction against certain forms of hacking.

F. CIVIL LIABILITY FOR COMPUTER MISUSE

3.61 It is unnecessary for the purpose of this paper to investigate the application of the general civil law to forms of computer misuse. Only one matter requires consideration, and that is whether a remedy based on breach of confidence is available against a person who acquires confidential information by improper or reprehensible

---

97. Contrary to s.5(2)(a). In the examples given, a conviction would require the presence of a number of factors. First, the information to which the hacker obtains access must be "personal data" (defined in s.1(3) by reference to s.1(2) "data"). Secondly, the hacker must become a "data user" in respect of this information. For this purpose, the data user must "hold" the data as defined in section 1(5), and one of the requirements of this definition is that the data user has already, or intends to, amend, augment, delete or rearrange the data, or extract the information constituting the data. This "processing" of the information must be done by reference to the data subject (s.1(7)), and shall not be construed as applying to any operation performed only for the purpose of preparing the text of documents (s.1(8)). See further J.A.L. Sterling, The Data Protection Act 1984, 2nd ed. (1985), para. 690.

means.[98] If the answer to this question were, "yes", then, for example, "hackers" who obtained confidential information could be restrained by injunction from using that information and might be liable in damages for any material loss caused by the breach of confidence. Whether, if this were the law, it would be a sufficient response to such conduct is discussed in Part VI below.[99]

3.62 In our Report on Breach of Confidence in 1981 we doubted[100] whether the fact that information had been obtained by reprehensible means impressed it with an obligation of confidence. Of particular relevance to this conclusion was the decision of Sir Robert Megarry V.-C. in Malone v. Metropolitan Police Commissioner.[101] The case concerned the tapping by the Post Office at the request of the police of a subscriber's telephone line. In the course of his judgment, Megarry V.-C. dealt with the situation where "the alleged misuse [of information]" was "by someone to whom the plaintiff had no intention of communicating anything", which introduced the issue of "the unknown overhearer".[102] He then gave examples of the risks of being overheard inherent in the circumstances of

---

98. According to the analysis in our Report on Breach of Confidence, Law Com. No. 110, Cmnd. 8388, (1981), para. 3.1, this aspect of the remedy is logically distinct from those breach of confidence cases in which information which is not publicly known is entrusted to a person in circumstances imposing an obligation not to disclose or use that information without the authority of the person who has imparted it. That aspect of the remedy has no particular relevance to computer misuse and is not pursued here.

99. Paras. 6.4 - 6.6.

100. Law Com. No. 110, para. 4.8. Such doubts had previously been expressed by the Younger Committee, Report on Privacy (1972), Cmnd. 5012, para. 632.

101. [1979] Ch. 344. Discussed in Law Com. No. 110 at para. 4.9.

102. Ibid., p.376.

communication, and said -[103]

> "I do not see why someone who has overheard some secret in such a way should be exposed to legal proceedings if he uses or divulges what he has heard. No doubt an honourable man would give some warning when he realises that what he is hearing is not intended for his ears; but I have to concern myself with the law, and not with moral standards. There are, of course, many moral precepts which are not legally enforceable.
>
> When this is applied to telephone conversations, it appears to me that the speaker is taking such risks of being overheard as are inherent in the system.... In addition, so much publicity in recent years has been given to instances (real or fictional) of the deliberate tapping of telephones that it is difficult to envisage telephone users who are genuinely unaware of the possibility. No doubt a person who uses a telephone to give confidential information to another may do so in such a way as to impose an obligation of confidence on that other: but I do not see how it could be said that any such obligation is imposed on those who overhear the conversation, whether by means of tapping or otherwise." (emphasis added)

3.63 Since Malone was decided, dicta in the case of I.T.C. Film Distributors v. Video Exchange Ltd.[104] have provided some support for the view that information reprehensibly obtained may be subject to a duty of confidence. Warner J. was prepared to accept[105] a submission that an earlier case, Lord Ashburton v. Pape -[106]

> "... was not an isolated decision but is illustrative of a general rule that, where A has improperly obtained possession of a document belonging to B, the court will, at

---

103. Ibid., pp.376 - 378.

104. [1982] Ch. 431.

105. Ibid., p.438.

106. [1913] 2 Ch. 465.

> the suit of B, order A to return the document to B and to deliver up any copies of it that A has made, and will restrain A from making any use of any such copies or of the information contained in the document." (emphasis added)

In the I.T.C. case the defendant had, during the course of a copyright action, obtained some files from the plaintiff's solicitor, "by a trick and not merely by accident".[107] The defendant was restrained from using the documents on another basis, but Warner J. accepted that, had the plaintiff acted in proper time, a remedy based on breach of confidence would have been available. Whether this case establishes a general proposition is not clear. Certainly, it appears that Malone was not cited to the court. If the principle does exist, then it may be relevant in cases where unauthorised access has been obtained to confidential information stored on a computer.

G. THE SCOPE OF THE PRESENT LAW RELATING TO COMPUTER MISUSE: CONCLUSIONS

1. Computer fraud

3.64 In general, the existing criminal law appears to be adequate to cover most cases of computer fraud. The only problem we have been able to identify relates to cases involving the "deception" of a computer (as opposed to a human being); but even there, when property is obtained, a charge of theft or conspiracy to defraud (if two people are involved) will very often lie.[108]

---

107. [1982] Ch. 431, 437.

108. See paras. 3.2 - 3.11 above.

2. Obtaining unauthorised access to a computer

(a) Hacking

3.65 At present the criminal law does not extend to the person who merely obtains unauthorised access to a computer by hacking, except to a limited extent in respect of dishonestly abstracting electricity and in certain circumstances where an offence might be committed under the Data Protection Act 1984.[109]

(b) Eavesdropping on a computer

3.66 Eavesdropping on a computer is in principle no different from any other form of eavesdropping. As such it is partly covered by the Interception of Communications Act 1985 and, in general, it is covered by the laws relating to privacy which operate in England and Wales. The law relating to unauthorised surveillance is beyond the scope of the present exercise.

(c) Using a computer for unauthorised private purposes

3.67 The present criminal law does not provide any special remedies for the use of computers by authorised users for unauthorised purposes, unless such conduct falls within one of the general fraud offences discussed above.[110] Our provisional view, on which we would welcome comment, is that there is nothing about the unauthorised use of a computer, as opposed to any other object or machine, which would justify the extension of the criminal law beyond its present limits in this area.

---

109. See paras. 3.13 - 3.29 and 3.58 - 3.60 above.

110. See paras. 3.2 - 3.11.

3. Unauthorised alteration or erasure of data or software

3.68 The law of criminal damage now seems to extend to persons who damage a computer system, without the need for any further reform of the law. We would, however, welcome comments on whether this offence is felt to be appropriate to deal with "damage" such as that caused in Cox v. Riley:[111] our provisional view is that such activities can properly be said to fall within the meaning of "damage" for the purpose of the Criminal Damage Act 1971. We should add that "computer viruses" and "logic bombs" are merely sophisticated examples of criminal damage and, while such cases might give rise to difficulties in detection, the substantive law encompasses such activities within the 1971 Act.[112]

4. Unauthorised copying of data or software

3.69 In our view the law relating to the temporary appropriation of items on which information is stored does not give rise to problems which are peculiar to computers.[113] Similarly, the definition of property for the purpose of theft, and the argument as to whether it is possible to appropriate information belonging to another with the intention of permanently depriving the other of it, are problems which have general implications outside the

---

111. (1986) 83 Cr.App.R. 54. See paras. 3.35 - 3.40 above.

112. See paras. 3.35 - 3.40 above. The danger that a hacker might inadvertently cause criminal damage (and therefore not be guilty of the offence under the 1971 Act) is considered further in Part VI below (paras. 6.11 - 6.18).

113. We raised for consideration the general issue of criminal liability for temporary appropriation of property in our Working Paper on Conspiracy to Defraud: see (1987) Working Paper No. 104, paras. 13.4 - 13.6.

region of computer misuse.[114] We have not dealt with the provisions relating to "software piracy" contained in the Copyright, Designs and Patents Bill currently before Parliament.

5. Use of information held under the Data Protection Act 1984

3.70 We consider that it is too soon to evaluate the practical impact of the 1984 Act.[115] However, we have drawn attention to the possible application of criminal offences created by the Act to the unauthorised obtaining of access to a computer by hacking, and we will refer to the concept of personal data in our discussion of options to reform the law relating to hacking in Part VI below.

6. Civil liability for computer misuse

3.71 In general, computers present no special problem in respect of tortious liability under the civil law. It seems that, where information stored on a computer is obtained by reprehensible means, it may be open to English law to develop a remedy in the form of breach of confidence, but this course has yet to be finally chosen by the courts.[116]

---

114. These questions also arose in our review of conspiracy to defraud, but we decided that it was neither necessary nor appropriate to pursue it further in that context: ibid., paras. 10.44 - 10.48.

115. See paras. 3.49 - 3.60 above.

116. See paras. 3.61 - 3.63 above. We refer to the Law Commission's recommendations for reform of the law of breach of confidence in this area at para. 6.5 below.

PART IV

REFORMING THE PRESENT LAW (1): OUR GENERAL APPROACH

4.1 For ease of presentation we have divided our consideration of possible reform of the present law into four Parts. In this Part of the paper we consider, in the light of our conclusions in Part III, and of our earlier comments in relation to the nature of "computer crime",[1] the way in which the reform of the criminal law relating to computer misuse should be approached. From our conclusions in Part III,[2] it appears that only two kinds of computer misuse might be said to justify an extension of the present scheme of general criminal offences. The first would involve the amendment of one aspect of the Theft Acts which seems to us to be deficient in its application to certain kinds of computer fraud.[3] This is dealt with in Part V of the paper. The second is hacking,[4] which is considered in Part VI below. In Part VII we look at the jurisdiction of the courts in England and Wales to try the main offences of computer misuse, both existing and possible. In particular, we consider the difficulties which may arise in cases where the acts constituting the offence are done partly in England and Wales and partly in another country.

A. POSSIBLE GENERAL APPROACHES TO REFORM

4.2 The Scottish Law Commission[5] identified three

---

1. See paras. 1.5 - 1.6 above.
2. See paras. 3.64 - 3.71 above.
3. See para. 3.64 above.
4. See para. 3.65 above.
5. Report on Computer Crime (1987), Scot. Law Com. No. 106, paras. 3.9 - 3.12.

possible approaches to the reform of the law relating to computer misuse which, for our purposes, it is useful to examine.

1. A computer crime statute

4.3 Under the first approach, it would be possible to enact a comprehensive statute which created special offences of, for example, computer fraud and criminal damage of a computer. This has been done in most States in the U.S.A., following the model of Florida's Computer Crimes Act 1978.[6] In our provisional view, such an approach would not be appropriate in this country. The policy behind the Theft Act 1968 and the Criminal Damage Act 1971 was to create "broad band" offences which are so defined that they include a range of conduct and factual circumstances, and to dispense with distinctions based on the kind of property stolen or damaged. Our provisional view is that there is no reason to change this policy in relation to computers, but we would welcome comment on this matter.

2. Limited reform of the general law

4.4 The second approach[7] would be to reform the present criminal law only where there is a need for a new criminal offence to deal with specific kinds of computer misuse and provided that such reform would not affect the general application of the criminal law to other forms of conduct. Where computer misuse raised problems relevant to the general law of, for example, theft or intellectual property, such issues would only be tackled as part of a comprehensive review of the wider subject. Our provisional view is that,

---

6. See Appendix A, para. 33 below.

7. Report on Computer Crime, para. 3.10. This was the approach favoured by the Scottish Law Commission.

while there are arguments for and against a new offence of hacking, the structure of theft and fraud offences in England and Wales is such that it would also be possible to amend the Theft Acts in order to deal with one defect of the general law. It is therefore necessary to consider the third approach to reform considered by the Scottish Law Commission.

3. A "half-way approach"

4.5 The "half-way approach" referred to by the Scottish Law Commission[8] means rejecting the creation of wholly new offences, except where these are absolutely necessary, but being prepared to contemplate the widening of existing general offences (by, for example, the amendment of definitions or conditions) in order to make these existing offences more appropriate for incidents of computer misuse.[9]

4.6 The obtaining of unauthorised access to a computer by hacking is not at present covered by the criminal law. If it is felt necessary to criminalize such conduct, our provisional view is that this could not be done by extending an existing crime, but would require the creation of a new offence. We set out earlier some general guidelines relevant to the creation of new criminal offences, and we would refer here to those guidelines and to our comments on "computer crime".[10] In particular, before an offence of

---

8. Ibid., para. 3.12.

9. The Scottish Law Commission felt (ibid.) that this approach was not open to them because, in Scotland, the relevant existing crimes were common law offences, and therefore not defined in precise statutory terms which it would be possible to amend in order to deal with problems relating to computer misuse.

10. See paras. 1.11 and 1.5 - 1.6 above.

hacking could be created, the exact mischief at which such an offence is aimed must be identified.

4.7 Our provisional view is that the half-way approach is the most appropriate to the problem of computer misuse in England and Wales. We consider in detail in Part VI whether hacking should become a criminal offence and, if so, what kind of criminal offence would be appropriate. We are fortified in our view that this is the area of computer misuse which raises the most important questions in relation to the scope of the criminal law by the fact that other law reform bodies who have considered these issues have reached a similar conclusion.[11] First, however, in Part V we examine the need for a reform of the general law in relation to computer fraud and, in particular, the reform of the meaning of "deception" in the Theft Acts in order to deal with the problem which we identified in Part III.[12] We note also that a reform such as we provisionally propose in Part V would have the effect of criminalizing certain forms of hacking which are at present excluded from the criminal law. This point is relevant to our discussion in Part VI.[13]

---

11. See Appendix A, para. 15 below.

12. See paras. 3.6 - 3.7 above.

13. See para. 6.15 below.

PART V

REFORMING THE PRESENT LAW (2): COMPUTER FRAUD

A. "DECEIVING" A MACHINE

5.1 Our earlier discussion of the scope of the existing general criminal law in relation to frauds committed by means of, or with the help of, computers highlighted one particular problem area concerning offences involving deception. It seems that, where a computer or other machine is manipulated in order to obtain a benefit of some kind and no person is deceived, the element of deception is not satisfied and therefore a prosecution on such a charge may fail. In our working paper on conspiracy to defraud last year,[1] we considered this problem and suggested that there was a strong case for clarifying the scope of offences of obtaining by deception, so as to cover deception which involves the manipulation of a computer. We pointed out that it may be a matter of chance in some cases whether a person, such as a computer operator is deceived or no one at all. In either case the end result is the same and it is fraudulent conduct which we thought should be covered by the criminal law.

5.2 Our provisional view was that no new offence need be created to deal with this problem.[2] We proposed instead that the definition of "deception" in the Theft Acts should be extended to cover cases where a computer (or any other

---

1. (1987) Working Paper No. 104, Conspiracy to Defraud, paras. 10.3 - 10.9.

2. The working paper included (at para. 10.8) a brief discussion of a possible new offence aimed merely at the dishonest use of a machine. We provisionally rejected such an offence because of its excessive width and do not need to consider it further in this paper.

machine) is "deceived", rather than any human mind. A similar approach has recently been adopted elsewhere[3] and has been adopted here in the case of two offence-creating enactments. Thus, in relation to forgery and kindred offences the Forgery and Counterfeiting Act 1981 provides, in section 10(3), that -

> "references to inducing somebody to accept a false instrument as genuine, or a copy of a false instrument as a copy of a genuine one, include references to inducing a machine to respond to the instrument or copy as if it were a genuine instrument or, as the case may be, a copy of a genuine one."

Similarly, section 39(2C) of the Value Added Tax Act 1983 (inserted by section 12(5) of the Finance Act 1985) provides -

> "The reference ... to furnishing, sending or otherwise making use of a document which is false in a material particular, with intent to deceive, includes a reference to furnishing, sending or otherwise making use of such a document, with intent to secure that a machine will respond to the document as if it were a true document".

The effect of this provision is to deem a deception to have taken place where false information is fed into a computer.[4]

5.3 Our proposal would involve extending the existing definition of deception along similar lines, but with appropriate modifications. We suggested that it might include a provision such as -

---

3. See the Victoria Crimes (Computers) Act 1988, s.6 noted at Appendix A, para. 34 below.

4. The latter provision was enacted on the recommendation of the (Keith) Committee on Enforcement Powers of the Revenue Departments (1983), Cmnd. 8822, Vol.2, para. 18.3.17 in order to fill the lacuna in the VAT legislation revealed by the case of Moritz (see para. 3.6 above).

> "inducing a machine to respond to false representations which the person making them knows to be false, as if they were true".

As with the other legislation mentioned, reference is made to a "machine" rather than to a computer which, if used here, might be an undesirable limitation on the proposed extension.

5.4 The deception offences affected by a change of this kind would be those contained in sections 15, 16, 20(2) of the Theft Act 1968 and sections 1 and 2 of the Theft Act 1978. Sections 1 and 2 both assume the existence of a person who is not merely the victim of the offence but who is also personally affected by the deception.[5] The former section postulates that "the other is induced to confer a benefit on the understanding that the benefit has been or will be paid for"; and the latter refers in subsection (1)(b) to a person who "induces the creditor or any person claiming payment on behalf of the creditor to wait for payment ...". Both these sections would, therefore, require further amendment to ensure that the offences concerned apply to cases where a machine has been "deceived". However, we do not put forward any drafting suggestions at this stage.

5.5 Taken together, the amendments to the Theft Acts, required to deal with a deception which involved the manipulation of a computer or computer system rather than the deception of a person, would be largely technical and, we believe, relatively uncontroversial extensions of the criminal law. Although we have already raised these matters in an earlier paper (and have received comment on them), we

---

5. E. Griew, The Theft Acts 1968 and 1978, 5th ed. (1986), para. 6.15.

look forward to having the views of those who did not see that paper.

B. OBTAINING (COMPUTER) SERVICES BY DECEPTION

5.6 One effect of giving "deception" an extended meaning should be mentioned at this stage, because it has a bearing on the discussion in the next section concerning possible criminal liability for computer hacking. Assuming such a change in the law were to be made, if an individual were to make use of a commercial computer service (such as commercial data-bases, computerised "mail boxes", specialised software or even just the processing capacity represented by a mainframe computer) by using a password he is not entitled to use, and avoids payment for such services,[6] he would be liable (assuming dishonesty to be found) to be convicted of the offence under section 1 of the Theft Act 1978. Under the present law such an individual might only be convicted in similar circumstances where he had practised a deception on a person, for example by deceiving an authorised user or the computer's operator into disclosing a password.[7] The effect of the proposed change would be to criminalize one aspect of computer hacking, namely the dishonest and unauthorised use of computer services for which payment would otherwise be expected. Whether such an extension would be a sufficient response to the problem of computer hacking is considered below.[8]

---

6. Perhaps at the same time passing on the charge to a wholly innocent third party. Having gained unauthorised access to a number of Prestel computers, Gold and Schifreen caused charges to be made to account holders without the knowledge or consent of the latter: [1988] 2 W.L.R. 984, 987.

7. Although even then it would have to be shown that there was a causal nexus between the deception and the obtaining of the service: see para. 3.34 above.

8. See para. 6.15 below.

C. CONSPIRACY TO DEFRAUD

5.7 This offence is currently under review by the Commission and several options for its reform were put forward in a working paper issued at the end of last year.[9] One option for the possible replacement of the common law offence is the extension of existing offences and the creation of specific offences of fraud to ensure that, so far as is necessary and desirable, all the conduct which can at present be prosecuted as conspiracy to defraud becomes a specific offence capable of being committed by an individual.[10] The suggested redefinition of "deception" for the purposes of the Theft Acts was but one of a number of changes which might be required if this approach were followed. A second option put forward is the creation of a new fraud offence which would cover much of the conduct which can now be prosecuted as conspiracy to defraud.[11] The fraud offence, as we proposed to define it,[12] would be of general application and would cover a number of existing offences, including most of the deception offences in the Theft Acts. Were this option to be followed there might be no need to retain these as separate offences. By not requiring proof of deception (as with conspiracy to defraud at present[13]), the fraud offence would present an alternative way of avoiding the difficulties connected with

---

9. (1987) Working Paper No. 104, Conspiracy to Defraud.

10. Ibid., Part X.

11. Ibid., Part XII.

12. "Any person who dishonestly causes another person to suffer financial prejudice or a risk of prejudice, or who dishonestly makes a gain for himself or another commits an offence".

13. See para. 3.10 above.

cases involving the "deception" of a computer.[14] A third option is to replace common law conspiracy to defraud by a statutory offence of conspiracy to defraud.[15] No decision has yet been taken on which option, if any,[16] is to be recommended, but we hope to issue our final report on conspiracy to defraud in 1989.

---

14. Except possibly in the case of obtaining services by deception which might still need to be retained as a separate offence: Working Paper No. 104, para. 12.30.

15. Ibid., Part IX.

16. One further option was to retain the existing law: ibid., Part VIII.

PART VI

REFORMING THE PRESENT LAW (3): HACKING

6.1 We now turn to examine in this, the third part dealing with reform of the law, the question which we regard as the main issue arising for consideration in this working paper: Should the obtaining of unauthorised access to a computer be a criminal offence? Like most other law reform agencies and bodies elsewhere who have had occasion to review their laws in relation to computer misuse, we think that this is the central question which requires to be answered.[1] Although many jurisdictions have already acted to make unauthorised access to a computer a criminal offence, there is clearly room for more than one view on this issue and the arguments for and against extending the criminal law of England and Wales to cover this conduct will be examined below.

6.2 It is right to say at the outset that we ourselves have not yet reached even any provisional conclusion on this matter. We hope this part of the paper, and the specific questions raised in it, will stimulate an informed response in order to help us to decide whether or not to recommend new legislation.

6.3 The possible criminalization of conduct which is not at present directly covered by the criminal law must involve a consideration of whether it is in the public interest that such conduct should be regarded as criminal.[2] This in turn must involve consideration of whether it can be adequately controlled in some other way, in particular by

---

1. See Appendix A, paras. 15 - 26 below.

2. For some general guidelines relevant to the creation of new criminal offences, see para. 1.11 above.

the civil law. It is necessary therefore to examine this question as a preliminary issue.

A. COULD THE CIVIL LAW PROVIDE AN EFFECTIVE REMEDY AGAINST UNAUTHORISED ACCESS TO A COMPUTER?

6.4 On the assumption that it is desired to deter the unauthorised obtaining of access to a computer, can this be effectively done by remedies under the civil law, whether or not the civil law were to be reformed? Resort to the civil law in this case would entail, for example, the legitimate holder of the information (in many instances the computer owner) proceeding by way of a civil action against the person who acquires that information by obtaining unauthorised access to a computer, or the computer owner proceeding against the person who inadvertently corrupts data held on the computer through hacking.

6.5 The Law Commission has already recommended, in the context of its proposals for the reform of the law on breach of confidence, that a person should owe an obligation of confidence in respect of information improperly obtained by (among other means) "unauthorised use of or interference with a computer or similar device in which data is stored".[3] While implementation of this recommendation[4] might in theory enable an action for breach of confidence to be

---

3. Report on Breach of Confidence (1981) Law Com No. 110, Cmnd. 8388, para. 6.46.

4. The Home Secretary announced on 12 March 1985 (Hansard (H.C.), Vol.75, col. 157) that the Government intended to introduce legislation to implement the proposals in Law Com. 110 in order to provide further safeguards against unauthorised surveillance. The Solicitor General recently said that implementation did not have a high priority, because the report amounted essentially to a restatement of the common law (Hansard (H.C.), 2 February 1987, Vol.109, col.513 (written answers).

pursued against the hacker in some cases, we doubt whether this alone would provide a very effective means of deterring such conduct generally. Likewise, an action in negligence might in theory be available where it can be shown that data was carelessly corrupted or erased by a person as a result of his obtaining unauthorised access, but the prospects of success would in most cases be uncertain. In either case, injunctions to restrain a person from hacking would be of little use once access had been obtained or the damage done. The remedy of damages (which would have to be proved) is of course only effective if the defendant has the means to pay them. Damages may be expected to be irrecoverable in most cases of hacking.

6.6 Our provisional view therefore is that the civil law (whether reformed or not) could only rarely provide an effective remedy. We would welcome comments on this conclusion.

B. SHOULD THE OBTAINING OF UNAUTHORISED ACCESS TO A COMPUTER BY HACKING BE A CRIMINAL OFFENCE?

6.7 In the light of our conclusion about the ineffectiveness of the civil law, we must now consider whether or not a criminal sanction is required. Before we consider the arguments for and against creating a new offence, there are some special features concerning computers and their accessibility to which we think attention must be drawn at this stage.

(i) Computers are capable of storing and processing vast amounts of information. Information which twenty or thirty years ago might have been stored in large rooms full of filing cabinets can now be kept on a single disk smaller than a pocket sized note-book. The computer is a relatively recent invention which we must now accept as a feature of

late 20th century life. In general, the benefits which this new technology has brought to members of society are not in doubt.

(ii) Much of the information stored in computers is information of a nature which those who disclose it to the computer owner would not want disclosed to third parties. For example, information relating to individuals of a personal kind, bank accounts, credit ratings, medical records and trade secrets.

(iii) For large computer systems to be effective, and to be of maximum use to legitimate users, including those who supply information to computer owners, they must be readily accessible from "remote" computer terminals. This necessarily gives rise to problems of security which are of an entirely different kind from those which arise in connection with the safeguarding of manual records. Doubtless, many of these problems can be solved by improvements in technology[5] or, more particularly, by having regard, in all computer systems to the eighth Data Protection principle relating to computer security.[6] However, it must be recognised that even if this principle were implemented in respect of all information stored on computer, it is difficult if not impossible to create a totally secure computer system.

(iv) It may be possible for a person to obtain unauthorised access to information stored on the computer without the need for any physical presence

---

5. See para. 1.16, n.20 above.

6. See paras. 3.52 - 3.53 above.

other than at a terminal which is connected to the computer system by means of a telecommunication system. Without this physical presence, a person who seeks to obtain unauthorised access will not be exposed to the risk of prosecution for offences such as burglary or criminal damage which might be applicable if physical access were required.

(v) In deciding whether obtaining unauthorised access to information held on a computer should be a crime, analogies with other forms of conduct may be helpful but can be misleading. It is probably better, therefore, to consider the computer for what it is.

With these points in mind we now turn to consider the main arguments for and against an offence of obtaining unauthorised access to a computer.

1. The arguments for an offence

6.8 One argument in favour of an offence flows directly from some of the special features described above. It acknowledges the importance of computers for society as a whole and suggests that those who use and rely on computers may be inhibited from making full use of them, if they fear that others might obtain unauthorised access to information held on them. For this reason, it is in the public interest that society must try to deter hacking either generally, or at the very least in respect of computers holding certain kinds of information.

6.9 Obtaining unauthorised access to material to which the Data Protection Act 1984 applies[7] could be peculiarly socially damaging. If a case can be made for any crime of unauthorised accessing, it is arguably strongest in relation to such material. Although, as we explained in an earlier part,[8] the Act provides a limited and complex criminal sanction against certain forms of hacking, it does not deal with the obtaining of access to personal data per se, which is perhaps the mischief against which any new offence ought to be aimed. The Act imposes on certain data users a duty to keep personal data secure;[9] an offence of obtaining unauthorised access to such data would at the same time strengthen this protection.

6.10 However, apart from material to which the Data Protection Act applies, there is much other private material held in accessible computers whose disclosure could be equally damaging. Nevertheless, problems would arise with defining categories of information (apart from "personal data") for the purpose of an offence. It might be better therefore not to draw lines around certain categories of information, but to do as other jurisdictions have done and apply an accessing offence to all accessing. There is a further reason for doing so in the next argument we consider in support of an offence.

6.11 The Audit Commission of England and Wales expressed the view[10] that the hacker runs a risk of inadvertently

---

7. That is, personal data as defined in s.1(3) of the 1984 Act; see para. 3.50 above.

8. See paras. 3.58 - 3.60 above.

9. Data protection principle no. 8: see paras. 3.52 - 3.53 above.

10. Survey of Computer Fraud and Abuse, 3rd triennial Report (1987), p.13.

damaging or destroying data files or programs and thereby disrupting the work in progress. Assuming that the hacker was not aware of the risk of damage, he or she would probably not be guilty of criminal damage. However, even inadvertent damage might cause a computer system to shut down partially or totally and this will inevitably cause the expenditure of time and effort in order to repair the computer. Indeed, if internal controls detect an irregular access to the computer system a certain amount of effort will have to be expended in trying to track down the perpetrator. If the computer system disrupted was, for example, the air traffic control system at an airport, the consequences might be quite disastrous,[11] but the inconvenience caused by the failure of any computer is likely to be serious.

6.12 This further argument in favour of an unauthorised access offence therefore rests on the possible consequences of hacking to a computer system. Where the computer system is especially important, or the information stored on it especially valuable, these consequences will be more serious, but hacking could lead to the inadvertent damaging of any computer system. An offence of obtaining unauthorised access to a computer would signal society's disapproval of those who deliberately set out to breach security measures, and amount to a rejection of the claim that hacking is a harmless intellectual pastime. This rejection could have beneficial consequences beyond the number of successful prosecutions likely to be brought: for example, a hacking offence could discourage the practice of

---

11. Of course, the risk of a hacker penetrating air traffic control is probably very small, but it must be emphasized that no computer system is completely secure. Even a computer system without remote access may be subject to unauthorised access by, for example, an intruder, or an employee acting beyond the scope of his authority.

people exchanging information concerning hacking "targets" on "bulletin boards".[12] Certainly one would expect such an offence to discourage teachers from encouraging their pupils to develop computer skills by hacking. It would also discourage hackers from boasting about their achievements in the press and thereby encouraging other attempts.

6.13 Another positive side-effect of a hacking offence would be that its prohibition may serve to deter conduct which is made possible by the obtaining of unauthorised access to a computer, such as computer assisted fraud or theft, or the corruption of data or programs. An offence which may reduce the number of opportunities for subsequent (illegal) activities is worthy of further consideration.[13]

6.14 Finally, we note that the Scottish Law Commission recommended the creation of an offence of obtaining unauthorised access to a computer, after a similar proposal had been widely supported in Scotland on consultation.[14] Other law reform bodies have reached a similar conclusion

---

12. "Bulletin boards" are a means by which subscribers may exchange information via a computer system and a modem. The provider of a password which enabled another person to obtain unauthorised access to a computer would probably be liable as an accessory to a new offence of hacking.

13. An analogy may be made with the prohibition against possession or use of cannabis: although it has been suggested that the use of this drug has no deleterious side-effects, decriminalization is sometimes said to encourage a progression towards the use of more dangerous drugs.

14. Report on Computer Crime (1987), Scot. Law Com. No. 106, para. 3.7. We note also that more than a third of the consultees on the Scottish Law Commission's Memorandum consisted of individuals or organisations who can be expected to have commented from a U.K., rather than a purely Scottish, perspective: ibid., Appendix B.

and two Commonwealth jurisdictions[15] as well as most States in the United States have already enacted criminal offences along similar lines.[16]

2. The arguments against an offence

6.15 The main argument against the introduction, in any form, of a criminal offence of obtaining unauthorised access to a computer is that, although such conduct may constitute an invasion of privacy, it is not a matter in which the criminal law should interfere. No general right of privacy exists in English law even in the law of tort,[17] and while obtaining unauthorised access to a computer may appear to be akin to the tort of trespass, such behaviour is not generally subject to criminal sanction without some further aggravating feature.[18] Information is not property in English law (although in certain respects it has been likened to property) and it is no offence, as such, to read someone else's correspondence or files. There is no crime of industrial espionage in England and Wales. If it is desired to protect privacy, this should be done openly and not merely by trying to protect the privacy of information held on computers. For example, if there is concern about the privacy, of say, a list of patients with AIDS, should we not be just as keen to protect the information whether it is held in a card index system or in a computer?

---

15. Canada and Victoria, see Appendix A, paras. 18 and 20 below.

16. See further Appendix A, paras. 15 - 26 below.

17. Malone v Metropolitan Police Commissioner [1979] Ch. 344, 358.

18. See "Trespass on Residential Premises", Home Office consultation paper (1982), paras. 8 - 16.

6.16 A further argument against the creation of a hacking offence is that the offence may be very difficult to enforce. We understand that it is possible for a hacker to obtain access to data on a computer and to ensure that the fact that he has obtained access remains undetected,[19] or at least can be discovered only after a very time-consuming search. Perhaps the most likely way in which hacking will come to light (in the absence of an admission or other conduct, such as the publication of confidential information obtained by the hacking) is when data is found to have been erased or altered, or a fraud is detected. In those instances, if the identity of the hacker can be traced, a charge of criminal damage or an offence of fraud[20] may then be the appropriate response rather than a charge of obtaining unauthorised access. Sometimes conduct may be so serious and so socially damaging that it clearly merits a criminal sanction whatever the problems of enforcement. In other cases where the harm caused by the relevant conduct is not so great, the case for providing a criminal sanction will be weakened by problems of enforcement. It is arguable that mere hacking falls into the latter category.

3. The extent of the problem

6.17 Before deciding whether particular conduct, like hacking which is not already a crime, should now become

---

19. But it is also possible to protect computer systems with various security devices, to make unauthorised access more difficult. See para. 1.16, n.20 above.

20. There has been a difficulty in the interpretation of "deception" in relation to the Theft Acts (see para. 3.5 above), but our provisional proposal is that this deficiency should be remedied (para. 5.3 above). If this were done, it would become an offence dishonestly to obtain by deception the use of services (including computer services) for which payment would otherwise be expected (see discussion in para. 5.6 above).

subject to a criminal sanction, it is pertinent to ask what the extent of the problem is. We accept that much of the evidence relating to hacking is drawn from anecdotal sources and may be unreliable. However, we note that the Audit Commission for Local Authorities in England and Wales said, in its most recent report, that -[21]

> "... [hacking] is becoming a common form of computer abuse, whether it is for gain, malicious intent or just general browsing, and is emerging as the single largest computer-related criminal activity."[22]

The Audit Commission considered that incidents of hacking were increasing for two reasons.[23] First, the use of desk-top computer terminals in the workplace was becoming much more common, giving more opportunities to the hacker. Second, the Commission thought that the arrival of a new generation of employees who were already computer literate when they joined the job market increased the risk of hacking opportunities being identified and taken. The 1,214 respondents to the Audit Commission's survey reported 35 incidents of hacking, only one of which led to a financial loss, and concluded ("surprisingly", in the view of the Audit Commission[24]) that hacking did not represent a significant threat. However, the Commission remarked on the

---

21. Survey of Computer Fraud and Abuse, 3rd triennial Report (1987), pp.3-4.

22. As was shown in Part III of this paper, obtaining unauthorised access to a computer in order to browse through the information stored therein is not, in the absence of damage, likely to be a criminal activity. Most of the hacking cases described in Appendix A to the Audit Commission's report (Cases 71 - 102) fall within the category of "general browsing".

23. Ibid., p.4.

24. Ibid., p.13.

dangers of apparently "harmless" hacking;[25] it might lead to the inadvertent damaging of data files or programs, the disruption of work in progress, and the undermining of customer or public confidence.

6.18 We share the view of the Scottish Law Commission[26] that at present there is insufficient evidence of the scale and consequences of computer misuse to conclude that it "would of itself suggest an impending crisis of a kind that demanded prompt legislative action." In our view, this is applicable to computer misuse generally, and certainly to the obtaining of unauthorised access to a computer by hacking. Nevertheless, we too would consider that the absence of such evidence does not mean that there are no problems requiring solution; there is some force in the argument that, if the law is deficient in this respect, it would not be wise to wait for confirmation that serious consequences could follow before taking action.[27] However, to justify legislative action and particularly the creation of any new criminal offence, we believe that it is essential to be able to identify the nature and extent of any risks involved. For this purpose it is, in our view, insufficient to rely simply on anecdotal evidence and generalisations. What is required is a clear statement of the kinds of damage which might be caused by hacking and of the nature of any risks posed to programs and data stored in the computer and of access being obtained to data which the owner of the installation is required by law to protect. We need to know the extent to which owners are able to guard against these risks by the use of up-to-date technology and security measures. We are therefore particularly interested to hear

---

25. Ibid.

26. See para. 3.4 of its Report.

27. Ibid., para. 3.5.

from owners and organisations with detailed knowledge of these subjects.

4. Conclusions

6.19 As we said at the beginning of this part, we have not yet reached a provisional conclusion as to the need for the creation of a new criminal offence to cover hacking. We have adverted to certain special features of computers and their accessibility as a background against which the arguments for and against a new offence (which we have also discussed) ought in our view to be considered. We would welcome views on whether, notwithstanding the arguments against extending the criminal law, it is felt that there is a strong case for legislation to control hacking and, if so, what should be the basis of the offence.

C. OPTIONS FOR REFORM - GENERAL

6.20 If it were decided to criminalize hacking, how should the offence be defined? We discuss in this section of the paper four options for the extension of the criminal law.

(1) First, an offence of obtaining unauthorised access to a computer in order to inspect certain kinds of information stored thereon (option A).

(2) Secondly, an offence of obtaining unauthorised access to a computer in order to inspect information stored thereon (option B).

(3) Thirdly, an offence of obtaining unauthorised access to a computer whereby damage to computer data or software is caused (but without the need to prove that the individual concerned intentionally or recklessly caused such damage) (option C).

(4) Fourthly, an offence of obtaining unauthorised access to a computer (option D).

6.21 These options have two elements in common which would need to be given further consideration: first, the meaning of "obtaining access to a computer"; and secondly, the meaning of "unauthorised". After these general considerations, we proceed to discuss the options for reform in turn and finally look at the mode of trial and penalties which should be available for any proposed offence.

1. "Obtaining access to a computer"

6.22 Our provisional view is that it would be undesirable if a hacking offence were to overlap with certain kinds of computer eavesdropping.[28] Therefore we are concerned that "obtaining access to a computer" should not include merely "listening in" to a computer from a distance.[29] It may be that the natural meaning of "obtaining access" does not include eavesdropping,[30] but in any event a criminal offence should be defined so as to remove any remaining doubts. The Scottish Law Commission considered whether the offence should be expressed in terms of "to communicate with" a computer, but after consultation rejected this term on the ground that it carried a sense of two-way interchange, whereas it was the penalisation of

---

28. See paras. 3.30 - 3.32 above. We noted in Part I (para. 1.16 above) that by the phrase "obtaining unauthorised access to a computer" we do not include the obtaining of physical access to a computer.

29. The Scottish Law Commission saw no objection to eavesdropping being dealt with by a hacking offence (Report on Computer Crime (1987), Scot. Law Com. No. 106, para. 4.14).

30. The Scottish Law Commission took the view that there was some overlap (ibid.).

essentially unilateral activity which was intended.[31] We agree, but would be interested to know whether there are any other phrases which contain the idea of "obtaining access to" and also exclude passive eavesdropping.

6.23 It may be thought to have been premature to discuss "computer misuse" without first discussing the definition of a "computer", but our provisional view is that it would be better not to attempt to define "computer" in any legislation that may be recommended. Instead, the word should be given its ordinary meaning.[32] Like many things, a computer is in general easy to recognise, but very difficult to define. A technical definition based, for example, on the way a computer performs operations, may give rise to difficult questions in particular cases, and may be overtaken by technological advances. On the other hand, to leave the word undefined in legislation will, perhaps, leave some areas of doubt: for example, is a pocket calculator or a digital watch, a computer? We note that the U.S. Federal legislation on computer misuse provides that a "computer" does not include "an automatic typewriter or typesetter, a portable hand held calculator, or other similar device".[33] Our provisional view is that, while a detailed, technical definition of a "computer" would be undesirable, a partial negative definition excluding certain items, such as those mentioned in the U.S. legislation, might be helpful. We would welcome comments on this point.

---

31. Ibid.

32. This approach has been adopted in recent legislation, such as the Police and Criminal Evidence Act 1984: s.69 makes certain provision in relation to evidence derived from "computer records" but does not define a computer.

33. Some other jurisdictions, California for example, have at least found it necessary to exclude calculators from their definition of computer. See further Appendix A, paras. 51 - 58 below.

2. "Unauthorised"

6.24 Whatever phrase is used to describe the obtaining of access to a computer, a hacking offence would also have to distinguish between the proper and improper obtaining of such access. An obvious solution would be to require that one of the elements of a proposed new offence would be the unauthorised obtaining of access. A number of issues fall for preliminary consideration -

(i) A problem might arise in determining in every instance who was entitled to grant access to a computer system, the extent of such power to grant access, and whether such authority, express or implied, had in fact been given. Whereas the stereotypical hacker, using a home computer and modem in order to discover new passwords,[34] would seldom be acting with authorisation, express or implied, in a large business it may not always be clear whether access obtained by an employee, or the extent of the access obtained, was authorised or not.

One answer to this problem might be to provide that the obtaining of unauthorised access should depend on whether the "accessor" believed that he had the authority to obtain access. Whether there were reasonable grounds for such a belief would go to the credibility of the defendant's explanation, but would not determine the matter.

(ii) A test based on authorisation might create a difficulty in that some instances of reprehensible "authorised" access will arguably not fall within

---

34. See para. 2.11 above.

the scope of an offence defined in such terms. For example, if an employee with authority to grant access, intentionally gives someone else the password to the employer's computer system, and that other person obtains access to, for example, confidential information stored on the computer system, it is arguable that this access has been authorised and therefore falls outside the scope of the offence. On the other hand, it might be argued that a distinction must be drawn between "authorisation" and "proper authorisation"; and that in this example the employee's powers of authorisation were restricted to purposes within the scope of his employment. If the other person did not believe that he had proper authorisation, then both could be convicted of the new offence; one as a principal offender and the other as an accessory. Which view of unauthorised is to be taken should be made clear in the definition of the offence.

(iii) Our provisional view is that "unauthorised" should apply both to an initial unauthorised obtaining of access to a computer system and also to the obtaining of access to a "higher" level of the computer system, after an initial authorised access, than the subject was permitted. If the person exceeds any authority that he has been given, then he is to be taken as acting without authority.

(iv) It should be made clear that "unauthorised" refers to the obtaining of access to a computer system. Our preliminary view is that it would be undesirable for a hacking offence to extend to an authorised user who is using the computer system for an unauthorised purpose. For example, the

word-processor operator who has authority to use the office computer system in order to type the employer's letters ought not to be guilty of a hacking offence if he or she uses the computer system to produce private correspondence.

D. PARTICULAR OPTIONS

1. Option A

6.25 Option A would prohibit the obtaining of unauthorised access to a computer in order to inspect information falling within certain defined categories, for example, personal data as defined by the Data Protection Act 1984.

(a) Arguments for

6.26 Option A would give primary weight to the argument that the unauthorised accessing of certain kinds of information stored on computers can be particularly damaging. If option A were to be limited to personal data, this offence would reinforce the special regime created by the Act in respect of such information.

(b) Arguments against

6.27 Option A is open to the objection that liability for the offence would be conditional on the kind of information stored on the computer, and this might make it undesirable in the eyes of those who would like a hacking offence to cover all cases of hacking, irrespective of the information at risk. Although personal data can be categorised (adopting the definition provided in the Data Protection Act 1984), defining the further categories of information to be protected could be very difficult. Furthermore, the added requirement of obtaining unauthorised

access in order to inspect information reduces the force of the argument that hacking should be discouraged because of the attendant risk of damage.

6.28 It might also be said that had Parliament wanted to provide for the added protection of personal data by means of an unauthorised access offence, it could have done so in 1984. No evidence has come to light since the Act came into force that the present safeguards are inadequate.

2. Option B

6.29 Option B would be to create an offence which punished the person who obtained unauthorised access to a computer in order to inspect information of any kind. It might in addition be provided that such inspection should only be prohibited if it were done for the purpose of either gaining an advantage for oneself or another, or of damaging another person's interests.[35]

(a) Arguments for

6.30 Option B is based on the protection of information which is stored on a computer. In providing protection only for information stored on computer, it can be supported on the basis of the special features exhibited by a computer system.[36]

(b) Arguments against

6.31 First, it may be felt that option B is too restricted in its scope, because in cases where the hacker's

---

35. This option is very similar to that suggested by the Scottish Law Commission (Report, para. 4.12).

36. See para. 6.7 above.

only motive is to overcome security devices protecting a computer as a challenge, it might be difficult to prove the commission of this offence.[37] Secondly, as with option A, the offence does not focus on the attendant risk of damage which hacking may involve.

3. Option C

6.32 Option C would prohibit the obtaining of unauthorised access to a computer whereby damage is caused to data or software. Unlike the offence of criminal damage, it would not be necessary to prove that the damage was intentionally or recklessly caused;[38] there would be strict liability so far as the result is concerned (though it would be necessary to prove that he intended to obtain unauthorised access.)

(a) Arguments for

6.33 The major justification for such an offence is that it seeks to counter the inadvertent damage which a hacker might do to a computer system.[39] It is not based on the protection of information stored on a computer system but on the protection of the computer itself.

(b) Arguments against

6.34 The offence would not be committed unless there was proof that damage was caused; it might be felt, therefore, that it would not deter the hacker who was confident in his

---

37. If it is felt that such conduct should not be criminalized then this is a point in favour of option B, in comparison with option D below: see para. 6.35.

38. See paras. 3.35 - 3.40 above.

39. See the reasoning in paras. 6.11 - 6.12 above.

or her ability to obtain access to the system without causing any damage. This raises the fundamental issue of whether a hacking offence is designed to protect the confidentiality of the information stored on the computer, or the computer system itself.[40]

4. Option D

6.35 Option D would make it an offence intentionally to obtain unauthorised access to a computer. Such conduct would be covered without any requirement that the hacker had a subsidiary purpose other than to obtain access to the computer. Nor would there be any need to prove damage to data or software.

(a) Arguments for

6.36 The offence would clearly state the mischief at which it was aimed and encompass all forms of hacking regardless of any nefarious motive on the part of the hacker. It would punish a certain form of conduct, irrespective of whether harmful consequences were to follow. The offence would be "absolute" in the sense that it would be no defence for a hacker to show that, although he had obtained unauthorised access to a computer, he had taken all reasonable care to avoid causing damage to the computer system, or that there was no possibility of damaging the system. The information stored on a computer system would be protected because of the special features of computerised information.[41]

---

40. See the arguments in paras. 6.8 - 6.16 above.

41. See para. 6.7 above.

(b) Arguments against

6.37 In cases where there is no conceivable risk that the obtaining of unauthorised access might damage the computer system, what is in effect being protected by the offence is a right to privacy in the information based solely on the fact that it is stored on computer. It is arguable that this ought not to be a concern of the criminal law. Moreover, there would be a risk that some forms of relatively inoffensive conduct would be criminalized. For example, obtaining unauthorised access to a data base, such as a library's computerised records' system or a British Railways timetable, presumably entails no danger to the computer system, but could still be punished under such an offence.

E. MODE OF TRIAL AND PENALTIES

6.38 Our provisional view is that, if it were decided to make hacking a criminal offence in any of the above forms, it would be appropriate for the offence to be triable summarily only in the magistrates' courts, and a person convicted of such an offence should be liable to a fine not exceeding the statutory maximum (currently £2,000).[42] In our view it would be inappropriate for a hacking offence to be punishable with imprisonment, bearing in mind that if the hacker is convicted of recklessly or intentionally causing criminal damage, more severe penalties will be available to

---

42. Criminal Justice Act 1982, s.74(1), in conjunction with Magistrates' Courts Act 1980, s.32(9). We would also draw attention here to the general power of the court to order, on the conviction of a defendant for any offence, the forfeiture of property used or intended to be used in the commission of any offence: Powers of the Criminal Courts Act 1973, s.43 (as amended by the Criminal Justice Act 1988, s.69, which comes into force on 29 September 1988).

the court. We also note that, of the criminal offences created by the Data Protection Act 1984, none is punishable with imprisonment.[43]

F. ATTEMPTS

6.39 If hacking is criminalized and made triable summarily only, it will not be possible to convict a person of attempting to commit the offence.[44] Our provisional view is that special provision should not be made to create an offence of attempting to obtain unauthorised access to a computer.

---

43. Sect.19. With the exception of two offences, however, all are triable either way and therefore punishable on conviction on indictment with a fine.

44. Criminal Attempts Act 1981, s.1(4).

PART VII

REFORMING THE PRESENT LAW (4): JURISDICTION

7.1 In this part we consider the question of the jurisdiction of the courts in England and Wales in relation to the main offences covering computer misuse, both existing and possible, which have been discussed in this paper. The general position will be outlined first, before considering the particular problems of computer misuse.

A. COMMON-LAW RULES OF JURISDICTION

7.2 The common-law rules which continue to govern issues of territorial jurisdiction in England and Wales provide that a crime is regarded as being committed where (and only where) its last element takes place.[1] In respect of "result-crimes" (that is, those requiring for their completion not only conduct of a specified nature but also that a particular result shall follow), jurisdiction is determined by the place where the proscribed consequence of the accused's physical acts occurs, not where those acts took place.[2] In respect of "conduct-crimes" (that is, those which are committed by the accused's conduct itself), jurisdiction is determined by the location of the accused's actions which constitute the offence.[3]

---

1. This approach is founded upon an ancient common law rule that an offence can only be committed in one place. See further, Glanville Williams, "Venue and the Ambit of the Criminal Law", (1965) 81 L.Q.R. 276, 395, 518.

2. For example, the offence of dishonestly obtaining property by deception, contrary to s.15 of the Theft Act 1968, is committed where the obtaining takes place: e.g. Baxter [1972] Q.B. 1.

3. For example, the offence of blackmail contrary to s.21 of the Theft Act 1968 is committed where the demand is made: Treacy [1971] A.C. 537 (H.L.).

7.3 Difficulties in determining whether the court has jurisdiction may arise in respect of result-crimes and conduct crimes. In relation to result-crimes, it is necessary to determine the location of the proscribed consequence of the accused's acts. In respect of conduct-crimes, two recent cases illustrate the problem. In Tomsett,[4] a telex operator employed by a Swiss bank at its London branch wrongfully diverted a sum of money in an account in New York to an account in Geneva that had been opened by his co-accused. This was held not to have resulted in a theft[5] (a conduct crime) triable in this country. In contrast, more recently, in R v Governor of Pentonville Prison, ex parte Osman,[6] the Divisional Court[7] held that the act of sending a telex is capable of amounting to appropriation for the offence of theft.[8] These cases appear to present difficulties because a person's "conduct" can be divided into his actions alone (operating the telex machine) and the direct consequence of those actions (the transfer of the money).[9]

B. PARTICULAR FEATURES OF COMPUTER MISUSE

7.4 An important feature of many computer systems is their ability to communicate with each other and to transmit

---

4. [1985] Crim. L.R. 369.

5. Contrary to s.1 of the Theft Act 1968.

6. The Times, 13 April 1988.

7. The judges in this case were Lloyd L.J. and French J., as in Tomsett [1985] Crim. L.R. 369.

8. The court added (Transcript, p.68) -

> "We do not rule out the possibility that the place where the telex is received may also be regarded as the place of appropriation, if our Courts were ever to adopt the view that a crime may have a dual location."

9. See Arlidge and Parry, Fraud (1985), para. 11.10.

rapidly large quantities of data between machines.[10] It is as easy for such communications or such a transfer to take place between computers in different countries as it is for it to take place within a country.[11] It would be possible, for example, for a person dishonestly to use a computer in this country to send a message to a computer in another country authorising a transfer of money there.[12] In such a case, it is unclear whether, on the general principles set out above, an English court would have jurisdiction to try an offence of theft or fraud. Similar jurisdictional problems might also arise in relation to any hacking offence which was introduced, and also in cases where a person deliberately (or recklessly) damages or destroys information stored on a computer. We consider these issues further below under the headings of computer fraud, hacking, and unauthorised alteration or erasure of data or software.

1. Computer fraud

7.5 In December 1987, the Criminal Law Team of the Law Commission issued a consultation paper which reviewed and made provisional proposals for the reform of the rules of law in England and Wales which determine whether a criminal court in this country has jurisdiction to try an offence of fraud connected with another country.[13] The Law Commission decided in July 1988 that this subject merited speedy

---

10. See para. 6.7 above.

11. See para. 1.15 above.

12. See for example the alleged attempt to defraud the Union Bank of Switzerland of £32 million: The Independent, 6 July 1988.

13. Jurisdiction over Fraud Offences with a Foreign Element (1987).

consideration by the Commission itself, and propose to produce a Report which will contain the Commission's final recommendations and which is likely to include draft legislation to give effect to them.

7.6 The Criminal Law Team's paper concluded that, for several reasons, the rules are in urgent need of reform. It suggested that they are antiquated, having evolved before the introduction of electronic and other modern methods of communication and transfer of money across national boundaries; that they are narrow, technical and insular in character; and that they sometimes call for detailed investigation into the facts of particular cases solely for the purpose of determining whether the court has jurisdiction. The paper invited comment on a number of changes that might be made by legislation to rationalise and update this area of criminal law.

7.7 The main proposal put forward by the Criminal Law Team was that, in relation to certain fraud offences,[14] the present jurisdictional rules should be abolished and replaced with a new rule along the lines of that proposed in Stephen's Draft Criminal Code of 1879, on which the jurisdictional rules of New Zealand are based.[15] Section 7 of the New Zealand Crimes Act 1961[16] provides that -

---

14. These include, among others, the offences under the Theft Acts 1968 and 1978 of theft, obtaining property by deception, obtaining a pecuniary advantage by deception, obtaining services by deception, evasion of liability by deception and false accounting.

15. Ibid., paras. 2.23 - 2.24.

16. Sect.6 of the Act provides that -

> "Subject to the provisions of section 7 of this Act, no act done or omitted outside New Zealand is an offence, unless it is an offence by virtue of this Act or any other enactment."

> "For the purpose of jurisdiction, where any act or omission forming part of any offence, or any event necessary to the completion of any offence, occurs in New Zealand, the offence shall be deemed to be committed in New Zealand, whether the person charged with the offence was in New Zealand or not at the time of the act, omission, or event."[17]

7.8 The Team also provisionally proposed, in the light of cases involving a conduct-crime such as Tomsett,[18] that the English courts should have jurisdiction in cases where a person by his use of "machinery" here (such as a telex machine or a computer) produces a direct effect abroad (or vice versa).[19]

7.9 Clearly if these proposals are implemented,[20] they would have a bearing on cases of computer fraud involving acts committed partly here and partly abroad. We do not think that our consideration of the problem of computer frauds in this paper[21] requires us to alter those proposals in any respect.

---

17. The effect of this proposal would be that if, for example, the accused was charged with the offence of obtaining property by deception (a result-crime) our courts would have jurisdiction if either his conduct constituting the deception or the obtaining of the property occurred in England and Wales.

18. [1985] Crim. L.R. 369. See para. 7.3 above.

19. See Jurisdiction over Fraud Offences with a Foreign Element (1987), para. 2.11. This recommendation would mean that a conduct-crime may also be regarded as being committed in more than one place, a conclusion which the Divisional Court in Osman (para. 7.3 above) left open.

20. The Team also made provisional proposals for extending jurisdiction in relation to conspiracy, incitement and attempt to commit offences of fraud, and common law conspiracy to defraud. However, we do not think it is necessary to go into the details of those proposals here.

21. See Part V above.

2. Hacking

7.10 If an offence were to be created for England and Wales penalising the obtaining of unauthorised access to a computer,[22] when should the court have jurisdiction? In each of the options suggested in Part VI of the paper,[23] in order to determine the question of jurisdiction under the present common-law rules, the court would have to decide where the last element of the offence took place. As we have seen,[24] this can create difficulties and it may be desirable to make special jurisdictional rules to govern any proposed new hacking offence.[25]

7.11 The Scottish Law Commission recommended that where an offence of obtaining unauthorised access to a computer[26] was committed partly in Scotland and partly in another country, the Scottish courts should have jurisdiction to try the offender irrespective of whether at the material time he was himself in Scotland or in that other country.[27] Clause 4 of the Draft Bill which accompanied the Commission's Report provided that -

> "A court in Scotland shall have jurisdiction to entertain proceedings for an offence under this Act if at the time the offence was committed -

---

22. See Part VI above.

23. See para. 6.20 above.

24. See the cases discussed in para. 7.3 above.

25. Several recent statutes have included special jurisdictional rules to govern the criminal offences created therein. See for example, Financial Services Act 1987, s.47 and the Banking Act 1987, s.35.

26. The proposed offence is set out in full in Appendix A, para. 17 below.

27. Report No. 106, paras. 5.13 - 5.14.

(a) the accused was in Scotland; or

(b) the program or the data in relation to which the offence was committed was stored in a computer in Scotland."

7.12 To return to the general question of jurisdiction in relation to hacking, a specific rule ought to deal with a number of issues.[28] For example -

(1) Should our courts have jurisdiction if a person in England and Wales obtains unauthorised access to a computer system abroad?[29]

(2) Conversely, should our courts have jurisdiction if a person abroad obtains unauthorised access to a computer system in England and Wales?

(3) Should our courts have jurisdiction if a person in (for example) Switzerland obtains authorised access to a computer in England and Wales but, through that computer, gains unauthorised access to a computer in the United States?

(4) Should it be an offence if a person abroad obtains unauthorised access to a computer system abroad and causes it to transfer (without authority) information to a computer system in England and Wales?

---

28. These issues would arise if hacking was criminalized, whatever definition of the new offence were to be adopted. The questions formulated therefore refer to the general definition of hacking used in this paper (para. 2.10 above).

29. For convenience we use the word "abroad" to signify any place outside England and Wales.

We make no provisional proposal in relation to any of these questions. We would welcome comments on whether a specific jurisdictional rule is desirable or not.

3. Unauthorised alteration or erasure of data or software

7.13 Offences of criminal damage[30] are only rarely likely to raise jurisdictional problems, but cases can be envisaged in which the accused's conduct occurs in one jurisdiction and the direct effect of that conduct, the damage, occurs in another. Perhaps one of the most likely instances where this might occur would be in the area of computer misuse. Just as hacking can be committed without heed to national boundaries, so too can a computer (or data and programs stored in a computer) be damaged. Application of the present rules of jurisdiction to offences of criminal damage would suggest that the English courts would have jurisdiction only if the property was damaged or destroyed here. It might be difficult to decide whether, for example, sending an instruction from a computer here to a computer in New York (or vice versa) ordering the unauthorised destruction of data stored on a computer disk, constituted the offence of criminal damage in England and Wales.

7.14 It would be possible to have a special provision which enlarged the jurisdiction of the English courts so as to cover cases where the property damaged was a computer or property connected with a computer. However, we think it would be undesirable to reform the jurisdictional rules in relation to offences of criminal damage in respect of particular types of property in this way. The question of the jurisdiction of our courts in relation to all offences of criminal damage raises issues beyond the scope of this exercise and therefore we are unable to consider the matter further.

---

30. Contrary to s.1(1) of the Criminal Damage Act 1971.

PART VIII
PROVISIONAL CONCLUSIONS AND SUMMARY OF POINTS FOR CONSULTATION

8.1 We end this paper with a summary of our provisional conclusions and the options for reform of the law on which we invite comments from all interested persons.

8.2 In the light of our study of the present law, our provisional conclusion is that the general criminal law is sufficient to deal with most of the computer misuse which we have identified (paras. 3.64 - 3.71). Our provisional view is that only two kinds of computer misuse might be said to justify an extension of the present scheme of offences (para. 4.1). The first would involve the amendment of one aspect of the Theft Acts which seems to us to be deficient in its application to certain kinds of computer fraud. The second is hacking, the obtaining of unauthorised access to a computer. Our provisional view is that a comprehensive computer crime statute is neither necessary nor appropriate in England and Wales (para. 4.3). The present scheme of criminal offences relating to theft, fraud and criminal damage encompass a broad range of factual circumstances and, in general, avoid distinctions based on the kind of property stolen and damaged (para. 4.3). Our provisional view is that there is no reason to change this policy in relation to computers.

A. FRAUD

8.3 Our examination of the existing criminal law relating to fraud suggests that, with one minor exception, computers create no special difficulties for the substantive law (paras. 3.2 - 3.11). The only problem that we have been able to identify relates to cases involving the "deception" of a computer (as opposed to a human being); but even there,

when property is obtained, a charge of theft or conspiracy to defraud (if two people are involved) will very often lie (para. 3.64). In an earlier paper[1] we suggested that this problem might be remedied by extending the definition of "deception" in the Theft Acts. We suggested an amendment on the following lines: a deception should include -

> "... inducing a machine to respond to false representations which the person making them knows to be false, as if they were true".

We would welcome comments on this provisional proposal.

B. HACKING

8.4 The principal issue raised in this consultation paper is whether the obtaining of unauthorised access to a computer by "hacking" should be a criminal offence. Such conduct is not an offence at present, although it may in certain limited circumstances amount to an offence under the Data Protection Act 1984 (paras. 3.58 - 3.60).

8.5 We make no provisional proposals on whether hacking should be an offence; we have tried in Part VI to set out the arguments on both sides. We would welcome views on whether it is felt that the present law is adequate to deal with hacking (paras. 6.15 - 6.16), or whether such conduct should be criminalized (paras. 6.8 - 6.14). Is the civil law, whether reformed or not, an effective remedy against hacking (paras. 6.4 - 6.6)? We would be interested to hear whether it is possible or likely that a hacker might inadvertently damage the target computer system, and whether it is possible for computer owners to guard satisfactorily against such risks (para. 6.18).

---

1. (1987) Working Paper No. 104, Conspiracy to Defraud, paras. 10.3-10.9.

8.6 If it is felt that a new offence should be created, we invite comment on whether it should be an offence along the lines of one of the four options suggested (para. 6.20). These are -

(1) First, an offence of obtaining unauthorised access to a computer in order to inspect certain kinds of information stored thereon (option A: paras. 6.25 - 6.28).

(2) Secondly, an offence of obtaining unauthorised access to a computer in order to inspect information stored thereon (option B: paras. 6.29 - 6.31).

(3) Thirdly, an offence of obtaining unauthorised access to a computer whereby damage to computer data or software is caused (but without the need to prove that the individual concerned intentionally or recklessly caused such damage) (option C: paras. 6.32 - 6.34).

(4) Fourthly, an offence of obtaining unauthorised access to a computer (option D: paras. 6.35 - 6.37).

8.7 General points relevant to all the options put forward include -

(a) How should hacking be defined so as to exclude both physical access to a computer and eavesdropping on a computer (para. 6.22)?

(b) Should "computer" be defined, even if only to exclude certain items (para. 6.23)?

(c) Should the concept of "authorisation" be defined further if it is used in the definition of a new offence (para. 6.24)?

(d) If a hacking offence is created, what jurisdictional rules should govern its operation? Should a specific jurisdictional rule be created, or should the matter be left to the common law? Should our courts have jurisdiction if either a person in England and Wales obtains unauthorised access to a computer abroad, or if a hacker abroad obtains unauthorised access to a computer in England and Wales? We make no provisional proposal, but would welcome views on this matter (paras. 7.10 - 7.12).

8.8 We invite comment on our provisional view that, were it decided to make hacking a criminal offence, it should only be triable in the magistrates' court, and should not be punishable with imprisonment (para. 6.38).

8.9 We provisionally propose that any such hacking offence should not extend to attempts to commit the offence (para. 6.39).

C. USING A COMPUTER FOR UNAUTHORISED PRIVATE PURPOSES

8.10 The present criminal law does not provide any special remedies for the use of computers by authorised users for unauthorised purposes, unless such conduct falls within one of the general fraud offences (paras. 3.33 - 3.34). Our provisional view is that there is nothing about the unauthorised use of a computer, as opposed to any other object or machine, which would justify the extension of the criminal law beyond its present limits in this area (para. 3.67).

D. UNAUTHORISED ALTERATION OR ERASURE OF DATA OR SOFTWARE

8.11 The law of criminal damage now seems to extend to persons who damage a computer system without the need for any further reform of the law (paras. 3.35 - 3.40). We would, however, welcome comments on whether this offence is felt to be appropriate to deal with "damage" caused to a computer program stored on a disk, tape or other physical medium. Our provisional view is that such activities can properly be said to fall within the meaning of "damage" for the purpose of the Criminal Damage Act 1971 (para. 3.38).

APPENDIX A

COMPUTER MISUSE: THE LAW IN OTHER JURISDICTIONS[1]

A. INTRODUCTION

1. The diverse responses to the problem of computer misuse in other jurisdictions are a result of a number of factors. These include the following -

(a) the legal instruments with which legal systems deal with such misuse vary;

(b) different jurisdictions have been affected by computer misuse in various different ways. In Canada, the United States and Australia the position is further complicated by federal-state relations. However, one prevailing trend revealed by the OECD Report on Computer-Related Crime was a tendency not to over-criminalize in almost all of the countries studied.[2]

2. Nonetheless, the overwhelming majority of jurisdictions which have dealt with the issue of computer misuse have come to the conclusion that some legislation is necessary. The Law Reform Commission of Tasmania maintained that -[3]

> "... such legislation would make it no longer necessary for prosecutors to 'shoe-horn' cases into existing common-law crimes ... which acknowledge neither the technical complexities of computers nor

---

1. The Commission is most grateful to Mr Edward Phillips LL.B., B.C.L., Lecturer in Law at the University of Buckingham, for his help in the preparation of this Appendix.

2. Organisation for Economic Co-operation and Development, Computer-Related Crime: Analysis of Legal Policy, Paris (1986) (hereafter the "OECD Report"). The study covered most European countries and included Turkey, the United States, Canada, Australia and New Zealand.

3. Law Reform Commission of Tasmania, Computer Misuse (1986), Report No. 47, para. 11. We consider the Tasmanian Report in some detail because Tasmania is one of the few Commonwealth jurisdictions to have produced a comprehensive review of all the issues in this new area of the law.

the new types of undesirable activity which involve computers."

3. The OECD Report noted that a minority of jurisdictions regard computer misuse as presenting no special features requiring any particular new measures; the computer was simply an instrument for committing an offences which already exist. The Report noted that this is the attitude adopted for the time being by Belgium,[4] Iceland and Japan.

4. An example of the attempt to "shoe-horn" cases into existing crimes may be taken from the Hong Kong case of R v. Siu Tak-Chee.[5] The defendant, a computer technician, had accidentially obtained the secret passwords to an electronic mail box data system. The defendant then gained unauthorised access to the system. He apparently did this without malice or ulterior motive, merely out of curiosity. Nonetheless, he obtained access to private and confidential information. The prosecution charged him, under section 15 of the Theft Ordinance, with an offence relating to the abstraction of electricity, in this case worth less than one eighth of a Hong Kong cent. The defendant pleaded not guilty, and after hearing all the evidence the magistrate found the defendant guilty. However, in view of the small amount of electricity consumed, the magistrate discharged the defendant unconditionally and ordered that no conviction be recorded, adding that the prosecution should never have been brought.

5. In formulating legislative responses to computer misuse, at least three alternatives become apparent from the approaches adopted in other jurisdictions.[6]

---

4. Under Belgian law all public telephone and telegraphic communications are protected against tampering with messages, against the destruction of messages, and against unauthorised access to the contents of messages: this is apparently seen as including computer networks.

5. (1984), referred to in the Tasmanian Report, para. 7(ii).

6. See e.g. OECD Report, p.12 and pp.38-39; Report on Computer Crime (1987), Scot. Law Com. No. 106, paras. 3.9 - 3.12; and the discussion in this paper, paras. 4.2 - 4.7 above.

1. The "evolutionary" approach

6. By "evolutionary" we mean applying the general criminal law and restricting legislative change to the expansion of existing concepts and definitions to include certain types of computer misuse.

7. An "evolutionary" approach appears to have been followed in the Green Paper issued by the Queensland Government in 1987 on Computer Related Crime and the Queensland Criminal Code.[7] The OECD Report also found that this approach had been adopted in the American States of Alaska, Massachusetts, Ohio and Virginia.[8]

8. In Switzerland the Swiss Committee of Experts for the Revision of the Penal Code has proposed legislative amendment to section 150 of the Swiss Penal Code on the unauthorised use of services to cover a service to which "a data processing system applies or which an automatic device arranges."[9]

9. In the Australian context this approach has been criticised[10] on the following grounds -

(a) There must be certainty in the law. It is no answer to say that existing law is adequate; there are many grey areas.

(b) There must be effective deterrence. This cannot be achieved by the manipulation of sometimes esoteric offences in a piecemeal fashion.

(c) The penalties for computer-related crime must be commensurate with the overall economic damage which is

---

7. See p.6.

8. OECD Report, p.39.

9. OECD Report, p.58. Two statutes already exist at Federal level which, consistent with the Swiss approach, do not specifically involve computer-related offences but strengthen the protection of privacy in the processing of personal data.

10. Temby and McElwaine, "Technocrime - An Australian Overview", (1987) 11 Crim. L.J. 245.

caused by the particular wrongful conduct. The penalties available for traditional property offences, for example, may not be flexible enough.

2. Enacting computer-specific offences to "fit" into existing statutes

10. This is the approach favoured by the Law Reform Commission of Tasmania. They proposed, for example, a new offence of "damaging computer data" which would fit into the general provision of "unlawfully injuring property" under section 273 of the Criminal Code. The Commission specifically rejected the approach described above of simply amending the definition of property (in section 1 of the Code) to include "data".

11. Two European examples may be given. In West Germany, the Penal Code was amended in 1987 to include an additional fraud offence of "computer fraud".[11] The offence is defined partly in terms of the entry of incorrect or incomplete data into a computer. A further example is the Swedish Data Act 1973 (as amended in 1982). Although this is sometimes referred to as a computer-specific statute, in reality the computer provisions form part of the general provisions relating to the privacy of personal data files.[12]

3. Enacting computer-specific statutes

12. This is the solution which has either been adopted, or proposed, in a substantial number of jurisdictions. The majority of American states already possess such computer-specific statutes, following the example of Florida, which enacted the Computer Crimes Act 1978, one of the earliest computer-specific statutes.[13] In April 1987, the International Computer Law Adviser reported that every state except Arkansas, Vermont and West Virginia had enacted such statutes.[14] In addition there is the Federal Computer Fraud

---

11. Sect.263a.

12. It is an interesting point that, in its response to the OECD study, Sweden took the view that creating special rules for computer-related crime must be avoided and general provisions in criminal law used as far as possible: OECD, Report, p.19.

13. See further para. 33 below.

14. Vol. 1, No.7, p.16.

and Abuse Act 1984 (USCA, Title 18), which specifically addresses the issue of unauthorised access.[15]

13. Among current proposals for such statutes is the Israeli Draft Computer Act, recently distributed for comments by the Israeli Ministry of Justice.[16]

14. The Law Reform Commission of Tasmania did not favour the introduction of a separate computer-specific criminal statute because, they suggested, this would -

(a) tend to place undue emphasis on the presence of the computer in the facts of a particular case, rather than highlighting the anti-social aspects of the activity being criminalized,

(b) and may make it difficult for the prosecution and the defence to rely upon the legal principles and concepts embodied in the Criminal Code, which have had the benefit of much judicial and legislative consideration and improvement.[17]

B. CATEGORIES OF MISUSE

1. Unauthorised access

15. It appears to be common ground, among the jurisdictions which have considered the issue, that the main mischief to be addressed is that of unauthorised access. We now look at some of those jurisdictions in which an offence of unauthorised access has been introduced or recommended, and then consider other categories of computer misuse.

---

15. See para. 21 below.

16. International Computer Law Adviser (1988), Vol. 2, No. 6, p.4.

17. Report No. 47, para. 11.

16. The Scottish Law Commission identified eight different categories of computer misuse.[18] However, their final recommendation was that only unauthorised access should be criminalized; the other categories of computer misuse were either capable of being dealt with by existing law or, they thought, should not be criminalized at all. Furthermore, the manner in which the proposed offence of unauthorised access was couched covered most of the other categories. For instance, as far as "eavesdropping" on a computer was concerned, the Commission pointed out that some forms of what they considered to be eavesdropping could be regarded as examples of unauthorised access.

17. Accordingly the final proposal in the Bill presented with the Commission's Report appears as follows -

> "1(1) A person commits an offence if, not having authority to obtain access to a program or data stored in a computer, or to a part of such program or data, he obtains such unauthorised access in order to inspect or otherwise to acquire knowledge of the program or the data or to add to, erase or otherwise alter program or the data with the intention -
>
> (a) of procuring an advantage for himself or another person; or
>
> (b) of damaging another person's interest.
>
> (2) A person commits an offence if, not having authority to obtain access to a program or data stored in a computer, or to a part of such program or data, he obtains such unauthorised access and damages another person's interests by recklessly adding to, erasing or otherwise altering the program or the data.
>
> (3) For the purposes of this section, a person does not have authority to obtain access to a program or data stored in a computer, or to a part of such program or data, if he does not have the authority of a person entitled to control such access."

18. The Canadian Criminal Law Amendment Act 1985[19] also addresses

---

18. See Report on Computer Crime (1987), Scot. Law Com. No. 106, para. 2.1.

19. Amending the Criminal Code, and based, with modifications, on recommendations in the Report of the Canadian House of Commons Standing Committee on Justice and Legal Affairs' Subcommittee on Computer Crime.

the issue of unauthorised access but in narrower terms than the Scottish Law Commission's recommendations -[20]

> "Everyone who, fraudulently and without color of right,
>
> (a) obtains, directly or indirectly, any computer service,
>
> (b) by means of an electromagnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system ...
>
> is guilty of an indictable offence ..."[21]

However, the Act also introduced a new form of "mischief" to cover the unauthorised modification or destruction (without apparent right) of computerised data -[22]

> "Everyone commits mischief who wilfully
>
> (a) destroys or alters data;
>
> (b) renders data meaningless, useless or ineffective;
>
> (c) obstructs, interrupts, or interferes with the lawful use of data; or
>
> (d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto."

19. The proposals of the Law Reform Commission of Tasmania follow much the same pattern of a narrowly defined access offence coupled with the creation of other specific offences to deal with other categories of misuse. Their recommendation takes the following form -[23]

> "Any person who, without authority, knowingly gains access to a computer, computer network, or any part thereof is guilty of a crime."

---

20. Sect.301.2(1) Canadian Criminal Code.

21. For the purposes of the new section 301, the Act contains a definition of "computer system".

22. Sect.387(1.1).

23. Report No. 47, para. 8, p.25. "'Access' includes to communicate with a computer."

This proposal for unauthorised access is intended to exclude unauthorised use, which receives separate treatment as a different offence.[24]

20. Section 9 of Victoria's Crimes (Computer) Act 1988 provides for a new offence of "Computer Trespass". It states -

> "A person must not gain access to, or enter, a computer system or part of a computer system without lawful authority.
>
> Penalty: 25 penalty units or imprisonment for 6 months."

The offence does not contain any further definitions of the terms used.

21. The U.S. Federal Computer Fraud and Abuse Act 1984 is more specific in setting out its unauthorised access offences. Section 1030 of Title 18 defines unauthorised access as criminal if an individual does the following -

> "(a)(1) Knowingly ... obtains information that has been determined by the U.S. Government to require protection against unauthorised disclosure for reasons of national defence or foreign relations ...
>
> (2) Intentionally ... obtains information contained in a financial record of a financial institution ... or contained in a file of a consumer reporting agency.
>
> (3) Intentionally accesses[25] a computer without authorisation if such computer is exclusively for the use of the Government of the U.S. or in the case of a computer not exclusively for such use, if such computer is used by or for the Government of the U.S. and such conduct affects such use.
>
> (4) Knowingly and with intent to defraud accesses a Federal interest computer[26] without authorisation ... and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer.

---

24. Ibid., para. 7, p.24. See further para. 27 below.

25. The term "access" is not defined.

26. It should be noted that the U.S. statute takes the particular form of referring only to the "Federal interest" or federal computers because of the constitutional federal-state relationship.

> (5) Intentionally accesses a Federal interest computer without authorisation, and by means of one or more instances of such conduct alters information in that computer or prevents authorised use of that computer, and thereby causes loss to one or more others ... or modifies or impairs ... the medical examination ... diagnosis ... treatment ... or care of one or more individuals.
>
> (6) Knowingly and with intent to defraud trafficks ... in any password or similar information through which a computer may be accessed without authorisation if (a) such trafficking affects interstate or foreign commerce; or (b) such computer is used by or for the Government of the U.S."

This statute makes it clear that, except in the case of access to a computer "exclusively for the use of the Government" (s.1030(a)(3)), unauthorised access alone is not sufficient and that it must be linked to some other wrongful activity.

22. Other jurisdictions have felt it necessary to penalise mere unauthorised access generally. The OECD Report mentions[27] the Swedish Data Act 1973 as the first piece of legislation criminalizing mere unauthorised access.[28] Since the publication of that report, France has introduced a new law which provides that any entry into a computer system is an offence.[29] The Californian Penal Code penalises everyone who -[30]

> "Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network."

The maximum penalty is a fine of $5,000 or one year's imprisonment or both.

---

27. At p. 61.

28. Sect. 23 states: "Any person who unlawfully procures access to a recording for automatic data processing or unlawfully alters or obliterates or enters such a recording in a file shall be sentenced for data trespass."

29. Law number 88-19 (5 January 1988).

30. Sect.502(c)(7).

23. In considering the scope of the proposed unauthorised access offence, the Scottish Law Commission examined the question of practical authorisation and unauthorised access by employees. The Commission considered the position of an employee who is not authorised to have access to certain parts of a computer's stored data, and came to the conclusion that no fine distinctions were to be drawn. This would be equally true of those computers which allow only a limited amount of public access. Accordingly, the Commission recommended that the proposed offence should specifically refer to -[31]

> "... the obtaining of access to a program or data, or to a part of such program, or data, to which the person in question is not authorised to obtain access."

24. The Australian Review of Commonwealth Criminal Law concluded that "the most likely form of unauthorised access would clearly appear to be access by a person having some degree of authority to access, but exceeding that authority".[32] Their Discussion Paper suggested that this was one possible argument against legislative action; that such persons can usually be dealt with by some form of disciplinary action. Nonetheless, "outsiders" would be immune from disciplinary action and the question arose as to whether disciplinary action would be a sufficient sanction.

25. The U.S. Federal Computer Fraud and Abuse Act 1984[33] adopts the solution of specifically including a definition of "exceeds authorised access" as meaning -[34]

> "to access a computer with authorisation and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter."

---

31. Report No.106, para. 4.18.

32. (1988), Discussion Paper No.12, para. 4.4.

33. See para. 21 above.

34. S.1030(e)(6). Cf. Clause 1(3) of the Scottish Law Commission's draft Bill, set out at para. 17 above.

26. It is interesting to note that the U.S. statute originally contained a provision that no offence would be committed by someone who -

> "... having accessed a computer with authorisation and using the opportunity such access provides for purposes to which such access does not extend, if the using of such opportunity consists only of the use of the computer."

This provision was deleted in 1986.

2. Other categories of misuse

27. The Law Reform Commission of Tasmania proposed five new offences, in addition to the offence dealing with unauthorised access -

(i) Computer fraud: fraudulently obtaining a financial or other advantage or causing a detriment to another by the manipulation of data.

(ii) Damaging computer data: damaging, destroying, erasing or rendering meaningless, data.

(iii) Unauthorised use: unauthorised use of a computer.

(iv) Insertion of false information as data.

(v) Omission to record or store data where there is a duty to do so.[35]

---

35. In regard to the last-mentioned offence, the Commission concluded that the potential for harm resulting from the failure of someone to record or store data in a computer where they are under a duty to do so may be as great if not greater than the positive act of putting false or misleading information into the computer. The Commission pointed out that there were already similar provisions in Tasmania. They were emphatic that it was not their wish to criminalise simple negligence or forgetfulness. Accordingly, they set out a proposal which would take this into account -

"Any person under a contractual or other duty to introduce, record or store data into a computer or computer network, knowingly and dishonestly fails to so introduce, record or store, is guilty of a crime."

28. This point was considered in the Australian Commonwealth Discussion Paper which explored the existing Australian law on the matter. Under section 72 of the Australian Crimes Act, it is an offence for a Commonwealth officer fraudulently and in breach of his duty (a) to omit to make an entry in any book, record or document, and (b) by act or omission to falsify any book, record or document. The Review Committee felt that this provision could well cover the point at issue. Their tentative conclusion, therefore, was to avoid creating a new offence and to leave it to section 72 of the Crimes Act coupled with existing disciplinary procedures.

29. The Law Reform Commission of Tasmania stopped short at proposing to criminalize two types of computer misuse: first, "eavesdropping", and, second, the failure on the part of a computer system owner or manager to take adequate steps to safeguard private and confidential information relating to third parties that is held within that computer system.

30. Another category of misuse that has been identified in some jurisdictions and adopted as an addition or alternative to unauthorised access is the "theft of computer time". The OECD Report noted that many of the American state statutes incorporate "time theft" in their general provisions on computer crime prohibiting unauthorised access.[36]

31. This concept of computer time was utilised in US v. Sampson.[37] The defendant had used his home telephone line to gain access to a US Government computer without intending to pay for its use. He was discovered and charged under Title 18 USC 641 which states -

> "Whoever embezzles, steals, purloins, or knowingly converts to his own use or that of another, or without authority, sells, conveys or disposes of any record, voucher, money or other thing of value of the United States ..."

shall be guilty of an offence. The defendant admitted use of the computer for an average of 6 hours per week for 32 weeks and was

---

36. OECD Report, p.58.

37. (1976) 6 Computer Law Service Reporter 879; discussed in Brown, "Crime and Computers" (1983) 7 Crim. L.J. 68.

charged with stealing "things", that is, computer time and storage capacity. This conviction was upheld.

32. The sort of problems faced by utilising this concept may be illustrated by the Virginia case of Lund v. Commonwealth.[38] The defendant had used over $26,000 in computer time (this was based on the rental cost of the computer which had been accessed) and was convicted under the state larceny statute. The Supreme Court of Virginia, however, reversed his conviction on a strict interpretation of the statute, which did not include services as a proper object of larceny.

33. The Florida Computer Crimes Act 1978 does not use the concept of unauthorised access. Instead, the Act provides for "offences against intellectual property".[39]

> "(1) Whoever wilfully, knowingly, and without authorization modifies data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offence against intellectual property.
>
> (2) Whoever wilfully, knowingly, and without authorization destroys data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offence against intellectual property.
>
> (3) Whoever wilfully, knowingly, and without authorization discloses or takes data, programs, or supporting documentation which is a trade secret as defined in para. 812.081 or is confidential as provided by law residing or existing internal or external to a computer, computer system, or computer network commits an offence against intellectual property."

In addition, provision is also made for offences against "computer equipment or supplies",[40] and against "computer users".[41]

---

38. 217 Va. 688; discussed in Menelly, "Prosecuting Computer-Related Crime", (1985) 8 Boston College International and Comparative Law Review 551, 566.

39. Para. 815.04.

40. Para. 815.05.

41. Para. 815.06.

34. It appears that few jurisdictions have felt it necessary to enact legislation to cover the commission of traditional offences by means of a computer. Two examples are described here, Canada and the Australian Capital Territory. Of special interest also is the Victoria Crimes (Computer) Act 1988. Section 6 amends the Crimes Act 1958 and provides that "deception" -

> "(b) includes an act or thing done or omitted to be done with the intention of causing -
>
> (i) a computer system; or
>
> (ii) a machine that is designed to operate by means of payment or identification -
>
> to make a response that the person doing or omitting to do the act or thing is not authorised to cause the computer system or machine to make."

35. In Canada, the Criminal Code now makes it an offence, in section 301.2(1)(c), for anyone who "fraudulently and without color of right" uses a computer system with the intent to commit mischief in relation to -

> "(a) destroying or damaging property;
>
> (b) rendering property dangerous, useless, inoperative or ineffective;
>
> (c) obstructing, interrupting or interfering with the lawful use, enjoyment or operation of property... "

36. The Australian Capital Territory Crimes (Amendment) Ordinance (No. 4) 1985 addresses the issue of fraud perpetrated by means of a computer -[42]

> "A person who by any means, dishonestly uses, or causes to be used, a computer or other machine, or part of a computer or other machine, with intent to obtain by that use a gain for himself or herself or another person, or to cause by that use a loss to another person, is guilty of an offence ..."

37. The main difficulty in the formulation of computer-specific offences is the problem of formulating provisions that satisfactorily

---

42. Sect.115(1).

distinguish between substantial misuse and instances of trivial unauthorised access or use. The Review of (Australian) Commonwealth Criminal Law Discussion Paper put forward the tentative suggestion that one course would to be enact a provision prohibiting unauthorised access in unqualified terms, that is, "mere" unauthorised access, and relying on prosecutorial discretion in cases of trivial misuse.[43] The Review Committee accepted that this would not be a satisfactory solution.

3. Defences

38. The various computer misuse statutes as well as the proposals put forward by the reform bodies contain a number of defences. The most obvious and non-controversial of these is the "official authorisation" defence.

39. The U.S. state statutes generally contain defence provisions. There, the widespread use of computers by employees has been responsible for a number of provisions that make it clear that any authorised use of a computer cannot give rise to liability. An example may be taken from the Californian Penal Code where section 502(i)(1) provides that offence provisions do not apply -

> "to any person who accesses[44] his or her employer's computer system, computer network, computer program, or data when acting within the scope of his or her lawful employment."

Even when acting outside the scope of employment, the employee receives some measure of protection. Section 502(i)(2) provides that the offence provisions do not apply -

> "... to any employee who accesses or uses his or her employer's computer system, computer network, computer program or data when acting outside the scope of his or her lawful employment, so long as the employee's activities do not cause an injury ... to the employer or another, or so long as the value of computer services ... do not exceed one hundred dollars."

---

43. Discussion Paper No.12, para. 7.11.

44. Under s. 502(b)(1) "access" means to gain entry to, instruct or communicate with the logical, arithmetical, or memory function resources of a computer, computer system or computer network."

40. Connecticut law goes slightly further and expressly creates "authorisation" as an affirmative defence, providing that -[45]

> "It shall be an affirmative defence to a prosecution for unauthorised access to a computer system that a person reasonably believed that the owner of the computer system, or a person empowered to license access thereto, would have authorised him to access without payment of any consideration, or that person reasonably could not have known that his access was unauthorised."

41. New York law allows as a defence the argument that the defendant had reasonable grounds to believe that he or she was authorised to use a computer, while Texas law specifically exempts employees of communication and electric utilities from liability so long as their actions were in the course of employment and necessary to protect the property of their employer.[46]

42. The Scottish Law Commission considered that there would be circumstances where official investigating authorities, such as the police, should be authorised to obtain access to a computer without the knowledge or authority of the computer owner. The defence was formulated in the Commission's Draft Bill as follows -

> "1(4) ... a person shall not commit an offence ... if he obtains such access ... in pursuance of a warrant issued by the Secretary of State ...
>
> 2(1) ... the Secretary of State may issue a warrant requiring the person to whom it is addressed to obtain access to a program or data stored in a computer, or to any part of such program or data, for the purpose of acquiring information; and such a warrant may also require the person to whom it is addressed to disclose any information so acquired to such persons and in such manner as are described in the warrant."

Clause 2(2) then goes on to provide that such a warrant will only be issued (a) in the interests of national security (b) for the purpose of

---

45. (1987) International Computer Law Adviser, Vol. No.7, p.18.

46. Ibid.

preventing or detecting serious crime, or (c) for the purpose of safeguarding the economic well-being of the U.K.[47]

43. The Law Reform Commission of Tasmania did not put forward any provision relating to defences. Neither did the Australian Commonwealth Review Committee.

4. Penalties

44. A comparison of the penalties attached to computer misuse in the various jurisdictions reveals a wide disparity. While this may be a useful guide to the perceived seriousness or otherwise of computer misuse, little is to be gained from any attempt at a comprehensive listing of potential sentences. Accordingly, only a number of examples will be described.

45. Section 115 of the Australian Capital Territory Crimes (Amendment) Ordinance (No. 4) 1985, which deals with dishonest use of computers for gain,[48] provides for a maximum term of imprisonment of 10 years.

46. The U.S. Federal statute contains complex sentencing provisions with some offences carrying sentences of not more than one year, some for not more than 10 years, while some offences carry sentences for not more than 20 years. The severity of the sentences are related to a number of criteria, including the type of computer unlawfully accessed, the type of information unlawfully obtained, the level of damage caused to the computer owner and the mental element with which the unauthorised access was perpetrated.

47. The Scottish Law Commission recommended for their proposed unauthorised access offence a maximum penalty of five years' imprisonment on indictment (six months' on summary conviction) or an unlimited fine (the statutory maximum on summary conviction) or both.

---

47. This proposal was based on similar provisions in the Interception of Communications Act 1985 relating to warrants for "telephone-tapping".

48. See para. 35 above.

(They had originally proposed 3 months' imprisonment on summary conviction and 2 years' on indictment.)

48. The Law Reform Commission of Tasmania felt that there was no need to propose separate sentencing provisions for their proposed computer-related crimes, leaving it to the general provisions of the Tasmanian Criminal Code.

49. The Californian Penal Code provides for seizure and forfeiture of both hardware and software -[49]

> "Any computer, computer system, computer program, instrument, apparatus, device, plans, instructions or written publication used in the commission of any (offence) ... may be seized under warrant or incident to a lawful arrest. Any property seized ... is subject to forfeiture."

50. Similar provision is to be found in the Draft Israeli Bill, with the added protection that seizure is only permitted by order of the court.

C. DEFINITIONS OF "COMPUTER"

51. For the reasons given in the main part of this paper,[50] our provisional view is that it is unnecessary to define "computer" for the purposes of any new offence. However, some jurisdictions either provide a definition or have such a definition under consideration.

52. The Law Reform Commission of Tasmania proposed the following non-exhaustive definition -[51]

> "... 'computer' includes any device which is capable of performing logical, arithmetical, classificatory, mnemonic, storage or other like functions by means of optical, electronic or magnetic signals."

---

49. Sect.502(h).

50. See para. 6.23 above.

51. Report No. 47, p.12.

53. More elaborate treatment is given in the U.S. Federal Computer Fraud and Abuse Act 1984 -[52]

> "... the term 'computer' means an electronic, magnetic, optical electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device ..."

54. The Draft Israeli Bill goes slightly further and includes also "ancillary equipment and communications system connected to" a computer.

55. To the question whether a calculator or similar device is also a computer, the U.S. Federal Computer Fraud and Abuse Act 1984 provides an answer in the latter part of s.1030(e)(1) which provides that 'computer' does not include "an automatic typewriter or typesetter, a portable hand held calculator, or other similar device".

56. The Californian legislation also addresses this particular problem, albeit in a limited manner, in its definition of "computer system" as meaning -[53]

> "... a device or collection of devices, including support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions including, but not limited to, logic arithmetic, data storage and retrieval, communication, and control."

57. Many jurisdictions in an attempt at comprehensiveness have also provided similar definitions of terms ancillary to that of "computer". For instance the Californian statute goes on to define the following -[54]

> "(2) 'Computer network' means two or more computer systems connected by telecommunication facilities.

---

52. Sect.1030(e)(1).

53. S.502(b)(5).

54. Sect.502(b).

(3) 'Computer program or software' means a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions."

58. Although the Canadian Criminal Code contains no definition of "computer", the Code was amended by the Criminal Law Amendment Act 1985 to provide the following definitions in s.301 2(2) -

"... 'computer program' means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function.

'computer system' means a device that, or a group of inter-connected or related devices one or more of which:

(a) contains computer programs or other data, and

(b) pursuant to computer programs,

(i) performs logic and control, and

(ii) may perform any other function."

APPENDIX B

DUTY TO DISCLOSE INCIDENTS OF COMPUTER MISUSE

One issue which the Scottish Law Commission among others have raised is whether or not there should be a legal duty placed on computer users to disclose incidents of computer crime of which they have been the victims.[1] In their consultative memorandum the Commission said that they were not persuaded that there was a case for the imposition of such a duty. Most commentators agreed with the Commission, but some argued strongly that such a duty should be imposed. In our view the question whether there should be a duty to report certain kinds of crime raises issues beyond the scope of a paper on computer misuse. For convenience, however, we reproduce here the Scottish Law Commission's summary of the arguments for and against compulsory disclosure -[2]

For

"(a) Non-disclosure by the victims of computer crime simply encourages other wrongdoers to have a go.

(b) Non-disclosure means that the applicability, and possible need for reform, of existing law can never adequately be tested.

(c) Non-disclosure means that computer users who have not yet been the victims of computer crime are less alive than they should be to the need to take adequate steps to protect their own systems.

(d) Non-disclosure (where the victim is a company with shareholders) may mean that, with the help of "creative" accounting, shareholders are kept in ignorance of losses sustained by the company: they are therefore unable to consider, and if appropriate call in question, the adequacy of the management of the company."

---

1. Consultative Memorandum No. 68, paras. 6.17-6.20; Report No. 106, paras. 5.8-5.11.

2. Report No. 106, paras. 5.9 and 5.10.

Against

"(a) There is no general duty to disclose crimes, and there is no sound reason why there should be a duty to disclose computer crimes but not, for example, rape or assault.

(b) It would be impossible to define what is meant by "computer crime" for this purpose. Bearing in mind that the degree of computer involvement in traditional crimes like fraud or theft may vary from the negligible to the very considerable, the duty might have to extend to all frauds or thefts, but that in turn would mean that there would be a duty to report the theft of even an office pencil. This problem could, of course, be avoided by providing that the duty should only apply in respect of losses above a certain value, but it is difficult to discern any sound principle which would justify drawing such an arbitrary dividing line.

(c) Any duty of disclosure would be virtually unenforceable since, if the loss itself is concealed, it is most unlikely that the failure to disclose it would ever be discovered.

(d) While it is conceded that there may be problems for shareholders if a company fails to reveal losses caused by crime, this is a general problem and not just one arising from computer crime."

Printed in the United Kingdom by Her Majesty's Stationery Office at Basildon Rep Unit
Dd 290893 C15 8/88

HMSO publications are available from:

HMSO Publications Centre
(Mail and telephone orders only)
PO Box 276, London, SW8 5DT
Telephone orders 01-622 3316
General enquiries 01-211 5656
(queuing system in operation for both numbers)

HMSO Bookshops
49 High Holborn, London, WC1V 6HB 01-211 5656 (Counter service only)
258 Broad Street, Birmingham, B1 2HE 021-643 3740
Southey House, 33 Wine Street, Bristol, BS1 2BQ (0272) 264306
9-21 Princess Street, Manchester, M60 8AS 061-834 7201
80 Chichester Street, Belfast, BT1 4JY (0232) 238451
71 Lothian Road, Edinburgh, EH3 9AZ 031-228 4181

HMSO's Accredited Agents
(see Yellow Pages)

and through good booksellers

£4.50 net

ISBN 0 11 730192 2