The Law Commission

(LAW COM. No. 186)

CRIMINAL LAW

COMPUTER MISUSE

Presented to Parliament by the Lord High Chancellor
by Command of Her Majesty
October 1989

LONDON
HER MAJESTY'S STATIONERY OFFICE
£5.60 net

Cm 819

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 Commissioners are—
The Honourable Lord Justice Beldam, *Chairman*
Mr. Trevor M. Aldridge
Mr. Jack Beatson
Mr. Richard Buxton, Q.C.
Professor Brenda Hoggett, Q.C.

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.

COMPUTER MISUSE

CONTENTS

COMPUTER MISUSE

Summary

In this report the Law Commission reviews the nature and extent of computer misuse as it affects the criminal law of England and Wales, and makes recommendations for the creation of three new substantive offences of computer misuse.

THE LAW COMMISSION

Item 5 of the Fourth Programme: Criminal Law

COMPUTER MISUSE

To the Right Honourable the Lord Mackay of Clashfern, Lord High Chancellor of Great Britain

PART I

INTRODUCTION

A. THE NATURE OF THE SUBJECT

1.1 An increasing degree of interest and disquiet has become apparent in recent years in relation to the implications of, and the possible misuse of, the computerisation that plays an ever growing role in public, commercial and indeed in private life. In this report we are concerned with one aspect of that public concern: the misuse of computers or computer systems[1] by parties other than those entitled to use or control those computers, either by simply seeking access to the computers, or by going further and using the computers or amending the information held in them for what may be a wide range of ulterior motives. Such conduct can be generically described by the title of this report, 'Computer Misuse'.

1.2 In Part I of our Working Paper No. 110, *Computer Misuse*,[2] issued in September 1988, we summarised the technical background to the enquiry, and the terminology commonly used in discussing computers. We do not think that we need to repeat those matters here. We also indicated, and our subsequent work has confirmed that view, that the subject was one of particular difficulty.

1.3 That difficulty stems not only from the rapidly changing and developing nature of computer technology, but also from the new problems that that technology, and the misuse of it, pose for the criminal law. Before the criminal law is extended to deal with a newly apparent social problem it is necessary to be as certain as possible about the nature and extent of that problem; to be satisfied that the problem is not already met by existing legal sanctions whether civil or criminal; and to be satisfied that the particular and coercive remedies of the *criminal* law are appropriate to the requirements of the case. It is for these reasons that a wide variety of opinions have been expressed as to the extent to which, if at all, the criminal law needs to or should intervene further in this area. For these reasons also it is in our view particularly important to identify as closely as possible the exact forms of activity which are sought to be prevented by sanctions directed against 'computer misuse', and the practical effect that such sanctions may be expected to have. We have sought to keep those considerations carefully in mind in making and explaining the recommendations that are submitted in this report.

B. EVENTS LEADING UP TO THIS REPORT

1.4 Concern about computer misuse is of comparatively recent origin, not only in the United Kingdom but also in countries that have already enacted computer-specific criminal legislation;[3] and the current widespread and vigorous advocacy of such legislation in this country also has to a large extent developed since we first became engaged on the subject.

1.5 So far as the United Kingdom is concerned, in 1987 we published a consultation paper on Conspiracy to Defraud[4] in which we acknowledged the potentially serious consequences of computer misuse but confined ourselves 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.[5] The paper raised a number of issues in the more general context of computer misuse, and so we began a separate examination of the subject.

---

[1] In this report we will for convenience, except where the context clearly makes the usage inappropriate, refer to both computers and computer *systems* by the general description of "computer".

[2] Hereafter, W.P. No. 110.

[3] A survey of such legislation will be found in Appendix A to W.P. No. 110.

[4] Working Paper No. 104.

[5] See *ibid.*, paras 4.9–4.14 and 10.3–10.9.

1.6 In July 1987 the Scottish Law Commission presented a report on computer crime, pursuant to a proposal made by the Law Society of Scotland in July 1984.[6] In that report two new offences were recommended, each relating to the obtaining of unauthorised access to a program or data stored in a computer. First, it should be a crime to obtain such access in order to inspect, add to, alter or corrupt the data or program, with intent either to obtain an advantage for oneself or another person, or to damage another person's interests; secondly, it should be a crime to obtain such unauthorised access and damage the program or data, or another person's interests, by recklessly altering, corrupting, erasing, or adding to the program or data.

1.7 In September 1988 we published a working paper on computer misuse[7] which examined the applicability and effectiveness of the existing law of England and Wales in dealing with instances of computer misuse; and sought the views of interested persons on what, if any, reform of the criminal law was required in this area. The paper was widely circulated and attracted a great deal of interest. We received comments and suggestions from over one hundred individuals and organisations, and we are grateful to all of them for the help that they gave us. A full list of those who commented on the paper will be found in the Appendix to this report.

1.8 However, despite the length and detail of many of the replies, and the strong opinions that were expressed, we found the results of the consultation disappointing in one important respect.

1.9 We had indicated in paragraph 6.1 of W.P. No. 110 that we regarded the main issue arising for consideration in our study to be: Should the obtaining of unauthorised access to a computer be a criminal offence? Although the simplicity of this question conceals a certain number of difficulties, which we discuss below, for present purposes it sufficiently describes the activity colloquially referred to as computer 'hacking', an expression that we use in this sense in this report. Those replying to the consultation agreed with our assessment, and also urged, by an impressive majority, that such an offence, in some form, should indeed be introduced. We however had in paragraph 6.18 of W.P. No. 110 pointed to the then lack of evidence, which had also been perceived by the Scottish Law Commission,[8] in relation to the nature and extent of, and the particular damage caused by, computer misuse in general and hacking in particular. We specifically requested that we should be provided with 'chapter and verse' on these points, to enable us to assess the reasons put forward in support of new legislation, and the degree of urgency with which any such legislation was required.

1.10 Most of the replies to the consultation were however far from explicit in these respects. We understand and appreciate the reasons for that diffidence. The phenomenon of hacking involves consideration of the security devices used on computer systems; the success or failure of hackers in overcoming such devices; and the commercial implications of such activities; publication of details of these matters could be technically damaging and commercially embarrassing for the operators concerned. Nonetheless, we considered that we could not properly form a view, and report, without further specific evidence of the nature of the problems caused by hacking. Accordingly, after the consultation had closed in March 1989 we arranged a series of meetings with computer and software manufacturers, computer users in commerce, industry and the banking and financial sectors, and those responsible for seeking to apply the existing criminal law to cases of computer misuse, in order to seek a better understanding of the problems that had evoked the expression of opinion on consultation to which we have referred above.

1.11 We have gained the greatest benefit from these further discussions, and are very grateful to all those who went to considerable trouble to assist us. These discussions increased our understanding of the facts underlying the issue of computer hacking and have enabled us to form a clear judgment upon them. A good deal of this information was given to us in confidence, and we are therefore not able to cite identifiable cases in this report. We would, however, like to confirm that we have not approached the further submissions made to us in any way uncritically, but in order to form an

---

[6] Report on Computer Crime, Scot. Law Com. No. 106.
[7] W.P. No. 110.
[8] Scot. Law Com. No. 106, at para. 3.4.

assessment, which we set out in this report, of whether any further legislation is justified and, if so, of what form that legislation should take.

1.12 During the currency of this part of our work there has been a noticeable increase in the extent of public debate about the implications and dangers of, in particular, hacking. In large part that has been due to the energy of Miss Emma Nicholson MP, who has vigorously pursued these issues both inside and outside Parliament, and who in April 1989 presented a Private Member's Bill to legislate against hacking. We have not found ourselves able in this report to recommend legislation in the same terms as those proposed by Miss Nicholson, but we are glad to put on record the impetus that she has given to public concern about computer issues.

1.13 One prominent aspect of this concern has been a widespread view that the problems associated with computer misuse are sufficiently serious to justify the accelerated consideration of any possible legislation. In deference to that view the Commission has diverted additional resources to this project, to enable this report to be completed before the end of September 1989. Because of that accelerated timetable it has not been possible for the Commission in this case to follow its normal practice of accompanying its report with a draft Bill. We have, however, sought to set out our recommendations in sufficient detail to ease the drafting of legislation in the event of those recommendations being accepted.

C. THE FACTUAL BACKGROUND

1.14 W.P. No. 110 referred to the various ways in which computers are used in modern life and commerce. Here we summarise and expand on that account, in the light of the further evidence now made available to us. This account is relevant to all the policy issues discussed and recommendations made later in this report, but because of the importance of hacking in this study the factual account pays particular attention to features of computers that are relevant to that activity.

1.15 Although computers are sometimes thought of principally as a sophisticated means of collating and holding information, many computers are now used in 'operational' as opposed to purely information-storing roles. Such systems administer not only financial transactions (for instance, world-wide inter-bank fund transfer systems) but also a wide variety of complex operations. Many are in the public or semi-public sector: examples are air traffic control systems, and hospital systems for calculating drug dosages. Others are used in commerce and industry: for instance stock control and automatic reordering; reservation and automatic state of availability of hotel bedrooms, airline tickets, package holidays and so on; robotic control of machines and manufacturing processes; payrolls and the automatic issuing of pay cheques; and the programming of computers to trade on Stock Exchanges in response to economic data and price movements inputted by other systems. The extent to which and the complexity with which such operations are computerised appears to be increasing day-by-day.

1.16 The potential for mischief if such systems are illicitly altered or reprogrammed is thus very large. Cases of actual interference reported to us include the reprogramming by a disaffected employee of a computer-controlled robotic manufacturing process, with the result that machines reacted unpredictably to commands and a shop-floor operative was nearly killed; a hacker obtaining access to a travel agency/tour company network and then swamping a tour operator's reservation system with false orders; and a hacker causing mail-shots to be sent out automatically to thousands of non-customers.

1.17 The above are examples of misuse of a system by the alteration or reprogramming of its commands, or by the unauthorised addition of false data. Operational (or indeed information) systems are also vulnerable to attack by the introduction of 'viruses' or 'worms '. We do not use these as technical expressions, but simply as common and convenient labels to describe unauthorised programs which replicate themselves. Such programs use up the capacity of the computer system, or operate to change or delete existing legitimate programs or files, or both. We are satisfied that such incidents have in fact occurred in major commercial systems, causing the system in question to be shut down until the cause was identified and rectified.

1.18 Serious consequences can also attend the destruction of computer-held information, whether by straightforward deletion or by the planting of viruses. Examples reported to us include the programming by an employee of a firm of architects' computer-based design system, so that design files were deleted (and thus lost) when attempts were made to use them (this being a form of virus); and the entry by an outside hacker into a university computer system, where he deleted the results of two years' scientific research.

1.19 It may surprise laymen, as initially it surprised us, that such incidents are possible or, at least, that they are not preventable by security precautions. We have therefore been particularly acute to question our informants on this point. We would not regard it as a complete answer to demands for legislation that users can or must protect themselves, any more than the justification for a law of burglary is removed by the availability of burglar alarms. However, the justification for new and to some extent unusual legislation, and in particular for the basic hacking offence favoured by most of those commenting on W.P. No. 110,[9] must be affected by the nature of the threat that it is intended to prevent and the ease with which that threat can be avoided without criminalisation.

1.20 We therefore set out in paragraphs 1.21-1.36 below some of the broad characteristics of computer systems and their operation that appear relevant to this issue, having during our enquiries satisfied ourselves as to the substantial accuracy of this information. It is convenient for purposes of exposition to draw a distinction between 'outsiders' and 'insiders'. Insiders are people with legitimate access to the system who however use that system for a wrongful purpose, or exceed their legitimate level or degree of authority within the system. Outsiders are what is typically thought of when talking of 'hackers'. They obtain access to computers with which they have no legitimate connection, usually by approaching the system through a public telephone system by use of a modem.

1.21 A feature of many computer systems is that they are 'on line': that is, connected to other systems, or available to authorised users, through telephone connections that use either 'dedicated' lines or the general public telephone system. Many examples can be given. Inter-bank clearing systems are connected to the internal computer systems of each participating bank. The stocking and ordering systems of supermarkets are connected to suppliers' warehousing computers. The computers of travel agents are necessarily linked to those of hotels, airlines and tour operators. Pharmaceutical companies give access to their computerised database to customers wishing to have immediate information on dosages, safety levels and other precautions. We understand that a programme of computerising GPs' records and linking them on line with hospitals is or will shortly be underway. Within companies or organisations, many people will be given legitimate access to the system: for instance, managers may have a need for instant access to personnel information, and salesmen to stocking records and product data. Much of this latter access has to be on-line, either between remote locations or in some cases from public or domestic telephones used by employees in the field.

1.22 The usefulness of such systems depends in large part on the ease and extent of access that they give to authorised users. Such users can be controlled by the use of passwords and other devices. Passwords however can be lost or compromised, with substantial inconvenience in changing them for all of the users involved; and other more technical controls or limitations undermine the usefulness of the system. In addition, all systems are potentially vulnerable to insiders. Misuse by such persons may take the form of reprogramming, corruption or deletion of data by an authorised user; or access by an authorised user to a level beyond his authority; or a combination of those acts. Insiders in this context include not only employees of the owner or operator of the computer but also persons with authorised access to another system to which that computer is connected, and persons providing software or maintenance services to the system.

1.23 Outsiders, the typical hackers, have a more difficult task. Using a telephone

[9] This was "option D", discussed at paras. 6.35–6.37 of W.P. No. 110, and considered further below.

system (to which he may well have obtained access by methods that by-pass the charging mechanisms) the outside hacker must first identify a 'data line' (i.e. a line connected to a computer); then the hacker must use a modem that is compatible with the target modem; then his software communications system must match that of the target computer; then the hacker has to present the appropriate password to gain access to that system; then, if he is to exercise any kind of control over the system, the hacker must find out how to obtain 'system privileges', which is the convenient common expression for the level of authority that enables the holder to alter or manipulate, as opposed merely to read, the data held on the system. The hacker may conduct some of these operations on a random basis, by means of programs that dial or present many thousands of numbers until a positive result is obtained. A more promising avenue for the hacker however is the use of known passwords, or of knowledge of the general configuration of particular systems. We have already pointed out the difficulty of administering passwords in 'open' systems. Existing passwords, or information about the methods whereby they are changed or rotated, are regularly publicised and exchanged between hackers by means of (on-line) 'bulletin boards' that pool detailed information between hackers in all countries of Western Europe and North America about means of accessing particular systems. We have been shown a number of print-outs from such boards, and are in no doubt that they are a prominent feature of the hacking scene.

1.24 Hackers are also assisted by more general inside information about systems and about the nature and configuration of software. A development in recent years has been the interchangeability of software, so that the majority of types run on any hardware. Many hackers, we are informed, have a background in software development or systems engineering, and thus have inside knowledge of the types and kinds of access level, and security arrangements, that are in common use; or they may have acquired that knowledge through bulletin boards. While such knowledge is unlikely to give a hacker direct access to a particular system, it can substantially assist him in reading the 'thinking' of the system that he is trying to enter. This development was noted by the Audit Commission which, in a passage quoted in paragraph 6.17 of W.P. No. 110, referred to the implications for a future increase in hacking of the growth in numbers of 'computer literate' employees.

1.25 There exist a number of security devices, some of them of a comparatively simple nature, that can be used to counter such attacks. A good deal of the evidence put before us suggested that the need for attention to computer security has in some cases only been appreciated comparatively recently. It is important to stress, as is already well understood by the main users of computer systems, that no legislation can take the place, in protecting the legitimate interests of computer users, of proper investment in security systems, and the stringent administration of such systems once they are installed. However, the effectiveness and practicability of such steps varies according to the nature of the system under consideration.

1.26 In our view it would be very unusual for unauthorised outside access to be obtained to, or at least to any significant level of, a closed system that because of its nature emphasises security, such as an air traffic control or defence weapons system. However, we have had reports of such access being obtained to systems outside the United Kingdom; and we have well in mind the observation that if such incidents are possible, and the law is deficient in dealing with them, it would not be wise to wait for confirmation that serious consequences could follow before taking action.[10]

1.27 There is more positive evidence in the case of the more open on-line systems of the type referred to above. Internal discipline in the use and availability of passwords is one obvious measure of security, but we have already pointed out its practical limitations. Employees or outside users write passwords down and then lose them, or foolishly or dishonestly give them to other people; and the passwords or the password procedures will often be known to the engineers who installed or who service the system. Encryption (coding) of data is commonly used (in spite of the expense and inconvenience) on systems where security is important, but even that is vulnerable to leaking of the encryption codes. Other common means of discouraging hackers are the system's refusing entry after, say, three abortive attempts; or an 'answer-back' system,

[10] See Scot. Law Com. No. 106 at paras. 3.3–3.5, quoted in para. 6.18 of W.P. No. 110.

whereby the system, on initial contact, requires the caller to give his number and rings him there, provided the number is one that the system recognises. The first of these is, however, useless if the caller is not operating at random, but illegitimately has the right password. The answer-back system catches the use of an authorised password from an unauthorised telephone number; but it introduces what may be an unacceptable level of delay, and expense, into systems whose whole purpose is to give instant access to authorised users.

1.28 The problems of security are accentuated where users of one system, either authorised or unauthorised, enter another system, using connections of the kind that were described above. Some extreme examples have been quoted to us. For instance, a hacker entered a United Kingdom system, and then used it to enter the United States National Telephone Network; from there he contrived to obtain access to the computerised ordering system of a USA mail order company, and added large numbers of UK individuals to the company's mailing lists. Such acts are of course to some extent controllable by internal limitations on ease of access, but too severe such limitations may, again, reduce the effectiveness of the system's legitimate operations; and, of course, a chain of interconnected systems is only as strong as its weakest link.

1.29 Our conclusion on the evidence that we have received is that hacking by unauthorised entry or attempted entry is sufficiently widespread to be a matter of major and legitimate concern to system users. In this respect, the information that we now have differs from the result of the Audit Commission survey reported at paragraph 6.17 of W.P. No. 110, which was the main evidence available to us when W.P. No. 110 was published. The concern about this form of hacking is not so much the possibility of inadvertent damage to the system, that was referred to in paragraph 6.17 of W.P. No. 110, but the uncertainty and cost caused by repeated hacking attempts. This concern has frequently been described to us as concern about the 'integrity' of the system attacked. Put briefly, because of the possibility that any attempted entrant may have had password access to important levels of authority, sometimes to a level which has enabled him to delete records of his activities from the system, any successful unauthorised access must be taken very seriously. Substantial costs are therefore incurred in (i) taking security steps against unauthorised entry and in the equally important precaution of monitoring attempts to enter; and (ii) investigating any case, however trivial, where unauthorised entry does in fact occur. We have seen some estimates in figures of the amounts involved, which we have not been able to verify. However, we are satisfied, as we have said, that the costs are substantial.

1.30 Something like the current level of costs in relation to security measures is likely to be incurred whether or not the law on hacking is changed, since no-one can be confident that such a law will be totally effective. However, a law that deterred hacking should reduce the costs of monitoring attempts, and also costs falling into category (ii) above. In the following paragraphs we give examples of such costs; we should emphasise that none of the incidents referred to involved any proven misuse of the system beyond unauthorised access. The degree of detail that we have used in quoting these cases seeks to respect the confidentiality of our informants; and we should add that not all of those informants replied to the formal consultation, and therefore not all of them are listed in Appendix A hereto.

1.31 What we believe to be a reliable estimate has been given to us that the cost of restoring a commercial computer system that has been illegitimately entered can amount to hundreds of thousands of pounds for investigating and rebuilding the system, and for the loss of the system while those operations take place. Users who have identified an intrusion may be advised that the software used on the system should be rewritten, since only then can damage be identified or lack of damage be authoritatively confirmed.

1.32 Many computer manufacturers employ highly skilled (and thus very expensive) teams of staff whose only function is to assist customers in identifying possible entries by hackers and advising on remedial measures.

1.33 A case has recently occurred of a computerised customer information network being entered from a customer's premises by an unauthorised user, who managed to penetrate to a high level of authorisation. Although so far as can now be known the hacker caused no actual damage, the computer owner closed and completely

regenerated the system as a precaution. That occupied over 70 man-hours of highly skilled time, as well as the costs of non-availability of the system, and of informing all customers of its closure.

1.34 We have been told that a computer operator with knowledge of university computer systems used that knowledge to enter the internal systems of eight universities, thus requiring lengthy investigation at all locations. Computer authorities now spend substantial periods of time on a daily basis reviewing the records of traffic on their systems in an attempt to identify cases of unauthorised access.

1.35 A large international system was entered by a hacker who appeared to have acquired a sufficiently high level of privilege to be able to read and collect passwords. The entire system was closed down, and the software rebuilt to exclude any possibility of the hacker's having rendered it insecure. The work had to be completed within 72 hours if the system were to remain functional, and occupied upwards of 10,000 man-hours of highly skilled staff.

1.36 A further, and necessarily less specific, concern has been expressed about the current high level of interest in and practice of hacking, and the comparative impunity with which it takes place. It is entirely possible that the 'amateur' hackers act as a smokescreen for, or collaborate with, persons with more dishonest or sinister motives. That can occur either because entry by the latter is masked by or mistaken for entry by amateurs; or because the culture and information services of the bulletin boards provide dishonest people with means of access to systems that they could not otherwise obtain. We have not been able to reach a firm view as to how substantial this problem may be. However, there is no doubt that the acts engaged in by the simple or amateur hacker are exactly the same as the necessary preliminaries to the unauthorised removal or alteration of computer-held data.

D. THE PROPOSALS OF THE SCOTTISH LAW COMMISSION

1.37 We referred in paragraph 1.6 above to the proposals of the Scottish Law Commission, published in July 1987,[11] to which we have given very detailed consideration in the course of our work. In its report the Scottish Law Commission appear to have considered,[12] as we did ourselves in W.P. No. 110,[13] that the main issue affecting a decision whether or not to introduce an offence prohibiting unauthorised access or hacking was whether such an offence was necessary or justified for the protection of information. However, as we indicate in more detail in Part II of this report, the further evidence that we have received since the publication of W.P. No. 110, which we set out above, has convinced us that the main argument in favour of a hacking offence does not turn on the protection of information, but rather springs from the need to protect the integrity and security of computer systems from attacks from unauthorised persons seeking to enter those systems, whatever may be their intention or motive.[14] It is for that reason that we propose, as a deterrent counter to hacking, two offences: the first, a broad offence that seeks to deter the general practice of hacking by imposing penalties of a moderate nature on all types of unauthorised access; and the second a narrower but more serious offence, that imposes much heavier penalties on those persons who hack with intent to commit, or to facilitate the commission of, serious crime.

1.38 Our proposed offences differ from the unauthorised access offence proposed in clause 1 of the draft Bill annexed to the Scottish Law Commission's report.[15] For the reasons that we set out in more detail in paragraphs 3.8-3.9 below, we do not think that that offence would adequately address the particular problem that our research has shown hacking to present. Both Commissions are of course agreed that some legislation is required against unauthorised access to computers. However, in the two years since the Scottish Law Commission reported, perception of the problem posed by computer misuse and evidence of its nature has been increasing very rapidly. The further

---

[11] Scot. Law Com. No. 106.
[12] See *ibid.*, at paras. 3.6, 3.13(2) and 3.14(2)–(3).
[13] At paras. 6–8–6.15
[14] See in particular paras. 2.11–2.15 below.
[15] Scot. Law Com. No. 106, p. 130.

evidence that we have received has led us to differ from our Scottish colleagues on the precise form such legislation should take.

1.39 The evidence that we have received has also strongly reinforced the view taken by the Scottish Law Commission[16] that computer misuse is a problem of international dimensions, which may often involve the unauthorised accessing of computers across national boundaries. That is obviously very likely to be the case between England and Wales, and Scotland, particularly because of the frequent incidence of Great Britain-wide computer networks. It would therefore in our view be obviously desirable that the rules of the criminal law in relation to unauthorised access to computers should be uniform throughout the United Kingdom, and we hope that that end will be achieved in any legislation.

E. THE STRUCTURE OF OUR RECOMMENDATIONS

1.40 Against the background set out above and in W.P. No. 110 we now review and make recommendations as to the law reform issues raised by computer misuse. The response to consultation indicated that we had been correct in W.P. No. 110 in identifying the three types of computer misuse with which we should be concerned in this study as: (i) computer fraud; (ii) obtaining unauthorised access to a computer ('hacking'); and (iii) unauthorised alteration or erasure of data or computer programs. We deal separately with each of those problems.

1.41 In Part II of this report we discuss the need for new criminal offences in respect of each of the above-mentioned forms of misuse, and recommend the creation of three criminal offences. In Part III we set out our recommendations in more detail, and discuss issues of procedure and sentencing relevant to our proposed offences. Part IV deals with several further matters that have arisen in the course of our deliberations: the jurisdictional rules that should apply to our proposed offences; evidence produced by a computer; powers of arrest, search and seizure; telephone-tapping in order to obtain evidence of computer crime; and whether there should be a duty to report computer-related offences.

[16] *Ibid.*, para. 5.13.

PART II

THE NEED FOR NEW OFFENCES

2.1 Our conclusion from our further review of the issues identified in Part III of W.P. No.110 is that the most appropriate approach to the reform of the criminal law pertaining to computer misuse is to create a number of new criminal offences, which however will differ considerably in their gravity and, thus, in the penalty appropriate for their commission. First, and most simply, an offence of basic hacking triable only in the magistrates' court and punishable with imprisonment for a maximum of three months. Secondly, an offence of hacking with intent to commit or further a serious crime, triable either way and punishable on conviction on indictment with a maximum of five years' imprisonment. Thirdly, an offence to punish the unauthorised alteration or destruction of programs or data held in a computer, triable either way and punishable on conviction on indictment with a maximum of five years' imprisonment. First however, we look at the area of computer-related fraud and indicate the reasons why we do not in this report propose any alteration of the relevant law.

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.[17] While many of the cases of computer misuse reported generally and to us have been cases of fraud, we have not received evidence to cast substantial doubt on the conclusion that we expressed in W.P. No. 110[18] that, with one minor exception, the general criminal law is adequate to meet this form of misconduct.

2.3 The experience of our commentators seems to be that most computer frauds are perpetrated by 'authorised' (inside) users. Our findings also provide further support for the results of the Audit Commission's survey, to which we referred in W.P. No. 110,[19] which concluded that by far the most common way of committing a computer fraud was in some way dishonestly to enter false data into a computer ('input fraud'). More complex frauds have been attempted on financial systems, but such attempts are covered by the general criminal law. It may perhaps be pointed out in passing that if computer records are altered by an *authorised* user in order to create a false impression (as we are reliably informed has occurred in recent cases) that is plainly forgery;[20] a conviction for forgery was not obtained in *Gold and Schifreen*[21] only because the elements of the system which the hackers attacked during the accessing of the computer did not, unlike commercial records held within a computer, involve the recording or storing of information.

2.4 Our only reservation on the applicability of the general offences of dishonesty to computer fraud in W.P. No. 110 was that at present it is not possible in law to deceive a machine within the meaning of deception under the Theft Acts.[22] This is not a problem unique to computers, and was therefore raised also in our Working Paper on Conspiracy to Defraud.[23] In the course of the present exercise we received little evidence of cases where a conviction for a fraud offence was lost because of that problem. On the contrary, our consultation appeared to confirm the view that we expressed in W.P. No. 110 (at paragraph 6.4):

> "When a computer is manipulated in order dishonestly to obtain money or other property, a charge of theft or attempted theft will generally lie."

Convictions for theft have been obtained, for example, in cases where false data is entered by someone into a computer in order to obtain payments to which that person (or another) is not entitled, often by transfer to a false or specially created bank account; and where forged cash-point cards (or cards stolen from someone else) have been used

---

[17] W.P. No. 110, para. 2.2.
[18] *Ibid.*, para. 3.64.
[19] *Ibid.*, para. 2.4.
[20] Contrary to section 8(1)(d) of the Forgery and Counterfeiting Act 1981.
[21] [1988] A.C. 1063; the case is discussed at length in paras. 3.14–3.22 of W.P. No. 110.
[22] See W.P. No. 110, paras. 5.5–5.6.
[23] (1987) Working Paper No. 104.

to obtain money from a cash dispensing machine. In both of these types of cases, and in most, possibly in all,[24] others which initially appear to involve some kind of 'deception' of a machine, the manipulation involves an *appropriation* of money or other property, sufficient to constitute theft. Other cases where convictions have been obtained have involved the reprogramming of computers to produce bogus cheques, or false entries in banking records. Further, even in cases where there is no appropriation, and a machine has been 'deceived', if two or more people are involved a charge of conspiracy to defraud will lie.[25]

2.5 Our conclusion is, therefore, that while steps need to be taken to deal with the problem of 'deceiving a machine', the gap in the law that is involved would seem to be comparatively modest. That is particularly because it appears that, *at present*, machines comparatively seldom make decisions about the provision of services or the release of liabilities, so as to raise questions under sections 1 and 2 of the Theft Act 1978, as opposed to furnishing money or the opportunity to obtain money, which latter cases fall under the present law as discussed in paragraph 2.4 above. Nonetheless, it was clear from the response from consultees in connexion not only with W.P. No. 110, but also in respect of the discussion of the topic in our Working Paper on Conspiracy to Defraud, that there is widespread support for the Commission's provisional proposal in the latter Working Paper to make it an offence to deceive a machine.

2.6 For that very broadly-stated objective to be achieved it would be necessary, as we pointed out in paragraph 5.4 of W.P. No. 110, for there to be fairly extensive amendment of a number of sections of the Theft Acts 1968 and 1978, and in particular the adaptation to cases involving machines of provisions, such as those in sections 1 and 2 of the Theft Act 1978, that presuppose the existence of a person upon whom the deception operates. As our work progressed, it became clear that we had been over-optimistic in assuming, as we stated in paragraph 5.5 of W.P. No. 110, that such amendments would be largely technical and uncontroversial. Further consideration has convinced us that the process of legislative reform will in fact be complex, and the basis on which it should proceed needs review of a width that cannot easily be undertaken in the present study.

2.7 We have therefore concluded that the proper course is not to make proposals on this topic in this report, but to deal with it, as was originally envisaged would be the case, in the context of our study of conspiracy to defraud. We have not so far concluded whether, in that context, 'deceiving a machine' requires treatment as a separate topic, or whether it can be accommodated within any more general reform of the law. We should emphasise that we are far from having lost sight of this issue; but we have not received evidence to suggest that this reform is of the immediate urgency that has been represented to us to attach to the other matters dealt with in this report.

2.8 There is, however, one area very relevant to computer fraud in which we regard early action as of the utmost importance. On 11 April 1989 we submitted to you our Report on Jurisdiction over Offences of Fraud and Dishonesty with a Foreign Element,[26] in which we made detailed recommendations for the reform of the present antiquated and insular rules governing the jurisdiction of the English courts over international fraud. We pointed out in that report that modern technology, including in particular the use of computers, had greatly facilitated the international transfer of money and obligations, and thus the ability to plan and implement in one country a fraud that has its deleterious effect in another country.

2.9 We have during our present work, and since the publication of that report, had a number of discussions with persons concerned with computer fraud, including commercial operators and public enforcement agencies. We have been told that the enactment of the Bill attached to our report would be an important weapon in the fight against computer-related fraud which, because of the nature of computer systems, often

---

[24] See the view of the Court of Appeal in *Lawrence* [1971] 1 Q.B. 373 at p. 378E that it may be that any case of obtaining property by deception contrary to section 15 of the Theft Act 1968 also amounts to theft. This issue was not resolved when the case went to the House of Lords: [1972] A.C. 626. See also Smith & Hogan, *Criminal Law*, 6th ed. (1989) pp. 521–522, and *Dobson* v *General Accident Fire and Life Assurance Corporation plc* (1989), *The Independent*, 22 August 1989.

[25] See W.P. No. 110, paras. 3.10–3.11.

[26] (1989) Law Com. No. 180.

has an international element. We regard the proposals incorporated in that Bill as an integral part of our recommendations on computer-related crime, and hope that they will be so treated in any legislation.

B. THE THREAT PRESENTED BY HACKING

2.10 In W.P. No. 110 we perceived hacking to be the major concern in the area that we identified as constituting 'computer misuse', and our consultation has confirmed that view. We asked the question, 'Should the obtaining of unauthorised access to a computer be a criminal offence?' and set out considerations relevant to that question in Part VI of that Working Paper. In the light of the responses to that question we have concluded that hacking by unauthorised entry (or attempted entry) is sufficiently widespread to be of major concern to computer system users: we set out the evidence in support of this view in section C of Part I of this report. In this section we explain why that evidence has led us to recommend the creation of two new criminal offences to deal with hacking.

2.11 Some special features of computers and computer systems were set out in paragraph 6.7 of W.P. No. 110. Those features largely reflected the information storage capacity of the computer, but it is also important to note the operational role played by many computer systems, to which we referred in paragraph 1.15 above. The arguments put forward in paragraphs 6.8-6.10 of the Working Paper concentrated on the threat that hacking posed to the confidentiality or value of information stored on a computer. The main argument that was put forward in the Working Paper against the offence, in paragraph 6.15 of W.P. No. 110, was that the criminal law does not generally protect confidentiality or privacy, or provide sanctions against the removal of information. However, the further information that we have received on consultation has enabled us to look at the matter in a somewhat different light.

2.12 We accept that the introduction of computers has created radical alterations in the methods and conditions of information storage. Computers enable information to be held and handled in an amount, in a way and at a speed that is quite novel. The availability of such facilities and the use that is made of them are generally accepted to be strongly in the public interest. However, a computer system accessible from remote sites presents problems of security that are not suffered by a user who keeps his information on paper and is protected by physical barriers to access, and in addition by the laws of burglary or, at least, criminal damage. That difference does not betoken any choice on the part of the computer user to be less secure, but rather is inherent in the nature of the operation that he is running.

2.13 Computerised information storage presents the user and the criminal law with a set of problems that are qualitatively different from manual methods of storage. Nevertheless, we would have difficulty in accepting that those developments alone would justify the introduction of a hacking offence. That, however, is not the end of the matter, since in our view the case for a criminal offence of basic hacking does not turn on the need to protect information, and for that reason we reject, as did the great majority of our consultees, Options A and B that were put forward in W.P. No. 110 and which were based on that assumption.[27] Rather, we are persuaded that hacking should be criminalised because of the general importance of computer systems, in accordance with the analysis that we set out in paragraph 1.29 above. We of course accept that the *effect* of introducing an offence of unauthorised access will be to criminalise some people who look at other people's information and, by the same token, to give some protection of the criminal law for that information. We do not, however, regard those contingent effects of an unauthorised access offence as militating against the creation of such an offence if, as we are persuaded, there are other and strong grounds for taking that step.

2.14 In our view therefore the most compelling arguments for the criminalisation of

[27] Option A was to 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. It was considered at paras. 6.25–6.26 of W.P. No. 110. Option B was to create an offence of unauthorised access to a computer in order to inspect information of any kind. It was discussed at paras. 6.29–6.31 of W.P. No. 110.

hacking are those stemming from, first, the actual losses and costs incurred by computer system owners whose security systems are (or might have been) breached; secondly, that unauthorised entry may be the preliminary to general criminal offences; and thirdly, that general willingness to invest in computer systems may be reduced, and effective use of such systems substantially impeded, by repeated attacks and the resulting feeling of insecurity on the part of computer operators.

2.15 The deterrence of such invasions of computer systems is a proper public goal. Directly or indirectly they cause substantial expense and interfere with valuable operations, both public and private. The importance of the integrity and proper functioning of operational computer systems is, we think, obvious, and the need for total confidence in that integrity leads to great expense and inconvenience if such systems are penetrated, even if later investigations show that no actual impairment of the system had been achieved. Because even attempts to gain unauthorised access to such systems have those possible consequences, there seem to us to be the strongest reasons for using the criminal law to express disapproval of such conduct.

2.16 We also see merit in the further argument in favour of such an offence that was raised in paragraph 6.13 of W.P. No. 110, that it might serve to deter conduct such as fraud or criminal damage[28] the opportunity for which arises consequent to the unauthorised access. There are three aspects to this case. First, a person who is contemplating fraud may be deterred if even the necessary preliminary conduct exposes him to the attention of the enforcement authorities, and possible conviction.[29] Secondly, some of the present numbers of 'innocent' hackers, which numbers the proposed offence seeks to reduce, may, once they have gained entry to a system, go on either by accident or design to commit fraud or cause damage. While we do not, in contrast to the position represented by Option C in W.P. No. 110,[30] think that the prevention of accidental damage is the central reason for having an offence of unauthorised access, the undoubted possibility of such damage would be reduced if the incidence of hacking were reduced. Thirdly, we see some force (although we would not wish to exaggerate this point) in the concern[31] that the activities of people who hack for idle pleasure may serve as a smokescreen concealing, or a recruiting ground for, persons with more sinister motives. We would have difficulty in regarding that, standing on its own, as a sufficient justification for the criminalisation of mere unauthorised access, but it is a consideration that certainly does not detract from the other arguments in favour of that offence.

2.17 The view is sometimes expressed (though it was not prominently represented in our consultations) that hacking should not be criminalised because hackers are not interested in using the information that they find, but act purely for the challenge and excitement of breaking down security barriers designed solely to keep them out.[32] We reject this argument because the insecurity that hacking causes to computer-owners is the same whether or not the hacker intends to make use of any particular information that he may find. We also see no merit in the suggestion that hackers are doing computer operators a favour by testing out their defences. It is for those operators to decide how their systems shall be tested. If they *invite* outside attack they cannot complain if such attacks are made and succeed: but that is irrelevant to the uninvited and unauthorised intrusions with which most system owners are concerned.

2.18 We have also further considered the argument, discussed in paragraph 6.16 of W.P. No. 110, that the introduction of unauthorised access offences may prove nugatory, because the conduct that they seek to prevent is difficult to detect or, at least, difficult to trace to its source with the specificity required for criminal prosecution. We have discussed these suggestions with law enforcement agencies, computer operators and those responsible for public telephone services, and are satisfied that the suggestions are unduly pessimistic. We consider that the means already exist adequately to enforce the offences that we recommend in this report.

---

[28] Or conduct amounting to "unauthorised modification" of a computer program or data. See further paras. 2.26–2.33 below.

[29] For our proposals in respect of hacking with intent to commit a serious offence, see paras. 3.49–3.60 below.

[30] W.P. No. 110, paras. 6.32–6.34.

[31] Referred to in para. 1.36 above.

[32] See, for example, *The Times*, 10 August 1989, p. 28: "Inside the top hackers' party"—a report on a conference for hackers which had been held in Amsterdam the previous week.

2.19 We do not think it necessary to pursue these issues in great detail, but there is one particular facet of the means of detecting of hacking to which we should draw attention. We refer in this context to hacking as outside access, almost certainly by means of a public telecommunications system. The detection of 'inside' unauthorised access is merely a matter of the computer-owner investing in sufficient safety-devices and a sufficient control system to be able to detect what use is being made of the computer and which insider is doing it.

2.20 In the case of outside hacking, provided that the owner of the computer under attack gives the full co-operation to the authorities that they are entitled to expect, it is possible first to identify the line down which the unauthorised signals are being passed to the computer, and then for the authority running the public telephone system to monitor the time, duration and destination of calls on that line, with a view to comparing the pattern with the traffic arriving at the attacked computer. Such monitoring is not 'telephone tapping' because no attempt is made to intercept the calls themselves, or to scrutinise their content. Moreover, section 45(1)(b) and section 45(2)(a) of the Telecommunications Act 1984[33] provide that the authorities running a public telecommunications system do not commit an offence if they disclose such information for the prevention or detection of crime or for the purpose of any criminal proceedings, provisions that would clearly extend to the investigation of an unauthorised access offence.

2.21 The legitimate powers of the authorities however go further than that. As one would expect, the provisions against telephone tapping do not extend to the interception of a communication with the consent either of the sender or of the receiver of that communication.[34] Communication between a remote station and a personal computer is typically by means of a modem attached to a telephone line. When the operator types an instruction or message on to his own keyboard, that instruction is sent through the telecommunications system to the target computer, which sends or 'echoes' the instruction back to appear on the operator's screen display. The operator then knows that the target computer has received the message. The implications of this procedure in the present context is that the 'echo' transmitted over the public system *by the targetted computer* is a record of the traffic initiated by the hacker. We share the view of our informants that the interception of that 'echo', with the consent of the owner of that computer, is a perfectly legitimate procedure.

2.22 Such methods will identify the *number* from which the traffic is coming. They do not necessarily identify the individual who is using that number, but we doubt whether that will pose practical problems in many cases. We have also been reassured to learn that the policy of the operators of public telecommunications systems is to identify and take such steps as the law allows against unlawful uses of their systems.

2.23 Our researches do not therefore allow us to accept the suggestion that hacking is so difficult to identify or detect that it would be fruitless to make it a crime at all. We do not shrink from the fact that hacking, of its very nature, will often go undetected or, at least, unpunished. The same can unfortunately be said of many other crimes. However, we do not see the main justification of the offence as being that it will necessarily secure the conviction of a large number of individuals. Rather, the criminalisation of hacking will, in the words of one of our best informed respondents, change the climate of opinion, by removing the present aura, if not of acceptability then at least of fun, that surrounds hacking. We set out the desirable changes in attitude in paragraph 6.12 of W.P. No. 110: they include persuading young people not to enter into, or to be instructed in, hacking, and the deterrence of 'bulletin board' practices. Our informants, particularly from the police forces and from industry, strongly supported the efficacy and justifiability of legislation against hacking in achieving those ends, and we are persuaded that their view is correct.

2.24 Our conclusion is, therefore, that an offence of unauthorised access is justified and indeed necessary in order to change attitudes and reduce the present widespread incidence of hacking. As we have said, the introduction of such an offence will have little effect on the amount that any responsible operator spends on security, since it will

[33] As substituted by section 11(1) of, and Schedule 2 to, the Interception of Communications Act 1985.
[34] Interception of Communications Act 1985, s.1(2)(b).

be recognised that total deterrence is impossible. It should, however, at least in the longer term, reduce the overall incidence of hacking, and thus increase confidence in computer systems and reduce the incidence of costs of the type referred to in paragraphs 1.29-1.35 above.

2.25 Opinion on consultation was strongly in favour of an offence of unauthorised access, the preference being for a basic offence along the lines of Option D in W.P. No. 110.[35] Our further inquiries since consultation closed have reinforced that view and we *recommend* that an offence along those lines should be created. Our detailed recommendations as to the form such an offence might take are contained in Part III of this report. For the reasons there stated, in addition to a basic offence of obtaining unauthorised access to a computer, we *recommend* an offence of obtaining unauthorised access to a computer with intent to commit a serious crime.

C. UNAUTHORISED DESTRUCTION OR ALTERATION OF INFORMATION HELD IN A COMPUTER

2.26 In W.P. No. 110 we identified several ways in which this kind of conduct might be carried out.[36] These include physical destruction, electronic erasure (as occurred in the leading case in this area, *Cox* v *Riley*[37]), viruses and worms.[38] Our review of existing criminal offences relevant to such conduct[39] focussed on the Criminal Damage Act 1971, section 1 of which provides that-

> "(1) 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 commits an offence. "

2.27 Our provisional view was that the wide meaning attributed by the courts to the word 'damage', including as it did any injury impairing the value or usefulness of property, had had the effect of extending the law of criminal damage to cover the tangible property (i.e. the floppy or hard disk, or streamer tape) on which programs or data were stored. On this reasoning any unlawful interference with the data or program would amount to damage to the tangible storage medium, providing that its value was thereby diminished.

2.28 It does not seem to have been seriously questioned that the unauthorised destruction of data and the reprogramming of operational computers ought to be criminal. That was the view taken by our consultees and we consider it to be correct. Alteration or erasure of data without authority has, in the absence of specific justifications provided by law, no social value; it involves deliberate interference with the property of others, and not merely trespassing on their premises or looking at their information; and, as the examples given in paragraphs 1.16-1.18 above indicate, it can cause substantial loss and, in the case of operational systems, physical danger. While it is clear therefore that these activities ought to be outlawed, it is more controversial whether the present law of criminal damage is an adequate response in the way that we provisionally suggested. Our conclusion on further consideration, which was supported by the weight of opinion on consultation, is that clarification of the law is required. The main reasons for that conclusion are as follows.

2.29 'Property' means, for the purposes of the Criminal Damage Act 1971, property of a tangible nature.[40] In *Cox* v *Riley*,[41] the deleted computer program had been stored on a plastic circuit card, which latter could be and was identified as the tangible property which had been damaged. Several consultees have made the point that there may be more difficulty in other cases in pointing to a physical medium on which the altered or erased data has been held; indeed it has been suggested to us that in some cases data is stored by means of electrical impulses that are only very notionally

---

[35] Option D proposed to make it an offence intentionally to obtain unauthorised access to a computer. It is discussed in paras. 6.35–6.37 of W.P. No. 110.
[36] W.P. No. 110 at paras 2.16–2.17.
[37] (1986) 83 Cr. App. R. 54.
[38] See para. 1.17 above.
[39] W.P. No. 110, at paras. 3.35–3.40.
[40] Criminal Damage Act 1971, s.10.
[41] (1986) 83 Cr. App. R. 54.

attached to any tangible property. For the commission of a criminal offence to depend on whether it can be proved that data was damaged or destroyed while it was held on identifiable tangible property not only is unduly technical, but also creates an undesirable degree of uncertainty in the operation of the law.

2.30 The Divisional Court in *Cox* v *Riley*[42] in effect held, following the unreported case in the Court of Appeal (Criminal Division) of *Henderson and Battley*,[43] that the circuit card had been damaged because to reprogram it would require more than a minimal amount of time and effort.[44] That analysis looked back to *Fisher*,[45] a case decided on section 15 of the Malicious Damage Act 1861 which, unlike the 1971 Act, referred to 'damage with intent to destroy *or to render useless*' (emphasis added). While the reasoning in *Fisher* is somewhat ambiguous, it is possible that the court regarded 'rendering useless' as forming a separate head of 'damage'. It is therefore not entirely clear that the view that damage can occur where there has been *no* physical impairment of the tangible object has survived the repeal by the 1971 Act of the specific offence discussed in *Fisher*. The problem is that neither *Cox* v *Riley* nor *Henderson and Battley* squarely address the point that the dictionary definition of 'to damage' requires some injury to a thing;[46] the decisions concentrate on the second limb of that definition, that the injury must lessen or destroy its value. In our view, therefore, those authorities cannot be relied on with sufficient confidence as stating the present law on the meaning of damage.

2.31 That the meaning of 'damage' has caused practical as well as theoretical problems following the decision in *Cox* v *Riley* is evidenced by the experience of the police and prosecuting authorities who have informed us that, although convictions have been obtained in serious cases of unauthorised damage to data or programs, there is recurrent (and understandable) difficulty in explaining to judges, magistrates and juries how the facts fit in with the present law of criminal damage.

2.32 Another disadvantage of the criminal damage offence is that the Criminal Law Act 1977 introduced special procedures for determining the mode of trial for criminal damage according to the value of the property damaged.[47] Broadly speaking, if the value involved is £2,000 or less, the magistrates proceed as if the offence were triable only summarily.[48] If the value is clearly over £2,000, the charge is dealt with like any other offence triable either way. Where computer data or programs are allegedly damaged, it may well be difficult to assess the value of such damage.[49] This difficulty would of course remain even if the Criminal Damage Act 1971 were amended, as some of our consultees have suggested, so as to include data and programs within the meaning of property for the purpose of that Act. We consider this point further in Part III below.

2.33 It is on any view unacceptable that there should be the present degree of uncertainty as to the conviction of persons who unlawfully alter or erase data. However, the only alternative to making it clear that such alteration or erasure of data is criminal would be to provide that such conduct should henceforth *not* be criminal at all. It is clear that that outcome would be unacceptable. We therefore *recommend* that the unauthorised alteration or destruction of data or programs, when it is done with intent to impair the operation of the computer or the reliability of data held in a computer, should be a criminal offence. Our preferred approach to the creation of such an offence is set out in detail in Part III of this report. For the reasons there given, we recommend the creation of a new offence, to be known by the broad title of 'the unauthorised modification of computer material', to be triable either way and to be punishable on conviction on indictment with imprisonment for up to five years.

---

[42] *Ibid.*

[43] 29 November 1984.

[44] See (1986) 83 Cr. App. R. 54, at pp. 56–58.

[45] (1865) L.R. 1 C.C.R. 7.

[46] "... to injure [a thing] so as to lessen or destroy its value." The Oxford English Dictionary, 2nd ed. (1989).

[47] See now Magistrates' Courts Act 1980, s.22.

[48] The offence is then punishable only with a maximum of three months' imprisonment or a fine of £1,000 or both: Magistrates' Courts Act 1980, s.33.

[49] In *Cox* v *Riley* it appears that the measure of damage taken was the cost of reprogramming the plastic circuit card.

PART III

THE TERMS OF THE NEW OFFENCES

A. INTRODUCTION

3.1 We have described in Part II of this report the considerations that have led us to conclude that it is necessary to introduce three new criminal offences which, broadly defined, would be:

(i) Unauthorised access to a computer;

(ii) Unauthorised access to a computer with intent to commit or facilitate the commission of a serious crime;

(iii) Unauthorised modification of computer material.

3.2 Although these offences deal separately with three different kinds of computer misuse, they are closely related in forming a code that imposes penalties of increasing seriousness according to the seriousness of the conduct with which they deal and the measures necessary to deter that conduct. In particular, offences (i) and (ii) above, unauthorised access to a computer and unauthorised access with intent to commit a serious crime, are intended to operate together in a 'hierarchical' manner, to provide an effective deterrent against all forms of unauthorised access. The first offence imposes restraints on the general mischief of unauthorised access to computers. Since its main purpose is the general deterrence of hackers, without requiring in any particular case proof of an intent to commit a further crime or of the alteration of the data or programs in the computer, it is appropriate that the crime should be a summary one only. That marks it off from the more serious form of hacking, committed with intent to facilitate a crime, which is justifiably met by a penalty of up to five years' imprisonment. A further serious form of computer misuse, the unauthorised alteration of computer data or programs, is equally met by a penalty of up to five years' imprisonment. Together these three offences will provide appropriate responses to each of the forms of computer misuse that we have described above.

3.3 We now consider each offence separately, indicating the policy and other limitations affecting its definition. We have already indicated, in paragraph 1.13 above, that the timescale within which this report has had to be completed has prevented us from following the Commission's normal practice of accompanying the report by a draft Bill. In order to make the nature of our recommendations clear we have sought in this part of the report to state as explicitly as possible what we consider the terms of the new offences should be. However, it will be appreciated that we have not attempted the formal drafting of legislation, and we recognise that in the event of our recommendations being adopted it will be necessary for these recommendations thereafter to be cast into proper legislative form.

B. THE UNAUTHORISED ACCESS OFFENCES

1. The basic unauthorised access offence

3.4 We indicated in paragraph 2.25 above that opinion on consultation was strongly in favour of a basic hacking offence, along the lines of Option D suggested in W.P. No. 110, and that we were persuaded that that remedy was justified and appropriate to meet the dangers presented by hacking that we had identified. That apparently straightforward solution however conceals a number of difficulties, both of policy and of definition, which we now consider.

3.5 We have indicated in paragraph 1.9 above that the term 'hacking' is conveniently used to refer to *all* forms of unauthorised access to computers, whether perpetrated by outsiders or by insiders, as we defined those terms in paragraph 1.20 above. However, as we said there, 'hackers' are quintessentially thought of as outsiders, entering or trying to enter from a distance systems with which they have no legitimate connection. It is in our view important to ensure when settling the terms of an offence that is directed at unauthorised users of a system or part of a system, whether outsiders or insiders, that one does not concentrate exclusively on outside hackers. Otherwise one may in so doing inadvertently direct *criminal* sanctions at employees, or other authorised users, who out of idle curiosity, or failure to seek authorisation that would if asked for be forthcoming, obtain access to part of their employer's data or computer system without permission.

3.6 With this in mind, we have given careful consideration to the *mens rea* of the unauthorised access offence, and also to the definition of 'access'. We indicate our recommendations on these matters in paragraphs 3.13-3.37 below. Our objective has been to ensure that the offence adequately encapsulates the basic conduct sought to be prevented, of trying to gain unauthorised access to a computer system, or to an unauthorised part of a computer system, without thereby criminalising those employees and other insiders who are merely careless, inattentive or imperfectly informed about the limits of their authority. At the same time, however, if an employee deliberately seeks to enter part of his employer's system from which he is clearly debarred his conduct is of the same type as the outside hacker, and our proposed offence will apply to him as much as it applies to the outside hacker.

3.7 We have also had to consider whether the offence should be *simply* to obtain or attempt to obtain unauthorised access to a computer, or whether the hacker should be required in addition to have some subsidiary purpose when seeking to obtain entry. Option D, the preferred choice of our consultants, was formulated in paragraph 6.35 of W.P. No. 110 as making 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."

We considered however, that we needed to review the issue of ulterior intent because it was raised by the Scottish Law Commission and in Miss Nicholson's Bill, and also because the presence or absence of a requirement of ulterior intent may have important implications for the level of punishment appropriate for an unauthorised access offence.

3.8 The offence proposed by the Scottish Law Commission[50] prohibited unauthorised access "in order to inspect or otherwise to acquire knowledge of the program or the data or to add to [etc] the data. . . with the intention of procuring an advantage for himself or another person, or of damaging another person's interests". The Scottish Commission explained these limitations by saying that an offence expressed *simply* in terms of unauthorised access might give rise to sentencing problems, as the activities that it covered could vary greatly in seriousness.[51] However, the further requirements that the Scottish Law Commission proposed in its view justified a maximum sentence of five years' imprisonment.

3.9 While we appreciate this concern, we are unable to agree with the legislative formulation to which it is thought to point. Ulterior intent limitations of this type, when set out in statutory form, either limit criminal sanctions to proven cases of fraud, dishonesty or malicious damage, or they do not. If they do so limit the law, there will be problems of proof and the law will also fail to impose sanctions on the casual hacker. The law would thus not achieve what we, and most of those replying to our consultation, thought to be principally required, namely a simple means of deterring all hackers, whether fraudulent or malicious or not.[52] If however the ulterior intent limitations are not interpreted in this strict fashion, but operate in practice to allow the law to catch most or all hackers, the (alleged) restriction of the definition of offences to serious cases will be in danger of being used as a justification for the attachment of severe penalties to types of conduct that vary widely in their seriousness.

3.10 Our view is that these problems can be avoided by adopting an offence that expressly covers all cases of hacking, as did Option D in W.P. No. 110, but carrying a comparatively moderate penalty. However, to cover more serious cases of hacking we *recommend* that, in addition to a basic unauthorised access offence, there should be a further offence of unauthorised access, which would consist of committing the basic unauthorised access offence with intent to commit or to facilitate the commission of a serious criminal offence. Where it can be established that the hacker was not a simple

---

[50] Clause 1(1) of the Draft Bill at p. 30 of Scot. Law Com. No. 106.

[51] Scot. Law Com. No. 106, paras. 4.5–4.8.

[52] In that respect, as we indicated in paras. 1.36–1.39 above, our evidence does not enable us to agree with the Scottish Law Commission that the terms of their offence " . . . draw attention to the real mischief at which [it is] aimed": Scot. Law Com. No. 106, para. 4.8. The weight of the evidence that we have received (much of which may not have been made available to the Scottish Law Commission) established that the mischief lies in attempts at securing unauthorised access, whatever the motive behind those attempts.

intermeddler, but was intent on serious criminality (even if he had not yet reached the stage of committing or even, in law, of attempting the offence in question), then in our view it is not enough to limit the sanction imposed on him to punishment of the level that we think appropriate for an offence of unauthorised entry.

3.11 In making this proposal we see the deterrent effect of the hacking offences as operating in what we have termed a 'hierarchical' manner: a summary offence to deal with the general mischief of hacking, but an offence with substantially greater penalties to deal with hackers who have distinctively criminal intentions. This approach, to balance the competing interests of effective deterrence on the one hand and economy of punishment on the other hand, was suggested by a number of those replying to our consultation, and in a helpful periodical article commenting on W.P. No. 110.[53] We set out in paragraphs 3.49-3.60 below the detailed terms of the ulterior intent offence, which we think will be a valuable addition to the weapons against computer misuse.

3.12 With that explanation of the background, we now indicate the terms in which we recommend the unauthorised access offences should be expressed.

(a) *The scope of the basic access offence*

3.13 For the reasons set out in Part II above we recommend that the essence of the offence, subject to the qualifications set out below, should be obtaining or trying to obtain unauthorised access to programs or data held in a computer. A person would only be guilty of that offence if he intended to try to gain such access and if he knew at the time of so intending that such access was unauthorised.

3.14 We therefore *recommend* the creation of an offence of access to computer programs or data that would provide that a person was guilty of the offence if he caused a computer to perform any function with intent to secure access to or obtain information about a program or data held in a computer. The *mens rea* of this offence would be that the accused, at the time when he caused the computer to perform the function, knew that his access was unauthorised.

3.15 Such a formulation would in our view constitute the gist of a clear and enforceable offence although, were a Bill to be drafted along such lines, it would need to contain other provisions to deal with some of the issues that we raise below.[54]

3.16 The intended scope of the offence is perhaps best illustrated by way of an analysis of a standard 'log-on' procedure common to many computer systems. First the computer user enters his identity code (often his name or initials) and his (secret) password. The second stage follows the verification of that combination by the computer system. If the combination is recognised the user is offered a 'menu' of available functions or, at least, the opportunity to access the services or information available from or held in the computer. We are informed that for security reasons it is becoming common for this stage to take the form of a clear screen, on the assumption that only authorised users will know how to proceed. The third stage is of course the taking of the opportunity offered at stage two to use the computer facilities.

3.17 We can illustrate the terms of the proposed offence by taking those stages in reverse order. At stage three the user unquestionably secures access to a program or data held in a computer. That person is guilty of the offence (subject to *mens rea*). At stage two, the user has caused the computer to perform a function (for example, displaying a menu or a blank screen) and he is guilty of the offence (subject to *mens rea*) because he intended thereby to obtain information (from the menu or welcome screen) with respect to any program or data held in the computer. This leaves the user at stage one. Under our proposals he would be guilty of the offence if (subject to *mens rea*) he causes a computer to perform a function (viz. check his identification combination) with intent to obtain information in respect of any program or data held in the computer. He will obtain information about a program or data stored in the computer by finding out whether or not the identification combination that he presents is recognised as valid by a program held in the computer. Since the offence consists in

---

[53] M. Wasik [1989] Crim. L.R. 257 at p. 262.

[54] For example, the meaning of "secure access to a program" and the fact that access to a program should include access to part of a program.

causing the computer to perform a function with intent to obtain that information, he will be guilty whether or not he succeeds in gaining the information, whether or not it is factually possible to gain that information and whether his aim is to obtain information about any particular program or data, or merely to explore the system generally.

3.18 The case where the offender reaches only the first stage will of course be unusual. Most detected hackers are likely to have actually gained access either to programs or to data. However, an offence defined solely in terms of gaining access to programs or data, or intending to do so, would not in our view be sufficient. There are two different grounds for that conclusion. The hacker who was detected at the first stage might claim that he was only interested in testing the system's defences, and not in actually gaining access to the system's contents. That claim might be hard to disprove. Secondly, however, the hacker who genuinely was merely (unauthorisedly) testing the system's defences would still in our view be someone whom the law should seek to discourage.

3.19 The position can be illustrated by reference to the provisional view that we put forward in paragraph 6.39 of W.P. No. 110, that special provision should not be made to deal with the person who unsuccessfully attempts to obtain access to a computer. Many commentators expressed concern about that approach, pointing out that much of the mischief caused by hacking arose from unavoidable uncertainty as to whether attempts to access systems had or had not been successful. We are persuaded of the force of those views, that the person who 'knocks on the door' of the target computer without authority may well be as productive of the mischief that the offence seeks to deter as is the person who actually gains entry. Since such conduct constitutes the gravamen of the offence, that fact should therefore be expressed by including the conduct in the definition of the main offence. That approach is in our view clearly preferable to leaving it to the courts to work out the difficult question of what conduct is 'more than merely preparatory',[55] so as to amount (under the general law of attempted crime) to an attempt to commit the consummated act of obtaining access.

3.20 The significance of 'attempts' is shown in practice by an example put to us by several consultees. A stereotypical hacker programs his computer to search through a dictionary in order to convey to the target computer (via a modem and a telephone line) every four letter word, in the hope of discovering one or more passwords that would enable him to secure (unauthorised) access to the target computer. An offence along the lines of our recommendation would be apt to cover such conduct, because such a person would be obtaining information (viz. whether a given password was or was not valid) in respect of a program or data held in the computer. It is right that such conduct should fall within the offence since the hacker's repeated attempts increase the uncertainty surrounding the integrity of the system, and cause the system operator to incur expenditure on monitoring and investigations into the source of the attacks, and on defensive mechanisms.

3.21 Within the general formulation of the offence, a number of matters arise for detailed consideration.

(b) *How must access be secured?*

3.22 A hacking offence is often expressed in terms of 'obtaining unauthorised access to a computer' or 'accessing a computer without authorisation'. For the purpose of drafting a criminal offence both phrases cause difficulty because they are apt to cover conduct other than that generally regarded as hacking. We are aware that the definition of the transitive verb 'to access' contained in the new edition of the Oxford English Dictionary is, 'To gain access to data etc., held in a computer or computer-based system, or the system itself.'[56] That definition carries the flavour of the concept that we wish to convey, but in general usage it may still be deficient in three particular respects. We consider these defects (which apply equally to 'the obtaining of access') in turn, and then explain why we have adopted the formulation suggested above.

3.23 First, the concept of access to a computer might be said to include merely coming into contact with a computer as a physical object; for example, an office cleaner

---

[55] Within the Criminal Attempts Act 1981, s.1(1).
[56] "The Oxford English Dictionary", 2nd ed. (1989).

entering without permission a room where there is a computer might be said to have obtained access to it. While such a person would never in practice be proceeded against, it would be undesirable to leave that question of policy to the discretion of the prosecuting authorities. Our view is that mere physical access ought not to constitute the offence, and that view was in general supported on consultation.[57]

3.24 Secondly, if the offence were expressed simply in terms of securing access to information, data or programs stored in a computer it might be construed as including the obtaining of access to 'hard-copy' of that information, etc., in the form of a print-out. Again, our view is that such conduct, while perhaps morally reprehensible, does not present the threat to the integrity of a computer system that is posed by 'electronic' hacking, which is the basis of the justification for the new offence.

3.25 Thirdly, in W.P. No. 110 we expressed the provisional view that it would be undesirable if a hacking offence were to overlap with certain kinds of computer eavesdropping.[58] Of those consultees who commented on this aspect of the Working Paper, opinion was fairly evenly divided. However, in our view the kind of conduct involved in electronic eavesdropping does not pose a threat to the operational integrity of the system concerned in the way that hacking does, but is aimed more specifically at the confidentiality of the information which it contains. It is therefore better regarded as a form of unauthorised surveillance, and as such raises issues beyond the scope of the present exercise. Our preferred definition of the offence does not extend to eavesdropping, and we do not think it right to recommend that special provision should be made for eavesdropping. Further, the technical evidence that we received convinced us that *at present* it is not possible except in the most favourable conditions and using sophisticated and expensive equipment to listen in effectively to emissions of electronic information from VDU screens, which is the typical case of electronic eavesdropping. That technical position might alter, but while that possibility justifies keeping the position under review, we could not recommend a change in the law solely because of possible future developments.

3.26 One way in which the definition of a hacking offence could be framed in order to exclude the three situations discussed above would be to define the *actus reus* in terms of 'causing a computer to perform any function'. That formulation covers any manipulation of a computer that is performed with the appropriate nefarious intent and is not, we believe, expressed in terms that technological developments might later render obsolete. It excludes *mere* physical access, and *mere* scrutiny of data, without interaction with the operation of the computer. If the *actus* were expressed in those terms, we recognise that the offence would extend, subject to *mens rea*, to the person who merely switches on a computer. We are satisfied, however, that the requirement that such access be intentional and unauthorised is a sufficient limitation on the offence, and that such conduct, with the appropriate *mens rea*, does carry with it the dangers associated with remote hacking.

(c) *The mens rea*

3.27 In our view it is necessary to make it explicit that the offence of unauthorised entry is only committed by someone who causes a computer to perform a function *with intent* to bring about the prohibited consequences. That is particularly so in view of the position of insiders and employees, to which we referred in paragraphs 3.4-3.5 above. Since it is possible for merely random tinkering with computer keys to admit an authorised computer user to an unauthorised level of access, we do not think that it would be right for the *mens rea* to be stated either expressly or impliedly in terms of recklessness only. As we said in paragraph 3.26 above, we recognise that our concept of securing access covers a broad range of conduct. We are therefore concerned to ensure that the offence should not become a 'catch all' for all forms of irregular conduct involving a computer, but should aim only at deterring the deliberate activities described in Part II above.

---

[57] In para. 1.16 of W.P. No. 110 we said that our use of the phrase "obtaining access to a computer" in that paper did not include the obtaining of *physical* access thereto.

[58] W.P. No. 110, para. 6.22. Within this concept have to be included both *electronic* eavesdropping by means of sophisticated electronic listening equipment and "passive" eavesdropping such as an employee simply looking at information displayed on a VDU that is outside the limits of his authority, but without exercising any control in respect of the information displayed. The essence of eavesdropping, as opposed to hacking, is that it does not involve, on the part of the eavesdropper, any operation of, or interference with the operation of, the computer system.

(d) *What consequences must be intended?*

3.28 We dealt in paragraphs 3.7-3.9 above with the objections to defining a *basic* hacking offence in terms of an ulterior intent to cause damage or secure a benefit outside the computer system; and with our reasons for recommending a special ulterior intent offence where the hacking is in order to further serious crime.

3.29 Our recommendation for a basic hacking offence does not require the hacker to have any intent that is directed outside the target computer system. It seeks to catch those who actively interfere with the system itself, in order to inspect its contents or test its access procedures. The offence would therefore require a person to cause a computer to perform any function with intent to secure access to or obtain information about any program or data held in any computer.

3.30 Several points need to be made about the concept of securing access to a program or data.

(1) It might be argued that a person did not 'secure access to a program' merely by running it, but only by accessing its constituent program instructions. Our view is that the offence should cover any use of a program (including but not restricted to causing a computer to display or output program instructions held therein) and that securing access to a program should be defined accordingly in any legislation.

(2) Securing access to a program should for the avoidance of doubt be defined to include the securing of access to *part* of a program.

(3) The ordinary meaning of 'data' is that of information or facts stored or held in a computer, and we do not consider that a technical definition, (such as that contained in section 1(2) of the Data Protection Act 1984) is desirable in the context of a criminal offence. However, in our view the legislative definition of the offence ought for the avoidance of doubt to make it clear that securing access to data includes causing a computer to display the data or to output it in some other form.

3.31 The concept of obtaining information about a program etc., is included to deal with the situation described in paragraph 3.18 above: that is, the person who attempts to log-on to a computer system without authority. Such a person intends to obtain information in respect of a program or data because he intends to discover whether a particular combination of identification and password will or will not enable him to gain access to programs or data held in the computer. We recognise that it *might* be sufficient if the offence were defined simply in terms of obtaining information, since a person who actually secures access to a program or data will thereby obtain information about it. However, since the case most likely to arise will be that of the person who not only intends to but actually does obtain access to a program or data, we think that that case should be expressly set out in the definition of the offence.

3.32 One further gloss on the intended object of the accused is likely to be necessary. That is, a person should be guilty of the offence if he intends to secure access to (or obtain information in respect of) any program or data held in *any* computer. He need not direct his intention to any particular program or data. In other words, he commits the offence if, were he successful in his operation of the computer, he would or might without authorisation secure access to (or obtain information in respect of) programs or data. That provision is in our view reasonable and necessary because a hacker who attacks a computer may well not know in advance, or care, what *particular* data or programs it contains.

(e) *Unauthorised*

3.33 We recommend that the basic hacking offence should not only require that the person secures the prohibited access intentionally and without authorisation, but that at the time he causes the computer to perform the function he should know that that access is unauthorised. We would suggest that a person's access to any program or data held in a computer should be regarded as unauthorised for these purposes if (a) some person other than the person whose access is in question is entitled to control access to the program or data; and (b) the person whose access is in question does not have consent from any such entitled person.

3.34 In the case of the remote hacker, working from his own home, there will usually

be no question but that he is acting without authorisation. However, the precise definition of authorisation is of particular relevance to the position of insiders and employees, and we discuss it in that context.

3.35 While the main justifications for a hacking offence concern the problems caused by attempts at securing unauthorised access from locations remote from the site of the computer, we recognise that most surveys in this area have shown that hacking is commonly perpetrated by employees or insiders who already have some degree of legitimate access to the system but who exceed the bounds of their authority. The thrust of the basic hacking offence is aimed at the 'remote' hacker, but the offence is apt to cover the employee or insider as well. For that reason it is particularly important, as we said in paragraphs 3.5-3.6 above, that (in addition to defining 'access' to exclude merely physical access to the computer itself) the *mens rea* of the offence should catch only the case where the employee consciously and deliberately misbehaves.

3.36 The first element in consideration of this point is that if the hacking offence is to be aimed at protecting the integrity of the computer (and our view is that it should), then there is no justification for exempting employees who threaten that integrity. We have emphasised in paragraph 3.27 above the importance that we attach in every case to a definition of *mens rea* in terms that make it clear that intentional and not merely reckless access is required. Any conduct by an employee that fell within the definition would, from the point of view of the consequences that he intended to produce, be a deliberate act of disobedience, and indeed of defiance of the law, and not merely carelessness, stupidity or inattention. The latter might legitimately attract disciplinary sanctions, but should not in our view be a ground of criminal liability.

3.37 There is however the further issue of whether the accused knows that his deliberate interference with the system is unauthorised. In paragraph 6.24 (i) of W.P. No. 110 we adverted to the possible difficulties that might arise in determining whether a particular employee in fact had authority to obtain access to a computer, and suggested that one possible solution might be to provide for a defence of belief in authority. On further consideration, we have formed the view that it would be more appropriate if the burden of proving that access to a program or data was known to be unauthorised were to rest on the prosecution. In most cases where prosecutions are brought, there will be no room for the 'remote' hacker to argue that access was authorised: it will be a simple matter for the person responsible for running the computer system to refute that claim. Where the offence is allegedly committed by an employee, we think that an employer should only have the support of the hacking offence if he has clearly defined the limits of authorisation applicable to each employee, and if he is able to prove that the employee has knowingly and intentionally exceeded that level of authority. We think that there is some importance in requiring the court, in a case where there is a dispute about authorisation, to identify, and to be clear about the status of, the person alleged to have authority to control the access which is in issue. In our view (and consultation has confirmed this point) such regulations should be laid down as a matter of good management practice, and if placing the burden of proving that access was known to be unauthorised on the prosecution encourages such practices, that can only be a good thing.

(f) *Use of a computer for unauthorised purposes*

3.38 There was strong support on consultation for the view expressed in paragraph 6.24(iv) of W.P. No. 110 that an authorised user should not commit a hacking offence merely because he uses the computer for an unauthorised purpose, and we so *recommend.* Such misconduct will vary infinitely in seriousness and may well involve general offences of dishonesty. It may also fall within our proposed offence of 'unauthorised modification',[59] subject to the important requirement that the computer owner would have to show that the addition of data or programs had *impaired* the operation of the computer. That may be difficult to establish where the alleged offender has used only a small fraction of the capacity of a large system. Generally, however, our view remains that there is nothing to distinguish the misuse of an employer's computer from the misuse of the office photocopier or typewriter, and that it is therefore inappropriate to invoke the criminal law to punish conduct more appropriately dealt with by disciplinary procedures.

[59] See paras. 3.61–3.79 below.

(g) *Computer*

3.39 Our consultees generally agreed with the view expressed in paragraph 6.23 of W.P. No. 110 that it would be unnecessary, and indeed might be foolish, to attempt to define computer; nor was there much enthusiasm for the *tertium quid* of definition by partial exclusion. In view of the nature of the proposed hacking offence, especially the *mens rea* required, (and the same considerations apply to our other proposed offences) we cannot think that there will ever be serious grounds for arguments based on the ordinary meaning of the term 'computer'. By contrast, all the attempted definitions that we have seen are so complex, in an endeavour to be all-embracing, that they are likely to produce extensive argument, and thus confusion for magistrates, juries and judges involved in trying our proposed offences.

(h) *Mode of Trial and Penalty*

3.40 We indicated in paragraphs 3.10-3.11 above that we see the basic hacking offence as operating in conjunction with a more serious offence of hacking with a specified form of ulterior intent to commit a serious crime. We recommend that the basic offence should be triable summarily only, in order clearly to differentiate the two offences.[60] We are accordingly unable to recommend that that offence should be punishable with a maximum of five or ten years' imprisonment, as was considered appropriate, for somewhat differently defined offences, by the Scottish Law Commission and Miss Nicholson respectively.

3.41 It has however been suggested to us that it would be appropriate to impose a maximum sentence of two years' imprisonment, by analogy with the penalty provided for the interception of a communication in the course of its transmission by post or by means of a public telecommunication system, contrary to section 1 of the Interception of Communications Act 1985; the argument being that if data is thus protected when in the course of transmission it should be similarly protected when on a private system or when it has reached its destination. We do not however think that the analogy is a complete one. The justification given by ministers for the creation of the interception offence was that "there is a special case for dealing with the interception of communications passing through public communications systems, because somebody has committed such a communication to a carrier over which he has no control and is entitled to believe that, except for good reason, his privacy will be safeguarded".[61] Every offence committed under the Interception of Communications Act therefore has in common the particularly serious consideration of invasion of a public service. By contrast, cases of basic hacking will cover a wider range of types of conduct, many of which will not reasonably merit penalties of the order envisaged by the 1985 Act. More serious cases of hacking, that fall within our proposed ulterior intent offence, will however be subject to a more serious penalty: see paragraph 3.59 below.

3.42 Following our recommendation that the basic offence should be triable summarily only, it must be a matter of judgment as to what maximum penalty is required to achieve our objective of generally deterring the kind of conduct that our offence would criminalise. Our conclusion is that in view of the persistent and widespread nature of hacking, and its popularity in some circles,[62] the necessary communication of disapproval and discouragement of hacking will not be achieved by an offence that is limited to monetary penalties.

3.43 It was pointed out in paragraph 6.38 of W.P. No. 110 that none of the criminal offences created by the Data Protection Act 1984 carry a penalty of imprisonment. We do not however regard that as a conclusive guide, since that Act is mainly concerned with regulating the conduct of registered data holders, or persons who ought to have so registered. That special situation, already closely regulated by administrative means, may be thought not to have required the further support of the possibility of imprisonment.

3.44 The maximum penalty that a magistrates' court may impose for a single offence is six months' imprisonment. We considered carefully whether this would be

[60] This raises the further issue of how to deal with the six month time limit within which summary offences must usually be brought, and we deal with this matter at paras. 3.46–3.48 below.

[61] *Hansard* (H.C.), 12 March 1985, Vol. 75, col. 255.

[62] See for instance n.32 to para. 2.17 above.

appropriate for the basic hacking offence. If the offence were punishable with a sentence of imprisonment of *any* duration, the sentencer would also be able to impose a community service order instead of a custodial penalty,[63] and this might well be a very suitable option to have available in dealing with cases under our proposed offence. However, we are concerned that if the offence carries a maximum penalty of *six* months' imprisonment, magistrates might receive the impression that the offence was regarded as sufficiently serious to deserve a custodial sentence in most cases. We do not wish to give that impression. In our view only the most deliberate and persistent of unauthorised access, if not done with intent to commit another offence, should be subject to imprisonment: though, as we indicated above, that sanction should be available for the worst cases.

3.45 In view of those considerations, we *recommend* that the basic hacking offence that we propose should be punishable with a maximum of three months' imprisonment or a fine of up to Level 4 on the standard scale (i.e. £1,000);[64] or both. We should also draw attention here to the general power of a criminal court to order an offender convicted of any offence to pay compensation to the victim of his offence for any loss or damage resulting from that offence.[65]

(i) *Time limits for prosecutions*

3.46 Section 127 of the Magistrates' Courts Act 1980 provides that a magistrates' court shall not try an information alleging a summary offence unless the information was laid within six months from the time when the offence was committed. Several of our consultees expressed the view that, if hacking were to be a summary offence, the particular nature of the investigative work that might be necessary could make it impossible to initiate proceedings within that six month time limit. We agree with that view.

3.47 There exist already a number of precedents modifying the six month limit in respect of certain offences. Two recent examples of such statutory modifications in respect of particular offences are the Road Traffic Offenders Act 1988, section 6, and the Social Security Act 1986, section 56. There appear to be two distinct kinds of provision, those which provide for an eventual (albeit extended) time limit during which cases must be brought, and those without such a long-stop.[66] A further relevant consideration is that the justices' clerk has a discretion to refuse to issue a summons on the ground of unjustifiable delay, even if the information is laid within the appropriate statutory limit, and the court can refuse to proceed after such a delay, on the ground that where such a delay may prejudice the defendant it can constitute an abuse of process of the court.[67]

3.48 In the light of the particular difficulties in detecting hacking offenders, we think that section 127 should be abrogated in relation to the basic hacking offence. However, we do not consider that it would be appropriate to provide for an open-ended period during which a prosecution might be brought. The summary offence is relatively minor and therefore, while recognising the difficulties in investigation, we would not wish to encourage either very lengthy enquiries, or investigations into incidents that took place many years earlier, if the only result of such investigations were a charge of basic unauthorised access. Of course, where there is evidence of hacking with an ulterior intent, our more serious offence would be applicable and no time limits would apply. Accordingly we *recommend* that the basic hacking offence should be subject to a

---

[63] Powers of Criminal Courts Act 1973, s.14.

[64] The standard scale of fines for summary offences is contained in the Criminal Justice Act 1982, s.37 and was amended (pursuant to section 143(2) of the Magistrates' Courts Act 1980) to take into account the change in the value of money by the Criminal Penalties etc. Increase Order, S.I. 1984 No. 447.

[65] Section 35 of the Powers of Criminal Courts Act 1973, as amended by the Criminal Justice Acts of 1982 and 1988. A magistrates' court may make a compensation order, in an appropriate case, up to a value of £2,000: Magistrates' Courts Act 1980, s.40.

[66] Section 6 of the 1988 Act provides that summary proceedings may be brought within six months from the date on which evidence sufficient in the opinion of the prosecutor to warrant proceedings came to his knowledge, subject to a long-stop preventing such action more than three years after the commission of the offence. The relevant date is proved by a certification procedure. Section 56 of the 1986 Act permits the appropriate prosecuting authority to bring proceedings within three months from the date on which evidence, sufficient in the opinion of the prosecutor to justify a prosecution, comes to his knowledge, or within 12 months from the commission of the offence, *whichever period last expires.*

[67] *R* v *Clerk to the Medway JJ., ex p. D.H.S.S.* [1986] Crim. L.R. 686.

provision along the lines of section 6 of the Road Traffic Offenders Act 1986, that proceedings must be brought within six months from the date on which evidence, sufficient in the opinion of the prosecutor to justify a prosecution, came to his knowledge, subject to a long-stop preventing a prosecution being brought more than three years after the offence was allegedly committed.

2. The ulterior intent offence

3.49 The essence of our second and more serious offence aimed at hacking is the commission of the basic unauthorised access offence *with intent* to commit or to assist the commission of a further more serious criminal offence, whether or not that further offence would involve the use of a computer. It is therefore a preliminary offence, in the sense that it falls short of the commission of the further offence; but it is also an aggravated form of the basic hacking offence. We therefore *recommend* the creation of an offence of committing the unauthorised access offence with intent either (a) to commit an offence for which the maximum penalty is five years' imprisonment or more; or (b) to facilitate the commission by himself or by any other person of any such offence.

3.50 We propose that this offence should be triable either way and punishable on conviction on indictment with imprisonment for up to five years. Within that general formulation of the offence a number of matters arise for detailed consideration. First, however, we consider the relationship between our proposed offence and the law relating to attempts to commit a substantive offence.

(a) *The law of attempts and the ulterior intent offence*

3.51 Section 1 of the Criminal Attempts Act 1981 provides that-

> "(1) If, with intent to commit an offence to which this section applies, a person does an act which is more than merely preparatory to the commission of an offence, he is guilty of attempting to commit the offence."

That definition requires there to be identified acts done by the accused which are immediately and not merely remotely connected with the commission of an offence. That distinction can, on the facts of a particular case, be difficult to draw. We also consider that there are circumstances in which hacking for a particular criminal purpose, although clearly not amounting to an attempt to commit the substantive offence, ought to be capable of prosecution as a serious criminal offence. Two examples may help to bring out these points.

3.52 The first concerns the hacker who gains access to a banking computer system without authorisation. For that person to persuade that computer system to transfer funds from another person's bank account to his own account, he will have to overcome further security checks. If some of those checks consist of secret passwords, the hacker may have to try a large number of alternatives in order to find one that works. If he manages to transfer and remove the funds, he will have committed theft. At what point, however, does he commit attempted theft? Trying the passwords in such a case probably does not amount to an act that is more than merely preparatory to the theft—especially if some subsequent steps would be required to transfer the funds. However, in our view it is undesirable that such a person may only be prosecuted for a serious offence if he actually succeeds in stealing the money. The speed with which such a theft may be carried out using a computer and the consequent difficulty of detecting the perpetrator require in our view a special extension of the criminal law in order to discourage such conduct, by exposing the hacker to prosecution at an early stage. Under our proposed ulterior intent offence such a person, if he were detected trying to find the password, would at that stage have committed the offence of obtaining unauthorised access to a computer with intent to steal.

3.53 The second example concerns the person who hacks into a computer (within the meaning of our basic offence) in order to obtain confidential and personal information which he intends to use in order to blackmail someone. That person would certainly not be guilty of an attempt to blackmail (because his conduct at that point is merely preparatory), but he would be guilty of unauthorised access with intent to blackmail, contrary to our proposed ulterior intent offence.

(b) *Intent to commit a further offence*

3.54 Our general outline of the ulterior intent offence provides that an intent to commit any further offence that carries a penalty of five years' imprisonment or more should be sufficient to constitute the offence. We propose that general test while acknowledging that there will be offences that, by their very nature, are unlikely in practice to be further offences for the purposes of our proposed offence. However, we did not consider that it would be prudent or indeed possible to draw up a list of offences that might constitute such a 'further' offence, because it is not possible to draw up a finite list of the nefarious ends that a person might try to achieve by first securing unauthorised access to a computer. An indictment for the ulterior intent offence would contain particulars of the further offence allegedly intended.

3.55 While the further offences are most likely in practice to be ones of dishonesty, protection of the person is not neglected. An (at present hypothetical) case is the person who hacks into a hospital computer containing details of blood groups and rearranges that data with the intention that a patient should be seriously injured by being given the wrong blood. If such an incident did occur, and the patient was seriously injured, the fact that a computer was used to cause the injury would not prevent a charge of assault or murder being brought, as appropriate. Our ulterior intent offence is aimed at the narrow area of conduct preliminary to the commission of the crime, falling short both of the completed offence and an attempt to commit that offence, where at present there is no criminal sanction. If enacted, the person in our example would be guilty of an offence punishable with a maximum of five years' imprisonment when he obtained the unauthorised access with the appropriate intent.

3.56 Since we are here concerned with acts preliminary to the commission of other crimes, we think that the law should be limited to use of a computer with a view to committing crimes of a reasonable degree of seriousness. We have selected the limit of offences carrying at least a five-year penalty as a broad indication of that seriousness. The same test is applied to determine what is an arrestable offence under the Police and Criminal Evidence Act 1984.[68] We also consider that that limit fits in with what in our view would be the proper maximum penalty for our proposed 'ulterior intent' offence, namely also five years' imprisonment.[69] That limit would further, in the case of reasonable suspicion of the commission of that offence, make available under the existing law certain powers of arrest, search and seizure.[70]

(c) *Facilitating the commission of a further offence*

3.57 A provision in these terms is necessary to ensure that the offence covers the person who claims (possibly truthfully) that he was not hacking in order himself to steal by transferring funds into his bank account, but (for instance) in order to enable a friend to commit such a theft. It also extends the offence to hacking in order to commit an offence not in that computer, but elsewhere, as in the blackmail example given above. It should be made clear in any legislation that the further offence may be intended to be committed on the same occasion as the hacking offence or on any future occasion.

(d) *Intent to commit an 'impossible' further offence*

3.58 Section 1(2) of the Criminal Attempts Act 1981 provides that-

> "A person may be guilty of attempting to commit an offence to which this section applies even though the facts are such that the commission of the offence is impossible."

Our proposed offence bears some relation to an attempt, to the extent that the intention to commit a further offence is not carried out. We would therefore recommend that a clause along the lines of section 1(2) should be included in any legislation creating the new offence, in order that it should be possible to convict a person who intended to commit the further offence even if, on the facts, that would not be possible.

---

[68] s.24(1)(a) and (b).
[69] See further para. 3.59 below.
[70] See further paras. 4.10–4.12 below.

(e) *Penalties and mode of trial*

3.59 Our new offence is intended, as we stated above, to occupy a position in a range of offences based on the securing of unauthorised access of a computer. Of course, the further offences contained in it will vary widely in their maximum punishment. However, the gravamen of the conduct in each case is the initial hacking; the unlawful intent aggravates conduct which is already an offence, and we therefore consider it right to have one maximum penalty irrespective of the maximum penalty provided for the alleged intended further offence. In our view, the appropriate penalty would be, on conviction on indictment, imprisonment for a maximum of five years.

(f) *Conviction of a lesser offence*

3.60 Where a person is tried on indictment for the ulterior intent offence, it should in our view be possible for the jury to acquit him of the ulterior intent offence, but to convict him of the basic hacking offence, and we recommend that a provision should be included to achieve that result.[71] Following such a verdict, the Crown Court should have the same sentencing powers in respect of that offence as the magistrates' court would have had.[72]

C. UNAUTHORISED MODIFICATION OF COMPUTER MATERIAL

3.61 We recommended in Part II of this report the creation of a new criminal offence to deal with the unauthorised alteration or destruction of data or programs. The form that such an offence should take has caused us some difficulties, and it may be helpful to set out those difficulties in order to assist explanation of our final recommendation.

3.62 A number of consultees who thought that the law of criminal damage was inadequate for this purpose suggested that a simple and effective remedy would be to amend the Criminal Damage Act 1971 so that the definition of 'property' contained in section 10 of the Act included 'data' and 'computer programs'. We have considered this solution, but do not consider it to be a viable option for law reform. Three reasons have so persuaded us-

(1) The general offence of criminal damage was created, following the recommendations of the Law Commission,[73] to replace a vast array of offences which each dealt with damage to particular forms of property. That property was invariably of a tangible nature. The Act does not elaborate on the meaning of 'damage', but for the reasons set out in paragraphs 2.29-2.30 above we think the better view to be that that meaning requires an element of physical injury. For that reason the offence is not apt to deal with the non-physical interferences with computer programs or data, and this problem would remain even if the meaning of property were to be extended in the manner suggested. We see force in the point that, in view of the theoretical difficulties posed by applying the concept of damage to intangible property such as data or programs, a person's guilt in every case tried on indictment may in practice depend on a jury's view as to what the ordinary meaning of the word damage should include. That would render the law unacceptably uncertain.

(2) An amendment along the lines suggested would not assist a magistrates' court in determining the value of the property damaged in order to decide the mode of trial.[74] Should this value be calculated by reference to the cost of replacing data or programs and, if so, how can commercially or scientifically unique data bases be valued, and how does one measure the cost of interruptions to an operational computer system? We do not feel that it is possible to resolve such questions in a satisfactory manner.

(3) The *mens rea* of criminal damage is intention or recklessness. Our view is that the new offence should cover only intentional conduct, so a basic amendment of the 1971 Act would not establish what we consider to be the appropriate *mens rea* in respect of

---

[71] The general provision enabling an alternative conviction to be returned (contained in section 6(3) of the Criminal Law Act 1967) does not apply when the alternative offence is triable summarily only.

[72] A provision along the same lines as we propose is contained in the Public Order Act 1986, ss.7(3) and (4).

[73] (1970) Law Com. No. 29, Offences of Damage to Property.

[74] See para. 2.32 above.

data and programs.[75] We have concluded that this offence should be limited to the person who deliberately sabotages a computer system by interfering with programs or data held in it in order to mark that case off from the person who alters data without authorisation but 'recklessly' in the criminal damage sense of the term. The latter will by no means escape punishment, since he will already be guilty of the basic unauthorised access offence, but his additional corruption of data may well be inadvertent, and no part of his plan. We consider that such a hacker is appropriately treated and deterred by the unauthorised access offence. It would not be justifiable to put him on the same level as the person who wants to alter or erase data without authorisation, who is properly subject to a much more severe penalty.

3.63 We conclude, therefore, that the intended limits of the new offence could not satisfactorily be accommodated within the present scheme of criminal damage offences. One illustration of the kind of conduct that we feel should fall outside an offence of unauthorised alteration, but which would be difficult to exclude from an amended version of the 1971 Act, is the employee who, without authorisation, loads software from a floppy disk of unknown provenance, that is in fact infected with a virus, on to his employee's computer. We are informed that there is always a risk that software from any source, but most especially pirated copies, could be infected with a virus. Such a person has certainly been careless, and may be reckless, but his conduct falls short of that degree of deliberation which marks out the person who actually intends to erase or alter data or programs without authorisation.

3.64 Accordingly, we *recommend* the creation of a completely new offence, triable either way and punishable on conviction on indictment with imprisonment for a maximum of five years. We envisage that such an offence should be known by the short title of unauthorised modification of computer material. Its principal content should be that a person is guilty of the offence if he causes an unauthorised modification of the contents of any computer's memory or of the contents of any computer storage medium, with intent thereby to impair the operation of any computer or computer program, or to destroy, or to impair the reliability or accessibility of, any data stored or otherwise held in any computer.

3.65 Our proposed new offence is intended to cover several forms of conduct, the most important of which are the following-

(1) What might be called 'simple' unauthorised modification, where a person intentionally and without authorisation (electronically) erases or wipes clean programs or data contained in a computer's memory or on a storage medium (such as a disk or streamer tape). The offence is not intended to cover *physical* damage to the computer or to disks etc., which would remain within the general law of criminal damage.

(2) The putting into circulation of floppy disks which are 'infected' with a virus, intending that that disk will cause some person somewhere to suffer a modification that will impair the operation of his computer.

(3) The unauthorised addition of a virus or worm to a computer's 'library' of programs, intending thereby to impair the operation of the computer simply by using up its capacity.

(4) The unauthorised addition of a password to a data file, thereby rendering that data inaccessible to anyone who does not know the password.

Bearing those examples in mind, we now turn to more detailed points arising from our general formulation.

1. Unauthorised

3.66 We consider it desirable that 'unauthorised' should bear the same meaning in all the offences that we are proposing in this report. We therefore refer here to our

[75] The meaning of "recklessness" in this context has exercised the appellate courts on a number of occasions in recent years. The present state of the law is in our view unsatisfactory, since "recklessness" includes the taking of an obvious and serious risk, whether or not the risk-taker realises that such a risk exists. A general discussion of the issue is not necessary here, the Commission's concern having been recently documented in paras. 2.8, 3.31 and 8.17–8.19 of A Criminal Code for England and Wales, (1989) Law Com. No. 177, Vols. 1 and 2. We would only point out that at present the *mens rea* of criminal damage makes it difficult to distinguish even between inadvertent and reckless conduct: neither of those states of mind should suffice for the proposed new offence.

discussion of the concept at paragraphs 3.33-3.37 above. In the context of the present offence, in order to show that a modification was unauthorised the prosecution will have to show first that some other person was entitled to decide whether to authorise such a modification, and secondly that that person did not give the requisite consent.

2. Causing a modification

3.67 This concept is intended to avoid the problems caused by the physical component in 'damage' that we identified above.[76] We suggest that in any legislation the concept should be further defined to make it clear that causing a modification of the contents of a computer's memory or a computer storage medium includes-

(1) Causing a program or data to be stored or 'held' in, or erased from, a computer's memory. In *Gold and Schifreen*[77] the House of Lords upheld the respondents' contention that 'recorded or stored'[78] entailed some degree of permanence. The addition of 'held' here denotes a temporary process.

(2) Causing a program or data to be stored on or erased from a computer storage medium. Such a medium would include any disk, tape or similar storage medium designed for storing computer programs or data in a form in which they could be processed by a computer. A 'computer's memory' by contrast is more apt to cover areas of 'read only memory' ('ROM') and 'random access memory' ('RAM') within the computer.

(3) Causing a program already stored on a computer storage medium (or stored or held in a computer's memory) to be altered in any way.

Modification should expressly include both temporary and permanent modifications, by analogy with the meaning of damage under the Criminal Damage Act 1971. Of course, any modification would have to be shown to 'impair' the operation of the computer or the reliability of any data held in it. 'Causing a modification' is therefore apt to cover any alteration or erasure of or addition to the contents of a computer's memory or a computer storage medium. It includes, subject to *mens rea*, both simple alteration or addition[79] and the introduction of a worm or virus that, without altering existing programs or data, uses up the computer's capacity.[80]

3.68 The term 'contents' is not used in our proposed offence in any technical sense, but is a way of including, for example, data and programs, while also avoiding the need for a technical explanation of exactly what forms such 'information' or 'instructions' might take. For example, by adding a worm to a computer's library of programs a person clearly causes a program to be stored by a computer's memory or on a computer storage medium. We do not consider it necessary to explain in the definition of the offence how such a program works.

3.69 There is one particular situation, however, which requires an extension of the definition of 'causes a[n unauthorised] modification' beyond that explained above. That is example (2) in paragraph 3.65 above: the person ('X') who copies a virus on to a floppy disk and then puts that disk into circulation, with the eventual result that another, possibly unknown, computer is infected by the virus. Clearly, when X copies the virus on to his own disk he is making an *authorised* modification to a computer storage medium, and therefore does not commit the offence. Equally clearly, when he puts the virus into circulation he does not know which (if any) computer will eventually be infected or indeed what (if any) impairment will be caused, and one cannot therefore say that he has at that stage 'caused a modification.'[81]

3.70 We think that this case can be met by providing that the offence is committed if, at the time the accused does an act which eventually causes an unauthorised modification, he intends to cause a modification of the contents of any computer

---

[76] See para. 3.62(1).
[77] [1988] A.C. 1063.
[78] In s.8(1)(d) of the Forgery and Counterfeiting Act 1981. See further W.P. No. 110, paras. 3.14–3.22.
[79] Examples (1) and (4) in para 3.65 above.
[80] Example (3) in para. 3.65 above.
[81] Neither can one properly say that he has attempted to cause a modification, because it is unlikely that his action is more than merely preparatory to the commission of the offence, within s.1(1) of the Criminal Attempts Act 1981: see para. 3.51 above.

memory or of the contents of any storage medium, and knows that the modification that he intends to cause is unauthorised. X in our example therefore does the act which results in the modification when he puts the infected disk into circulation, *provided* that he intends to cause an unauthorised modification to a computer's memory etc. somewhere. If X in London gives a disk that he knows to be infected to an innocent agent Y, who does not use it but gives it to Z in Newcastle, who does not use it but gives it to V in Plymouth, who copies the contents of the floppy disk including the virus on to his own hard disk and thereby has his data files corrupted then, provided that X intended when he gave Y the disk that a computer's memory etc. should be impaired, it matters not that X did not know the identity of the target computer, nor that he did not know the precise form of the modification that would result. We have been told that the problem of infected disks is substantial and serious, and we consider that the law should make adequate provision to meet that case.

3. The intent to impair

3.71 To constitute the offence the unauthorised modification must be caused with intent either (a) to impair the operation of any computer or computer program; or (b) to destroy, or to impair the reliability or accessibility of, any data stored or otherwise held in any computer's memory or stored on or in any such medium.

3.72 We have introduced the concept of impairing the operation of the system or destroying data because we think it important that the offence should not punish unauthorised modifications which improve, or are neutral in their effect on, the computer or its operations (including data holding). For example, on a simple network of computers used for word-processing purposes it might be the case that certain file management functions, such as copying and transferring files between users, are vested only in persons with special system privileges. If an ordinary user were to gain access to a general password and then copy a file from another person to his directory, that would amount to a modification of a computer storage medium. Without the requirement of an intent to impair the operation of the system, such a person would be liable to conviction of a serious criminal offence. Of course, his conduct would be a deliberate contravention of his employer's instructions, but we believe that such conduct is sufficiently dealt with by our basic unauthorised access offence which, subject to the act being clearly shown to be unauthorised, such an employee would commit.

3.73 It should be made clear that the intent need only be a general intent. That is, the accused must be shown to intend (for example) to impair *some* computer or to destroy *some* data, but his intention need not be directed at any *particular* program or data or at the operation of any particular computer.

3.74 The effect of a requirement of intention to impair is similar in some respects to the use of the concept of 'damage' in the Criminal Damage Act 1971. However, while it is unusual for there to be any argument in a case of *physical* damage as to whether the alleged acts constituted damage or improvement, in our view it is likely that with cases of modification of data or programs such difficulties may arise more frequently. We think that it is right therefore that the prosecution should have to show that the alleged modification was caused with intent to impair.

3.75 We should make one further point about the range of this offence. It is intended to catch those who actively interfere with the operation of a computer or with data held on it, with nefarious intent. To cover all such cases we have thought it right, as indicated in paragraph 3.66 above, to include cases of causing data to be temporarily held in a computer. However, that case might arguably include the initial act of attempting to log on, as described in paragraph 3.16 above. We do not intend that act to be covered by the unauthorised modification offence, even if it is committed with an intent to bring about an impairment, etc., in the future, once the hacker has successfully secured access. To make that clear, and to demonstrate the need to show a close connexion between the modification and the impairment, we have suggested in paragraph 3.64 above that the modification must be made with intent *thereby* to produce the stated consequences to the computer, program or data.

3.76 We have included case (b) in paragraph 3.71 above because there may be some deliberate attacks on *data* which should be covered by this offence, but which might be

argued not to involve an intent to impair the *operation* of the computer or one of its programs. Thus, for instance, a disk might be 're-formatted', effectively removing entirely all the data that it previously held, a situation that in our view is properly described as the destruction of data. Or a file on a disk may be 'deleted' with the effect that the area on the disk that it previously occupied is no longer marked out ('flagged') as an area that cannot have other data stored on it. Such a file may still be recovered by a computer expert, and so is not 'destroyed' until either that area on the disk is overwritten with other data or the disk is reformatted, but the accessibility of the file is in our view impaired. Or data may be corrupted, thereby impairing its accuracy and thus its reliability. Or, as in example (4) in paragraph 3.65 above, a modification may be made that denies the authorised user access. An intention to bring about any of these interferences with the proper running of the system should, if it is proved to be unauthorised, fall under the more serious offence of unauthorised modification.

3.77 We recognise that this offence is capable of catching some cases of authorised use of a computer for unauthorised purposes: for example, the employee who adds data to his employer's computer in order to help run his own business, or even to work out permutations for his football pools coupon. We have stated elsewhere that we see no justification for a special offence to cover such conduct. We would make the point here that unauthorised use could only constitute this offence if an intent thereby to impair the operation of the system could be shown, and that would be difficult where the employer's computer has a very large capacity and the employee's use is comparatively minor.

4. Relationship of our proposed offence to the Criminal Damage Act 1971

3.78 We *recommend* that it should be made clear in any legislation that neither an unauthorised modification of a computer's memory or computer storage medium, nor any resulting impairment of computer operations or data, should be capable of amounting to criminal damage under the 1971 Act. That would in effect reverse the decision in *Cox* v *Riley*. Our reason for this recommendation is that if it is accepted that the new offence should deal with all computer interference cases, and carry a maximum penalty of five years' imprisonment, it would not be right to perpetuate the present confusion, and also expose offenders to potentially higher penalties, by continuing to use the 1971 Act. This recommendation would not of course prejudice the operation of the 1971 Act in cases where the unauthorised modification leads to actual physical damage. For example, if a computer-operated saw were reprogrammed so that it ruined a load of timber, then (subject in both cases to the presence of the appropriate *mens rea*) the re-programming would amount to unauthorised modification and the consequent damage to the timber would come within section 1 of the Criminal Damage Act 1971.

5. Mode of trial and penalty

3.79 The offence of criminal damage contrary to section 1(1) of the Criminal Damage Act 1971 is triable either way and punishable on conviction on indictment with a maximum of ten years' imprisonment.[82] In our view, however, the maximum punishment for an offence which is limited to interference with computer programs or data need not be as severe. We therefore *recommend* that the unauthorised modification of computer material should be triable either way and punishable with a maximum of five years' imprisonment.

[82] Although we would at this point draw attention to modern sentencing practice in such cases, which is to impose sentences very much shorter than the maximum permitted by section 1(1). For example, in 1987, of the 216 persons convicted at the Crown Court of criminal damage who also received an unsuspended term of imprisonment, only nine were sentenced to over two years' imprisonment, and none were sentenced to more than four years' imprisonment: see Home Office, (1987) *Criminal Statistics England and Wales*, Supplementary Tables, Vol. 2: Proceedings in the Crown Court, Table S2.4 (p. 216).

PART IV

JURISDICTION, EVIDENCE AND PROCEDURE

A. JURISDICTION

4.1 As we indicated in paragraph 1.39 above, it has been made very plain to us in our work that computer misuse is a problem of international dimensions. A hacker, with or without dishonest intentions, may for instance sit in London and, through an international telephone system, enter or try to enter a computer in New York, or vice versa. More complex 'chains', involving computer systems in a number of countries before the 'target' computer is accessed, are entirely possible. In order to meet this situation, the general rule that is necessary, in our view, is that English courts should have jurisdiction over computer misuse that either originates from, or is directed against computers located in, this country.

4.2 We have already pointed out, in paragraphs 2.8-2.9 above, that problems of jurisdiction in relation to international fraud, whether or not it is computer-related, would be solved by the adoption of the recommendations in our recent report.[83] In relation to the new offences proposed in this report, we recommend that similar provision should be made to that in clause 4 of the Scottish Law Commission's draft Bill,[84] namely that the courts of this country should have jurisdiction to entertain proceedings for one of those offences if at the time at which the offence was committed either the offender or the computer concerned was located in this country.

4.3 A number of ancillary points should be made. First, in relation to the offence of unauthorised modification of computer material, the general jurisdictional rule should apply not only to the computer in question but also to the material that is modified. Second, we *recommend* that provision should be made for the trial in England and Wales of attempts and incitement to commit computer misuse offences abroad, and of attempts and incitement to commit computer misuse offences here, for the same reasons as were set out in relation to offences of fraud in Parts IV and V of Law Com. No. 180, and subject to the same limitations as are there stated. In particular, the principle of 'double criminality' should apply, so that a conspiracy, attempt or incitement in this country to commit a computer misuse offence wholly abroad would not be prosecutable in this country unless the acts contemplated, if done, would punishable under the law of the country where they were to take place.[85] Thirdly, however, the ulterior intent offence recommended in paragraphs 3.49-3.59 above would not be committed unless the ulterior conduct contemplated would constitute one of a number of specific offences under the law of England and Wales. We think that that is a proper limitation for an English statute, which will not give rise to difficulties in practice.

B. EVIDENCE AND PROCEDURE

4.4 In paragraph 1.10 of W.P. No. 110 we made it clear that our enquiry was concerned only with the substantive law relating to computer misuse, and that evidence and procedure fell outside the scope of that paper. Nevertheless, a number of those commenting on the paper did bring to our attention aspects of evidence, procedure and the law relating to the investigation of offences, and it is therefore right that we should make some comments on the points that have been put to us.

4.5 We do not in this connection make any recommendations for the alteration of the present law. That is first because we have not formally consulted on any of these matters, and therefore cannot know whether the reforms suggested by some would command general acceptance, or may be subject to defects that only become apparent on more extensive scrutiny. Second, however, our review of the representations that have been made to us has in any event led us to conclude that alteration of the law is

---

[83] (1989) Law Com. No. 180, Jurisdiction over Offences of Fraud and Dishonesty with a Foreign Element.

[84] Scot. Law Com. No. 106, p. 32; the recommendation is discussed at p. 23 of the Scottish Law Commission's report.

[85] The considerations of principle leading to this recommendation are the same as those applying in the case of international fraud, and are fully set out in paras. 5.23–5.29 of Law Com. No. 180. We do not think it necessary to repeat them here.

probably not required; and that it is certainly not required with the degree of urgency that would be implied by the inclusion of proposals for reform in this report.

4.6 We now review the more important issues that have been put before us.

1. Section 69(1) of the Police and Criminal Evidence Act 1984 ('PACE')

4.7 This section, in its relevant parts, provides as follows-

"In any proceedings, a statement contained in a document produced by a computer shall not be admissible in evidence of any fact stated therein unless it is shown-

(a) that there are no reasonable grounds for believing that the statement is inaccurate because of improper use of any computer;

(b) that at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents."

4.8 We have received a number of criticisms of the general operation of this section. Those matters do not fall within our present remit, and we have not attempted to assess them. However, some commentators went further and suggested that the terms of the section would create a material difficulty in prosecuting computer misuse offences, in that in such a case, because of the actual or suspected interference with the computer concerned, evidentiary documents would by definition not be able to be vouched for as the section requires. That view was specifically rejected by others whom we consulted, and we do not believe it to be correct.

4.9 We can, we think, deal with this point quite shortly. In any computer misuse case it is likely that oral evidence, whether or not backed by documents, will have to be given to explain the normal working of the computer and the way in which it is alleged to have been interfered with. Here, as in other aspects of the prosecution of computer misuse crimes, it will be essential for computer owners and operators to be able to give full and accurate accounts of operational methods and working practices. None of that evidence will, however, fall within the terms of section 69. If on the other hand computer-produced documents are relied on in such a case, for instance to show the alteration of data or the attempts of a hacker to enter a system, they will be stating facts, so as to fall within the terms of section 69, but those facts will be data *at present* contained within the computer. We see no reason in such a case for exempting the prosecution from the general requirement imposed by section 69 of showing that the computer was, apart from the alleged interference of which evidence will be given, *otherwise* operating properly.

2. Arrest, search and seizure

4.10 We have received some representations that special powers of arrest, search and seizure are required to ensure that outside hackers can be detected and apprehended, bearing in mind that such people tend to operate in the privacy of their own homes, by using telephone connexions, rather than in the more public arena necessarily adopted by more orthodox criminals. Some extensive powers to this effect were included in Miss Nicholson's Private Member's Bill.

4.11 We have already pointed out[86] that even within the confines of the present law there are substantial and effective methods of identifying and apprehending both outside hackers and internal misusers of computers. In addition, if our recommendation is accepted that the 'ulterior intent' hacking offence should carry a maximum penalty of five years' imprisonment,[87] that will be an arrestable offence[88] which, in a case where there is reasonable suspicion that the offence is being committed, will under the

[86] See paras. 2.18–2.22 above.
[87] See para. 3.59 above.
[88] See PACE, section 24(1)(b).

present law attract powers of arrest,[89] entry in order to arrest,[90] and search of the arrested person's premises.[91] These are substantial weapons. To go further, as some have urged, and create powers of search before arrest, even in the case of suspected basic hacking, would be in effect to extend the search provisions of Part II of PACE to cases far different from the serious arrestable offences for which that regime was designed. For such a step to be contemplated there would, in our view, have to be as a minimum requirement very strong evidence of practical necessity, which evidence has not been provided by the, admittedly limited, submissions made to the Commission.

4.12 So far as the forfeiture of hacking equipment is concerned, we pointed out in W.P. No. 110[92] that extensive powers of forfeiture of property used or intended for use in committing offences are already provided by section 69(1) of the Criminal Justice Act 1988, and we consider that those powers are adequate in the case of computer-related offences.

3. Telephone tapping to obtain evidence

4.13 It has been suggested to us that in order properly to monitor the activities of hackers it is desirable that the police should be given powers to apply for warrants to intercept communications on public telecommunications systems, to a much wider extent than is provided by section 2 of the Interception of Communications Act 1985. Provisions to this effect were included in Miss Nicholson's Private Member's Bill. We have pointed out above that extensive surveillance and monitoring is already possible within the confines of the present law, with the co-operation of the owner of the computer system under attack. We doubt whether any extension of that law is necessary from a practical point of view; and are in any event clear that the widest consultation and consideration would be necessary before any extension were made of provisions that have only recently been debated in detail by Parliament.

4. A duty to report computer-related offences

4.14 We set out in Appendix B to W.P. No. 110 the arguments for and against the creation of a duty to disclose incidents of computer misuse that had been discussed by the Scottish Law Commission.[93] We did not invite consultation on this point, considering it to fall outside our terms of reference, but we did receive considerable indications during our work that reluctance to disclose incidents of misuse has caused difficulty to law enforcement agencies. Nonetheless, we see no reason to differ from the conclusion of the Scottish Law Commission that to create a duty to disclose the commission of these particular crimes would be a complete and unjustifiable departure from the general practice of the law. It may not be irrelevant in the English context to add that by section 5(1) of the Criminal Law Act 1967 Parliament substituted a much less far-reaching offence for the old offence of Misprision of Felony, which latter had consisted simply in an omission to report a serious offence to the police.[94]

---

[89] *Ibid.*, s.24(4)–(7).
[90] *Ibid.*, s.17(1)(b).
[91] *Ibid.*, s.32(2)(b).
[92] See n.42 at p. 94 of W.P. No. 110.
[93] See paragraphs 5.8–5.11 of Scot. Law Com. No. 106.
[94] See Smith & Hogan, *Criminal Law*, 6th ed. (1989), pp. 763–764.

PART V

SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS

5.1 In this part of the report we summarise our conclusions and our recommendations for reform of the law.

A. NEW SUBSTANTIVE OFFENCES OF COMPUTER MISUSE

5.2 We recommend that three new offences of computer misuse be created. Those offences should be–

1. Unauthorised access to a computer

The terms in which we consider that this offence should be created are described in paragraphs 3.13–3.39 above. For the reasons given in paragraphs 3.40–3.45 above, the offence should be triable summarily only, and be punishable with a maximum of three months' imprisonment or a fine of up to Level 4 on the standard scale.

2. Unauthorised access to a computer with intent to commit or facilitate the commission of a serious crime

The terms in which we consider that this offence should be created are described in paragraphs 3.49–3.58 above. The offence should be triable either way, and should carry a maximum penalty, on conviction on indictment, of imprisonment for five years (see paragraph 3.59 above).

3. Unauthorised modification of computer material

The terms in which we consider that this offence should be created are described in paragraphs 3.64–3.77 above. The offence should be triable either way, and should carry a maximum penalty, on conviction on indictment, of imprisonment for five years (see paragraph 3.79 above).

B. OTHER MATTERS

5.3 We recommend, in relation to the three new offences, that there should be wide provisions conferring jurisdiction on the courts of England and Wales, similar to those recommended in the case of fraud in our recent report[95] (see paragraphs 4.1–4.3 above).

5.4 We do not, in this report, make any recommendations as to the reform of the law of deception, reserving that matter for further report (see paragraphs 2.2–2.7 above).

5.5. We recommend that use by an authorised user of a computer for an unauthorised purpose should not, in itself, be a criminal offence (see paragraph 3.38 above).

5.6 We make no recommendations as to alterations of the law of evidence or procedure in relation to crimes of computer misuse (see paragraphs 4.4–4.14 above).

(Signed) ROY BELDAM, *Chairman*
TREVOR M. ALDRIDGE
JACK BEATSON*
RICHARD BUXTON
BRENDA HOGGETT

MICHAEL COLLON, *Secretary*
25 September 1989

* The policy adopted in this report was agreed before Mr. Beatson joined the Commission on 3 July 1989.

[95] (1989) Law Com. No. 180. Jurisdiction over Offences of Fraud and Dishonesty with a Foreign Element.

APPENDIX

List of individuals and organisations who commented on Law Commission Working Paper No. 110: "Computer Misuse".

R. C. Abnett
Arthur Young
Association of Chief Police Officers
Audit Commission for Local Authorities in England and Wales
D. I. Bainbridge
Barclays Bank plc
G. P. Boileau
BP International Limited
British Computer Society
British Telecom
P. Bromwich
M. A. Brown
Business Equipment and Information Technology Association
His Hon. Judge Gerald Butler, Q.C.
The Hon. Mr Justice Campbell
Dr S. Castell
Confederation of British Industry
Central Computer Services
Centre for Criminal Justice Studies, University of Leeds
Dr J. C. Chicken
His Hon. Judge Clarkson, Q.C.
Committee of London and Scottish Bankers
The Computer Exchange
Computer Sciences Company
Computer Users Forum
Computing Services Association
Council of Her Majesty's Circuit Judges
Cray Research (UK) Ltd
Criminal Law Reform Group of the Committee of Heads of Polytechnic Law Schools and the Association of Law Teachers
Crown Prosecution Service
M. J. Dalley
Data Protection Registrar
A. F. Davenport (Microplan Businesses Systems)
Deloitte Haskins & Sells
Digital Equipment Ltd (DEC)
Dr T. J Dyson and K. E. Tarn (Nottingham Health Authority)
EDP Auditors' Association (London Chapter)
Electronic Engineering Association
Ford Motor Company Ltd
B. Fothergill (Guardian Royal Exchange Assurance)
General Council of the Bar
Glaxo Export Ltd
J. Goldring
Miss Isabel Gurney
D. R. Harris
Dr M. A. Heather
Home Office

C. R. Hoyle (Bird and Bird)
IBM Computer Users' Association
IBM United Kingdom Ltd
ICC United Kingdom
ICI
International Computers Ltd (ICL)
Information Protection & Management Consultants Group of Hoskyns Group plc
Institute of Chartered Accountants Information Technology Group
Institute of Legal Executives
D. Jackson (University of London Computer Centre)
The Rt Hon. the Lord Jauncey of Tullichettle
The Hon. Mr Justice Jowitt
A. Kelman
D. E. Kershaw
D. N. Laine
Law Society Criminal Law Committee
Dr J. A. Linn (University of Aberdeen Computing Centre)
London Chamber of Commerce
The Rt Hon. the Lord Lowry
Magistrates' Association Legal Committee
Manchester Chamber of Commerce and Industry
The Hon. Mr Justice McCulloch
Metropolitan Police
D. H. Miles-Wilson
National Computer Users Forum
National Computing Centre Ltd
North Eastern Circuit Scrutiny Group
S. Overend
I. M. Paton
P. Pearce
Peat Marwick McLintock
The Hon. Mr Justice Phillips
A. L. Phillips
Police Federation of England and Wales
Police Superintendents' Association of England and Wales
Prudential Corporation plc
D. Radcliffe
Dr C. Reynolds
D. Roberts
The Hon. Mr Justice Rose
A. Sandman
Securities and Investments Board (SIB)
Serious Fraud Office
D. E. Sewell
Shell UK Information and Computing Services
P. Simpson
Society for Computers and Law
Society of Public Teachers of Law Criminal Law Sub-Committee
P. Sommer
Standard Chartered Bank
The Rt Hon. Lord Justice Staughton

The Hon. Mr Justice Steyn
I. Thomas
TSB Group plc
G. R. Turete
Universities and Research Councils Computer Board
M. Wasik
WBK International Ltd
Derek Wheatley, Q.C. (Lloyds Bank)

Printed in the United Kingdom for Her Majesty's Stationery Office
Dd 0503693 10/89 C20 3382 4235 78638 Job No. 895027.1C

HMSO publications are available from:

HMSO Publications Centre
(Mail and telephone orders only)
PO Box 276, London SW8 5DT
Telephone orders 01-873 9090
General enquiries 01-873 0011
(queuing system in operation for both numbers)

HMSO Bookshops
49 High Holborn, London, WC1V 6HB 01-873 0011 (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

ISBN 0 10 108192 8