SCOTTISH LAW COMMISSION
(Scot Law Com No 106)

Report on Computer Crime

Presented to Parliament by the Lord Advocate
by Command of Her Majesty
July 1987

EDINBURGH
HER MAJESTY'S STATIONERY OFFICE
£5.00 net

Cm 174

The Scottish Law Commission was set up by section 2 of the Law Commissions Act 1965 for the purpose of promoting the reform of the law of Scotland. The Commissioners are:

The Honourable Lord Maxwell, *Chairman*
Dr E M Clive,
Professor P N Love, CBE,
Mr J Murray, QC,
Sheriff C G B Nicholson, QC.

The Secretary of the Commission is Mr R Eadie. Its offices are at 140 Causewayside, Edinburgh EH9 1PR.

ISBN 0 10 101742 1

Scottish Law Commission

Computer Crime

To: The Right Honourable the Lord Cameron of Lochbroom, QC,
Her Majesty's Advocate

In pursuance of our duty under section 3(1)(*a*) of the Law Commissions Act 1965 to receive and consider any proposals for the reform of the law which may be made to us, we have examined a proposal relating to the subject of computer crime. We have the honour to submit our report.

(*Signed*) PETER MAXWELL, *Chairman*
E M CLIVE
PHILIP N LOVE
JOHN MURRAY
GORDON NICHOLSON

R EADIE, *Secretary*
22 June 1987

174—B

Contents

Part I Introduction

1.1 On 13 July 1984 we received from the Law Society of Scotland, under section 3(1)(*a*) of the Law Commissions Act 1965, a proposal in the following terms:

> 'to consider the applicability and effectiveness of the criminal law of Scotland in relation to the use and abuse of computers, computer systems and other data storing, data processing and telecommunications systems with a view to proposing appropriate reform of the law where that may appear to be necessary.'

1.2 At the time when that proposal was received by us, so-called computer crime was the subject of intense and frequent media interest. Horror stories abounded concerning vast commercial frauds being perpetrated, allegedly by the application of electronic wizardry; and fears were raised that outsiders, known as hackers, could with relative ease break into computer networks and cause untold loss and damage. None of this interest has abated in the intervening years, and as recently as the end of 1986 a large company of insurance brokers expressed the view that 'computer assisted fraud and theft will probably cost UK companies £40 million this year'.[1]

1.3 Recognising that the term 'computer crime'[2] itself begs the question as to what computer-related activities already are, or in future should be, crimes, we sought to determine the scale and nature of any perceived problems, to assess the applicability of existing criminal law, and to examine the possibilities for reform. In March 1986 we published our provisional conclusions and proposals for reform in a consultative memorandum[3] entitled 'Computer Crime' (hereafter referred to as 'the Memorandum'). The Memorandum was widely circulated for comment, and attracted a great deal of interest. We have received comments and suggestions from many individuals and organisations both in Scotland and elsewhere, and we are most grateful to all of them for the help that they have given us. A full list of those consultees who commented on the Memorandum will be found at Appendix B to this Report.

1.4 Our consultation revealed a considerable difference of opinion among consultees as to the shape that any reform should take. Indeed, some consultees suggested that there is no need for any reform at all, on the basis that existing Scots criminal law has sufficient inherent flexibility to enable it to accommodate contemporary technological wrongdoing without difficulty. Among those who favoured some reform there were broadly two schools of thought. One school of thought expressed a preference for a cautious and limited approach to reform and, while accepting that there is probably a case for creating an offence to penalise the unauthorised obtaining of access to computers, concluded that any further reforms should await a full examination of all the problems that may be found in, for example, the law of theft and the law of intellectual property. This school of thought was of the view that there can be no justification for creating new offences solely in relation to computers when any underlying difficulties in the law arise equally in relation to many other activities as well. The other school of thought was of the view that, since computers now play such a central role in all aspects of day-to-day life, it is essential to have a clear and comprehensive statement of what the law does and does not permit in relation to

1. 'Computer Security in Practice', a Report by Hogg Robinson Limited, Risk Management Services Division, 1986.
2. The term has been criticised by one writer as being ungrammatical, inelegant, and symptomatic of fundamental confusion (Tapper, ' "Computer Crime": Scotch Mist?' [1987] Crim LR 4). While acknowledging these criticisms we, like Tapper himself, have used and will continue to use the term as a convenient shorthand.
3. Consultative Memorandum No 68.

174—C

their use, even if that means singling them out for special legislative attention or devising offences which may to some extent duplicate existing offences of general application.

1.5 The wide divergence of views outlined above is scarcely surprising given that the widespread use of computer technology is still a comparatively recent phenomenon, that computer use and misuse involve many different areas of the law, both criminal and civil, and that some of the activities which are possible subjects for reform raise sharp and difficult questions about whether the interests involved should receive the protection of the criminal law at all. In these circumstances we have decided that it would be appropriate in this Report to examine the scope for wide-ranging reform though, as will be seen, our own preference falls short of a completely comprehensive computer crime statute of the kind favoured by some of our consultees.

1.6 In Part II of the Report we describe the activities which appear to be possible candidates for reform. In Part III we examine in greater detail the arguments for and against comprehensive reform. In Part IV we deal with those activities which we regard as being appropriate for reform, and suggest how new offences might be framed. In Part V we consider a number of ancillary matters. Finally, in Part VI we set out a summary of our recommendations, and in Appendix A we set out a draft Bill to give legislative effect to those recommendations.

Part II Forms of computer misuse

Categories of misuse

2.1 In the Memorandum we identified eight different categories of computer misuse, namely:

(1) erasure or falsification of data or programs so as to obtain a pecuniary or other advantage

(2) obtaining unauthorised access to a computer

(3) eavesdropping on a computer

(4) taking of information without physical removal

(5) unauthorised borrowing of computer discs or tapes

(6) making unauthorised use of computer time or facilities

(7) malicious or reckless corruption or erasure of data or programs

(8) denial of access to authorised users.

2.2 Several of these categories of misuse overlap each other to a greater or lesser extent, but we thought that, for the purposes of the Memorandum, it would be helpful to examine the adequacy of existing law and the scope for reform by reference to these fairly narrowly defined activities rather than by using broader classifications such as offences for gain, offences against property, and so on. Moreover, our categorisation was deliberately expressed in neutral terms so as not to convey any impression, at least initially, that the activities in question are at present, or should in future become, offences.

2.3 We invited consultees to let us know whether we had correctly and sufficiently identified the main categories of computer misuse. Although some consultees drew our attention to particular examples of misuse which we had not previously been aware of, all seem to have been satisfied that our general classification was accurate and comprehensive. In what follows, therefore, we shall continue to refer to the categories of misuse set out above. Initially it will be helpful to describe briefly what may be involved in each of these categories, to explain how and when they may overlap with each other, and to summarise our views on the extent to which they may be affected by existing law.

(1) Erasure or falsification of data or programs so as to obtain a pecuniary or other advantage

2.4 In this category we are primarily concerned with those cases where, by manipulating data or programs, a person obtains a financial or other advantage to which he is not entitled. In essence what is involved here is similar to, and indeed may be the same as, traditional fraud or theft. As with the traditional crimes this activity will most commonly be engaged in by an employee whose normal duties require him to input or process data for a legitimate purpose, and who abuses that position of trust for his own benefit.

2.5 In the Memorandum we tentatively expressed the view that in Scotland such activities, even where they involved computers, would be adequately dealt with by the common law crimes of fraud or, in some cases, theft. Referring to the classic definition of fraud given by Macdonald,[1] we did question whether it could be said

1. Criminal Law of Scotland (5th edn), 52: fraud 'involves a false pretence made dishonestly in order to bring about some definite practical result'.

that there had been a false pretence if no other human being was involved and the pretence was made solely to a computer. However, we concluded that the concept of 'false pretence' is probably sufficiently flexible to cope even with that sort of case. In this respect, we noted, Scots law may have an advantage over English law which, in the Theft Act 1968 and elsewhere, uses the concept of 'deception' which, it has been held,[1] requires a human mind to be deceived. Under both systems of law, of course, there will be many cases involving computers where it will nonetheless be perfectly possible to say that a false pretence has been made to a person, or that a person has been deceived.[2] In such cases what we have in mind is that a person will act to his, or his employer's, or some other person's detriment on the basis of false data that have been introduced into a computer record.

2.6 Many consultees who commented on this matter confirmed our provisional view that the Scots law of fraud, or in some cases theft, will be sufficiently flexible to accommodate itself to activities involving computers. Some consultees expressed a nagging doubt about whether the concept of 'false pretence' will always be appropriate where only computers are involved; and other consultees expressed the view that, even if Scots law is technically capable of dealing with these sorts of activities, it would nonetheless be desirable in the interests of clarity and certainty to formulate a computer-specific fraud offence to supplement the common law. We ourselves remain fairly satisfied that the common law crimes of fraud or theft will cover cases where these activities are perpetrated by the use of computers alone but, even if that is so, there remains the question whether such activities should nonetheless be made the subject of a new computer-specific offence. We return to that question later.[3]

(2) Obtaining unauthorised access to a computer

2.7 This activity, at least in the form known popularly as 'hacking', is probably the one that has attracted the greatest media attention in recent years. In the sense of hacking it involves an unauthorised person making contact with a remote computer or computer network, probably through the medium of a public telecommunication system, and thereafter gaining access to stored data or programs, possibly by overcoming security devices such as codewords, identification numbers and the like. It is to be noted, however, that the obtaining of unauthorised access to a computer can also occur much more directly, for example when an employee who is not authorised to use a computer, or who is not authorised to have access to certain parts of a computer's stored data, simply uses his employer's computer without authority and for an unauthorised purpose. This kind of activity is not strictly hacking since it does not involve long range communication, but it may be potentially more dangerous since an employee, as opposed to an outsider who may have to rely on mere guesswork, may find it easier to discover the passwords that will give him access to a computer's data and also the means of altering or corrupting that data.

2.8 It seems reasonably clear that many who indulge in the activity of hacking, in the sense of obtaining remote access, are merely curious to test their electronic and technological skills, and have no more nefarious motive in mind. However, it is equally clear that, whether by design or not, the activity of hacking may give access to secret or confidential information which the hacker is not entitled to see, and which the unscrupulous person may use to his own advantage. Moreover, although there is little evidence that remote hackers have gone on to perpetrate major frauds or thefts, it may be technically possible, subject to the security devices in use, for a hacker not merely to view stored data but in fact to manipulate that data in various ways. Additionally, and depending on the nature of the computer system being accessed, the effect of hacking may be to give the hacker services for which he avoids payment while at the same time passing on apparent liability for such payments to a wholly innocent third party. This, we understand, occurred in a recent case in England[4] where the defendants used other people's passwords to gain access to, and

1. *R* v *Moritz*, unreported, described in the Memorandum, para 3.7. It has been drawn to our attention that the particular problem which arose in that case has probably been cured by section 12(5) of the Finance Act 1985 which amended section 39 of the VAT Act 1983 so as to define 'intend to deceive' in terms of an 'intent to secure that a machine will respond to the document as if it were a true document'.
2. See for example *R* v *Thompson* [1984] 3 All ER 565.
3. Para 3.16 *et seq* below.
4. *R* v *Schifreen & Gold*, unreported.

to make use of, the Prestel network and other British Telecom systems with the result that the true users of the passwords were debited with the amount of use involved.

2.9 In the Memorandum we expressed the view that in Scotland—and assuming that no other activity is involved which is itself a crime—it is not at present contrary to law to obtain unauthorised access to a computer whether by hacking or in any other way. This view attracted no dissent from consultees. We went on to note, however, that the position may be different under English law where, in the case mentioned in the previous paragraph, section 1 of the Forgery and Counterfeiting Act 1981 (which does not apply in Scotland) was used successfully as the basis for the prosecution. However, this case is presently under appeal.

(3) Eavesdropping on a computer

2.10 This activity involves the use of what may be relatively inexpensive equipment to pick up from a distance the radiation emissions from a computer in use so as to display on the eavesdropper's screen the images which are simultaneously being displayed on the legitimate user's VDU screen. This is in fact a form of espionage which is comparable to reading a private document with the aid of a telescope or listening in to a private conversation with the aid of a concealed microphone and transmitter. The practical feature of electronic eavesdropping on a computer is that the eavesdropper cannot control the functions of the computer and in particular cannot determine what will be displayed on the computer's VDU screen at any given moment. This is in contrast to a person who gains unauthorised access to a computer and who may, subject to the existence and effectiveness of any security devices, be able to call up data and to manipulate data or programs at will.

2.11 Our view is that eavesdropping of the sort described, if not accompanied by any other activity such as damage to property or the causing of fear and alarm to others, is not presently a crime in Scotland. None of our consultees disagreed with that view.

(4) Taking of information without physical removal

2.12 In the Memorandum we identified this as a distinct form of computer misuse although strictly it is an activity which need not have anything at all to do with computers. The point is, however, that, as computerised data storage has become more and more common, the sheer volume of information kept in computers is now such that computers must be a prime target for those who seek, without authority, to obtain information which they would not otherwise be permitted to see. Moreover, such information may often be highly confidential and of considerble commercial value. In some instances it may even be information with a high Government security classification.

2.13 If information is stored on a physical medium, such as a piece of paper, a person who removes that piece of paper or whatever may be guilty of theft.[1] In such a case, however, he will be guilty of theft of the physical thing, namely the paper, and not of the information contained on it: though the nature and importance of the information may have a bearing on any sentence that is passed. If, however, information is taken without any physical removal—simply by reading and memorising, or by photographing, or by copying in some other way—there is, in our view, no crime according to the law of Scotland.[2] In summary, the explanation for this is two-fold. First, the law does not as a general rule recognise any right of property in information; and that which is not property cannot be the object of theft. Second, if information is taken without removal of the medium on which it is recorded, the 'owner' of the information has not thereby been deprived of the information: it is still available to him to use as he likes, and all that he has lost is its exclusivity or privacy.

2.14 None of our consultees disagreed with our assessment of the existing law in relation to information. Moreover, many agreed with the provisional conclusion which we expressed in the Memorandum, namely that no attempt should be made to solve any problems relating to the taking of information stored in computers without first having a wide-ranging review of the law of theft and the whole law

1. But see para 2.15 *et seq* below.
2. We understand that the position is the same under English law: see the Memorandum para 3.31 *et seq*.

relating to intellectual property and trade secrets. Several consultees, however, disagreed, arguing that the unauthorised taking of information is now a major commercial and industrial problem which should, if possible, be tackled in relation to computer data, and as a matter of urgency. We shall return in more detail to these opposing arguments in Part III of this Report.

(5) Unauthorised borrowing of computer discs or tapes

2.15 Recognising the difficulties inherent in the bare taking of information, as noted above, we went on in the Memorandum to consider the case where the actual medium on which data, or a computer program, is recorded is itself taken. The problem here is that, while an outright and permanent taking will undoubtedly be theft, a merely temporary taking followed by the return of the article concerned may not. In the context of computers, of course, a merely temporary removal of an article such as a disc or a tape is a perfectly foreseeable activity since any data or programs stored therein are capable of being copied at great speed prior to the return of the article concerned.

2.16 In the Memorandum we reviewed the law relative to the temporary appropriation of articles,[1] and in particular we examined a number of recent cases[2] which were concerned with the question whether there can be theft in the absence of an intention permanently to deprive the owner of the thing in question. These recent cases lend support to the view that there need not always be such an intention, but it is extremely difficult to extract from the cases a clear indication of the principles to be applied. In particular it is not clear to us whether they provide authority for the view that the temporary taking of something like a computer disc, possibly to copy its contents, can be regarded as theft. The judgments in the recent cases that we examined speak of an intention permanently to deprive not being necessary 'in certain exceptional cases'[3] or where the taking is 'aimed at achieving a nefarious purpose'.[4] It is, we think, impossible to say whether the reading or copying of a computer disc would be regarded as either exceptional or nefarious. In the Memorandum we expressed uncertainty as to whether or not the Scots law of theft would apply to the temporary taking for such a purpose of an article like a disc, and we remain uncertain on that point. In general our uncertainty regarding this aspect of the law of theft was shared by consultees.

2.17 In addition to the issue of permanent deprivation we also examined in the Memorandum the few Scottish cases[5] which deal with the concept of *furtum usus*, or theft of use. While not expressly conceding that *furtum usus* is a crime according to the law of Scotland, these cases give some support for the view that it is a crime to take a thing (in the leading case,[6] a car) clandestinely and without authority, and thereafter to use it. While there appear to have been no modern cases on this topic,[7] we expressed the view in the Memorandum that this line of authority might be capable of development to cover the temporary appropriation, and subsequent copying or reading, of discs or tapes. However, one of our consultees pointed out to us that there might be difficulty in saying that, for example, a disc is being *used* when its existing contents are merely read or copied. A disc exists primarily to receive and store data, and any subsequent reading of that data is really consequential to the primary use of the disc rather than constituting a use in itself. We can see some force in that argument, and we are accordingly now less than certain that the line of authority mentioned above would be appropriate for the kinds of activities presently being considered.

(6) Making unauthorised use of computer time or facilities

2.18 Obviously this is an activity which could in certain circumstances be a consequence of obtaining unauthorised access to a computer, and in that respect these two

1. The Memorandum para 3.34 *et seq*.
2. *Herron* v *Best* 1976 SLT (Sh Ct) 80; *Milne* v *Tudhope* 1981 JC 53; *Kidston* v *Annan* 1984 SCCR 20; *Sandlan* v *HMA* 1983 SCCR 71.
3. *Milne* v *Tudhope* above per LJC Wheatley at 57.
4. *Sandlan* v *HMA* above per Lord Stewart at 83.
5. In particular *Strathern* v *Seaforth* 1926 JC 100: see the Memorandum para 3.50 *et seq*.
6. *Strathern* v *Seaforth* above.
7. Probably because the most notorious form of *furtum usus*, namely joy-riding in cars, has for many years been the subject of an express offence in the Road Traffic Acts.

activities overlap to a certain extent. However, we listed this as a separate category in the Memorandum in order to deal specifically with the case where a person uses a computer not so much in order to gain access to its stored data but rather as a highly sophisticated tool which, by virtue of the way in which it has been programmed, can perform complex tasks or calculations. A person who makes use of a computer for such purposes will, we suspect, normally be an insider who is already authorised to use the computer for certain legitimate purposes, but it is conceivable that a person might make use of a computer in this way having first gained unauthorised access in order to do so. The purposes for which a computer might be so used could be very trivial, such as the calculation of a series of permutations for use in the person's football pools coupon; or could be much more serious involving, perhaps, the use of expensive and sophisticated programs for the purpose of private, and potentially competitive, research and development.

2.19 Apart perhaps from a somewhat inappropriate charge of theft of electricity, we doubt whether such activity would be contrary to the criminal law. In particular we doubt whether it would be a 'theft of use' as described above, principally because there would be no removal of the computer, or computer system, being used.[1] On the other hand, as we pointed out in the Memorandum, this kind of activity would, if perpetrated by an insider, be subject to appropriate forms of internal disciplinary measures and sanctions at the hands of an employer; and, if perpetrated by an outsider, or possibly an insider who did not have authority to use the computer at all, could be subject to the sanction of an unauthorised access offence, if such were to be created. Consultees were in general agreement with our assessment of the law on this matter.

(7) Malicious or reckless corruption or erasure of data or programs

2.20 This is an activity which could be relatively trivial but which equally could have very grave consequences. These consequences could be purely financial, albeit of considerable proportions, but, as was pointed out to us by members of the British Computer Society, could equally affect human life or the state of the environment. Apart from purely commercial uses computers are now widely used for activities as diverse as the operation of life support systems in hospitals and the monitoring and control of nuclear power stations. Obviously any deliberately induced malfunction in such computers could have appalling consequences.

2.21 It is in our view highly probable that the malicious or reckless corruption or erasure of data or programs will in Scotland constitute either the common law crime of malicious mischief or the statutory offence of vandalism.[2] This was the view which we expressed in the Memorandum, and it was confirmed on consultation. We note, incidentally, that a similar view has recently been taken in England where, in the case of *Cox* v *Riley*,[3] the Divisional Court upheld a conviction under section 1 of the Criminal Damage Act 1971 in circumstances where a person had erased a computer program from a plastic circuit card of a computerised saw so as to render the saw inoperable. However, it seems probable that the common law crime of malicious mischief does not extend to damage which is caused recklessly (as opposed to deliberately); and the statutory offence of vandalism (which expressly includes reckless conduct) may be tried only summarily. This means that in Scotland recklessly caused damage to programs or data, if substantial in extent, can probably not be prosecuted on indictment.

(8) Denial of access to authorised users

2.22 In the Memorandum we described this category of computer misuse as 'rather speculative' mainly because we were uncertain whether there is in fact any means of denying access to authorised users which would not in any event amount either to a known crime such as vandalism or at least to one of the other forms of misuse discussed elsewhere. We have heard nothing from our consultees to suggest that this topic merits any further consideration on its own account.

1. It might of course be different if the computer in question were a small portable one, and the operator took it home with him to use there. In that event the principles set out in *Strathern* v *Seaforth* above might apply. See also *Murray* v *Robertson* 1927 JC 1.
2. Criminal Justice (Scotland) Act 1980 s. 78.
3. (1986) 83 Cr App R 54.

Part III The case for reform

Is there a need for any reform?

3.1 Before considering the details of any possible reforms, or indeed the overall scale of any reform, it is desirable to ponder the above question, and to consider whether any reform of the law is required at all. This involves not only a consideration of the possible deficiencies in existing law which were noted in the previous Part of this Report but also a consideration of the available evidence about the scale and seriousness of so-called computer crime.

3.2 It is, we think, impossible to form any definite conclusion as to the present scale of computer crime. As noted in the Introduction to this Report,[1] a large company of insurance brokers has recently expressed the view that 'computer assisted fraud and theft will probably cost UK companies £40 million this year', and in January 1987 the Confederation of British Industry was reported[2] as endorsing the view that computer fraud is costing at least £30 million per year. By contrast, as we noted in the Memorandum,[3] the survey of computer fraud carried out in 1985 by the Audit Commission for Local Authorities in England and Wales gave no support to such high figures of loss.

3.3 The trouble is that, without having full details of all the cases involved, it is impossible to say whether particular incidents were of a kind that could not have occurred but for the intervention of a computer, or were instead of a kind that could have equally well occurred even if more traditional methods of accounting or whatever had been in use. In particular it is impossible to say whether the advent of mass computerisation has of itself brought about a substantial increase in the volume of corporate fraud and theft compared with what might have occurred anyway even if the computer had never been invented; though it does seem likely that the nature of computer technology, for example its ability to secure the movement of very large amounts of money instantaneously by electronic funds transfer, will have increased the risks to some extent. Of special relevance to the present Report, it is, we think, impossible to say with certainty whether any increase that there may be in computer-related crimes, or other undesired computer-related activities, is attributable to deficiencies in our present criminal law.

3.4 In short, we doubt whether there is at present sufficient hard evidence as to the scale and consequences of computer misuse which would of itself suggest an impending crisis of a kind that demanded prompt legislative action. On the other hand the absence of conclusive evidence does not mean that there are not problems requiring solution, and indeed many of our consultees have suggested to us that this is indeed the case.

3.5 It seems to us that, while one must be cautious not to over-dramatise the scale and extent of computer misuse at present, nonetheless the very nature of computers, and the multifarious uses to which they are put, do require that serious consideration should be given to the role of the criminal law in controlling their use and, particularly, their misuse. If there are deficiencies in the law which could be exploited to someone's advantage (and someone else's disadvantage), it may be wise to take appropriate steps now rather than wait for absolute confirmation of loss figures like those mentioned in

1. Para 1.2.
2. The Times 19 January 1987.
3. Para 2.61 *et seq.*

paragraph 3.2 above. Moreover, although for understandable reasons the commercial world seems to be primarily interested in incidents which can be categorised as fraud or theft, and which can therefore be measured in terms of quantifiable losses, there are, as we have seen, other forms of computer misuse, such as hacking, or tampering with data or programs, which may not produce such measurable losses but which may nonetheless be regarded as undesirable if only because of the potential loss and damage which they could cause.

3.6 In the Memorandum we came to the provisional conclusion that at least the activity of obtaining unauthorised access to a computer should become an offence. We reached that conclusion for several reasons. First, the nature of computer technology is such that opportunities now exist for gaining access to private data which never existed before, at least probably without having to break into a building or an office to do so. Second, because so much corporate and other data is now kept on computer, the unauthorised person who obtains access to a computer can find in one place vast amounts of information which previously might have been stored in a multiplicity of different locations. Third, although our law does not recognise any general concept of privacy, it does recognise certain circumstances in which unauthorised persons should not be permitted with impunity to pry into another's affairs. That is presumably why, among other reasons, the Data Protection Act 1984 imposes on certain data holders a duty to keep data secure. Deliberate hacking into another's computer is in our view an activity of that kind, and we consider that there is a clear public interest in seeking to prevent it. Fourth, quite apart from the fact that hacking may achieve unauthorised access to information, it may also be the prelude to other activities such as fraud or theft, or the corruption of data or programs. An offence which may serve to prevent these consequential activities seems to us to be worthy of serious consideration.

3.7 Taking all of these considerations into account we remain of the view that the obtaining of unauthorised access to a computer should become an offence. This view was in any event widely supported on consultation. We accordingly **recommend**:

(1) Provision should be made for it to be an offence to obtain unauthorised access to a computer.

(Paragraphs 3.6–3.7; clause 1(1), (2))

3.8 In Part IV of this Report we shall consider in greater detail how such an offence might best be expressed. For the moment we turn to the more general question: accepting that it should be made an offence to obtain unathorised access to a computer, is there a need for any further reform of the law?

The scope of any reform

3.9 A significant characteristic of obtaining unauthorised access to a computer, if that were to become an offence, is that it is an activity which, by its very nature, is related solely to computers. By contrast some of the other activities that we considered in Part II of this Report do not have that characteristic. Computer-assisted fraud or theft are simply particular manifestations of a much wider activity for which the criminal law already caters in a general way. Similarly the corruption of data or programs is simply an example of causing damage to property against which there is a prohibition in the general criminal law. The unauthorised acquisition of information (including the special problem of the temporary taking of articles used for data storage) may not be dealt with by the existing law but is not an activity which is specific to computers since information may be acquired from a multiplicity of sources. On the other hand, an unauthorised access offence could strike at some cases of information taking where that was the object of obtaining the unauthorised access. The unauthorised use of computer facilities is arguably computer-specific, but it is equally arguable that it is simply a particular example of making unauthorised use of another's property.

3.10 In the light of considerations such as these there is a school of thought, reflected on consultation, which takes the view that, in respect of computer misuse, any reform

of the law should be limited to the minimum that is required to deal with problems that exist solely in relation to computers. Any problems that affect the wider application of the law should not be tackled solely in respect of computers but should, if indeed they require tackling at all, be dealt with as part of a comprehensive review of, for example, the law of theft or the law relating to intellectual property. In particular, according to this school of thought, if existing law is able, or is likely to be able, to deal with specific forms of computer misuse, it would be unnecessary and wrong to draft new offences directed at computer misuse in the supposed interests of clarity or the avoidance of doubt.

3.11 There is, by contrast, another school of thought, also reflected on consultation, which believes that there is a strong case for adopting a much more comprehensive approach to reform even though that may mean tackling some problems solely in relation to computers. Each of these schools of thought attracted adherents from among our consultees; and it may be worth noting that the supporters of each school were not drawn solely from a particular professional or business background. Each group contained a fair cross section of our consultees. Standing this marked difference of approach it is desirable that the opposing arguments should be considered in some detail.

3.12 Before doing so, we should mention a sort of half-way approach that has been suggested in some articles and other writings on the topic of computer crime. That approach rejects the creation of wholly new offences (except where they are absolutely necessary) but is prepared to contemplate the widening of existing general offences, by for example the amendment of definitions or conditions, so as to make these existing offences more appropriate for incidents of computer misuse.[1] In our view this is an approach which may offer advantages when one is dealing with existing offences which are already expressed in statutory or codified form since the expression of these offences, or of any associated definitions, can readily and visibly be amended as required. Where, as in Scotland, the relevant existing offences, such as fraud or theft, are common law offences, and therefore not the subject of precise statutory definition, it would in our opinion be difficult, if not impossible, to adopt this approach. Accordingly, so far as Scotland is concerned, the choice appears to lie between the two approaches that have already been briefly described. We now turn to consider them in more detail.

The case for minimal reform

3.13 Some of the arguments for a limited approach to reform are general in character, while others relate more specifically to the particular reforms that might be contemplated were a more comprehensive approach to be followed. Inevitably some of the arguments overlap or merge into each other. Subject to that they are as follows:

(1) The creation of new offences should always be approached with caution. They should be created only where a clear defect in existing law exposes to risk of harm an interest, public or private, which merits the protection of the criminal law. With the possible exception of the obtaining of unauthorised access to a computer, none of the other activities which have been identified as probably not being adequately covered by existing law satisfy these criteria. This is particularly so since it appears that in many instances incidents of computer misuse occur largely or wholly as a result of a failure to take reasonable steps to protect the data or computer systems involved.[2]

1. This approach has been adopted in several countries, for example West Germany where the definition of 'fraud' in the Penal Code is to be enlarged to include 'computer fraud'.
2. Numerous commentators have drawn attention to the very low priority given to security by some computer users. For example, Hogg Robinson Ltd published in a report, 'Computer Security in Practice' (1986), the findings of computer risk management auditors from more than 50 company surveys carried out during the previous two years. These revealed an extremely low level of computer security with password security in particular showing considerable weakness. In one case the password of the chairman of a large company was 'chairman', and it had not been changed for five years.

(2) It is questionable whether the unauthorised 'taking' of information should ever be an offence. Limited protection is in any event given to certain kinds of information under copyright legislation. Furthermore, it is undesirable and contrary to the public interest that there should be any recognition of proprietorial rights in information: information is too valuable a commodity for the property in it to vest exclusively in a single individual. Even if that general view were not to find favour, it would be wrong, and possibly dangerous, to contemplate making the taking of information an offence, even in limited circumstances, without first carrying out a full analysis of what is involved in the concept of 'information', and a detailed examination of the whole law of intellectual property.

(3) In relation to the particular problem concerning the temporary taking of objects such as tapes or discs, without an intention permanently to deprive the owner of them, it is recognised that the law of theft is at best unclear, and possibly even inadequate. However, this is a problem which arises equally in relation to any article which is taken on a temporary basis. There is no special feature in computer-related articles which would justify a new offence while leaving the general law of theft unchanged in all other respects. It may be that the general law of theft is in need of review, but that is a separate exercise in itself which cannot be undertaken in the course of a different exercise devoted to computer crime.

(4) The problem of eavesdropping on a computer[1] while it is being operated is in a similar position. This is part of a much wider problem of surveillance and espionage and, if it is to be tackled at all, should be tackled on that much wider front. Once again there is no special feature about the computer-related activity which would justify specific reform. Indeed it is arguable that eavesdropping on a computer is not a major problem in any event since the eavesdropper cannot control what he sees but is entirely dependent on the chance that the authorised operator may display on screen something of interest.

(5) It is recognised that the unauthorised use of a computer's facilities, that is to say using a computer as a sophisticated tool for one's own purposes, is an activity which of itself is computer-specific. However, it is no different in quality from any other unauthorised use of somebody else's property. Accepting that our law may not recognise 'theft of use', at least in the absence of any removal of the thing in question, one may ask why it should be a crime for my neighbour to come into my house and, without authority, use my computer, but not be a crime for him to come into my workshop and use my lathe or my power saw. Once again there is nothing special about computers, as distinct from other kinds of property, which would justify a selective reform of the law to deal solely with computers. Quite apart from these considerations there is a further reason for not making this activity a computer-specific offence. By its nature the unauthorised use of the computer's facilities will normally be an activity that is indulged in by employees who already have some degree of permitted access to a computer. They will be subject to internal disciplinary controls which will normally, it is thought, be sufficient both for purposes of deterrence and for purposes of punishment. In the event that a wholly unauthorised person made use of a computer's facilities, he would first have to gain access to the computer. If that unauthorised obtaining of access were itself to be an offence, that would be sufficient without going on to make the subsequent use of the computer an offence as well.

(6) So far as activities amounting to fraud, theft or damage to property are concerned, they are adequately covered by existing law, and it is therefore unnecessary, and would in fact be wrong, to create new offences which would merely duplicate that existing law. Such a course would be likely to be confusing for prosecutors, particularly if the penalties for the new statutory offences were to be different from those for the existing common law crimes such as fraud or theft.

1. We have explained what we mean by this in para 2.10 above.

On the basis of all these arguments it would follow that the only new offence which should be created on this approach is one dealing with the obtaining of unauthorised access to a computer.

The case for wider reform

3.14 Subject to the same qualifications as were expressed at the beginning of the previous paragraph, the arguments in favour of wider reform are as follows:

(1) It is recognised that there must always be a cautious approach to the creation of new offences. However, the particular problems posed by computers, and the possibilities for misuse affecting not just private interests but wider public interests as well, are thought to justify being as comprehensive as possible in one's approach to reform. The scale of computer use in this country is now such that scarcely any aspect of private or public affairs is untouched by computers and some positive regulation of their use and misuse by the criminal law is in the general public interest. Moreover, there is at present a considerable degree of uncertainty about what the criminal law does and does not permit: bearing in mind that the proposal put to this Commission[1] required it to consider not merely the applicability of existing law but also its effectiveness, it is desirable that this uncertainty should be removed so far as possible.

(2) Largely for the reasons given in paragraph 3.13(2) above, it is agreed that it is probably undesirable to confer any proprietary status on information, and that, even if that were to be contemplated, it should not be attempted without the full-scale examination of the subject suggested in that paragraph. However, the advent of widespread computerisation has brought with it new features which did not exist in pre-computer days. First, vast amounts of information can be stored in a tiny physical space (in the case of a hard disc, for example, in a space no larger than a paperback book), and all or any of that information can be accessed instantly at the touch of a key. Second, the information so stored will frequently be of a highly confidential or sensitive nature being, for example, anything from personal staff records to corporate trading returns. Third, since computers now perform with ease many tasks which previously would have required the employment of many experts, the information stored in a computer may contain details of future product designs, corporate strategy, or financial and statistical analysis, all calculated by the computer itself. Fourth—and of particular importance—the nature of computer technology is such that huge amounts of that information can be copied to disc or printed out on paper within a very short time. (Many consultees expressed concern at the ease with which highly confidential information can be extracted from a computer.) For these reasons some attempt should be made to address the problem of the unauthorised 'taking' of computer-stored information.

(3) If a satisfactory way can be found to make the taking of information an offence, it may be that the particular problem concerning the temporary appropriation of data storage articles will diminish in importance. However, if that were not to be possible, those who favour the wider approach would wish to address this problem in relation to computers even though to do so would be to ignore, at least for the present, the wider problem in the general law of theft. The reason for this follows from the arguments presented in (2) above. If these arguments are sound, one can see the temporary removal of tapes or discs simply as a particular example of the abstraction of information, and it really should make no difference whether, for example, information is obtained directly from a computer or indirectly by removing a disc, reading or copying it elsewhere, and then replacing it. In both cases the special nature of computers, noted above, justifies the creation of an appropriate offence or offences.

(4) The case for an offence to deal with eavesdropping on a computer is recognised as being weaker in that this activity gives no opportunity to control, alter or select the data that is being displayed. However, it is nonetheless an activity

1. See para 1.1 above.

which can achieve the acquisition of secret or confidential information by clandestine means and, as such, is an activity which should be prohibited by law. Once again the widespread nature of computer use justifies the creation of an appropriate offence even though other forms of commercial or industrial espionage may for the time being remain outwith the criminal law.

(5) While some supporters of a wider approach to reform consider that the unauthorised use of a computer's facilities should be made an offence, most of those who commented on the Memorandum were prepared to concede that, for the reasons given in paragraph 3.13(5) above, this should not be done.

(6) So far as fraud, theft, and damage to property are concerned, it has been generally accepted that they are probably covered adequately by the existing law. However, several consultees suggested that it would be in the interests of clarity and certainty, and might increase the deterrent effect of the law, if these activities were to be made the subject of specific computer-related offences. That would also mean that computer-related activities of this kind would be dealt with by offences which were expressed in suitable language rather than having to rely on crimes which were formulated long before computers were ever invented. This alone should avoid any possible confusion for prosecutors and others. So far as penalties are concerned, although the maximum sentence for the common law crimes of fraud, theft, and malicious mischief is life imprisonment, in fact that sentence is seldom, if ever, imposed for these crimes. The maximum sentence for any new statutory offences could be fixed to coincide with what in practice is the highest sentence commonly imposed for the common law crimes.

Our approach to reform

3.15 We have already indicated[1] that we favour the introduction of an offence to deal with the unauthorised obtaining of access to a computer. The question then is: how much further, if at all, should any reform go? We, for our part, are satisfied that, for the reasons given in the previous paragraphs, a new offence should not be introduced to deal expressly with the unauthorised use of computer facilities. In relation to what we have described as eavesdropping on a computer we have considered with care the arguments for making this an offence. There can be no doubt that it is an undesirable activity. On the other hand, as has been noted, it is but one manifestation of what is plainly a much wider problem of industrial or commercial espionage. On that basis we would have been reluctant to recommend the creation of a new offence to deal solely with computer eavesdropping in the absence of a full examination of all the problems posed by modern surveillance techniques. However, since what we have described as eavesdropping is in truth an example of obtaining unauthorised access, if not strictly to a computer, then at least to some of the data stored in a computer, it seems to us that this activity could possibly be comprehended in the unauthorised access offence which we have already recommended. We examine how this might be achieved in Part IV of this Report.

3.16 That, then, leaves for consideration (*a*)activities amounting to fraud or theft, (*b*)activities involving the erasure or corruption of data or programs, and(*c*)activities involving, in some form or another, the taking of information.

3.17 So far as (*a*) and (*b*) are concerned, we have already stated that we are reasonably confident that they can be adequately dealt with by the existing law. So far as (*c*) is concerned, we are in no doubt that the taking of information generally should not become an offence. In our opinion the arguments summarised in paragraph 3.13(2) above are unanswerable. It may be that a detailed review of the whole law of intellectual property, or at least of the law relating to trade secrets,[2] is overdue, but this Report is not the place to embark on such a task.

---

1. Para 3.7 above.
2. The subject of trade secrets is currently under examination in other parts of the world: see for example Report No 46 (1986), Trade Secrets, by the Institute of Law Research and Reform, Alberta, Canada.

3.18 Where information is taken indirectly, as it were, by the temporary appropriation of an article, such as a tape or a disc, in which it is stored, the problem then, as we have noted, is whether that temporary appropriation can itself amount to theft. In our view the present state of Scots law on this matter is unsatisfactory.[1] However, the uncertainties of existing law go far beyond the taking of computer-related articles; or the taking of articles containing information. It would, in our opinion, be inappropriate, and probably unwise, to contemplate a reform of the law of theft, or the creation of a new offence, to deal with a specific activity which is no more than a particular manifestation of a wider problem; and we do not recommend that such a course should be followed.

3.19 It may be, of course, that a person who obtains unauthorised access to a computer will do so for purposes of fraud or theft; or to cause damage to programs or data; or to acquire the information that is stored in a computer. In so far as such activities may be the intended or actual result of obtaining unauthorised access, we can see no reason why they should not be dealt with by a new offence, or new offences. Indeed, as we shall explain more fully in Part IV of this Report, we have come to the conclusion that a new offence, or new offences, related to the obtaining of unauthorised access should attempt to distinguish between those who are merely curious (and probably harmless) and those who engage in the activity for malign purposes or with harmful consequences. In the result our recommendations in relation to activities amounting to fraud or theft, activities involving the erasure or corruption of data or programs, and activities involving the taking of information are, like our recommendation in relation to the activity of eavesdropping on a computer, made solely in the context of new offences directed expressly at such activities. In so far as such activities may be linked to, or form part of, the obtaining of unauthorised access to a computer, they should in our view be comprehended in a new offence or new offences.

3.20 We accordingly **recommend**:

(2) There should be no new offence directed at the unauthorised use of computer time or facilities.

(Paragraphs 3.13–3.15)

(3) Except in so far as the following activities may be linked to, or form part of, a new offence or new offences relating to the unauthorised obtaining of access to a computer,

(*a*) there should be no new offence directed expressly at what we have described as eavesdropping on a computer;

(*b*) there should be no new offences directed expressly at computer-related fraud or theft, or the malicious or reckless corruption or erasure of data or programs; and

(*c*) there should be no new offence directed expressly at the unauthorised taking of information stored in a computer.

(Paragraphs 3.13–3.17)

(4) There should be no new offence directed at the temporary appropriation of discs, tapes, or other data storage articles used in conjunction with a computer.

(Paragraphs 3.13, 3.14, 3.18)

1. See para 2.16 above.

Part IV The shape of reform—unauthorised access offences

4.1 The creation of a new offence to deal with the obtaining of unauthorised access to a computer was, with only a few exceptions, widely supported on consultation, and in Part III of this Report[1] we have recommended that such an offence should be introduced. It is now necessary to consider how such an offence might best be expressed. As will be seen, we have come to the conclusion that two somewhat different aspects of the obtaining of unauthorised access should be made subject to the criminal law, and at the end of the day we shall in fact recommend the creation of two new offences. However, both of these offences will contain certain common elements, and we now turn to consider what those elements should be.

Scope of offences

4.2 The first question, we think, is whether the offences should be restricted to what is commonly referred to as hacking, that is to say long range accessing from a remote computer, probably through the medium of some sort of telecommunication link, or whether they should include accessing of any sort, that is to say including cases where a person can physically, though without authorisation, make contact with a computer. This wider approach would accordingly extend the offences, for example, to the case of an employee who, without authority, sat down at his employer's computer and called up images on the screen. In principle we can see no reason why this wider approach should not be adopted. If it is accepted that the obtaining of unauthorised access to a computer is something which merits the attention of the criminal law, it should not make any difference whether that activity is performed from a distance by one who may be a complete stranger or directly, at close range, by a person such as an employee, but who equally has no authority to gain access to the computer's data or systems.

4.3 If this wider approach were to be adopted it would offer a further advantage. In the Memorandum we discussed at some length, in the context of long range hacking, whether any new offence should be expressed by reference to some form of telecommunication, or simply in terms of obtaining unauthorised access. We pointed out that the unqualified formulation of the offence would extend it, as we have just been discussing, to persons such as employees who could obtain direct access to a computer. The unqualified version of the offence, of course, removes the necessity of referring to any form of telecommunication. In fact, the unqualified version gained the support of most consultees, and it is our preference. We should add that some consultees drew attention to the desirability of making provision for cases where access might be achieved by means of a satellite link: such consultees were apprehensive that any obviously land based reference to telecommunication might exclude that possibility. We think that this risk will disappear if, as we propose, the offences contain no reference to any particular method of communication. We therefore **recommend:**

(5) The offences should be expressed in terms which do not refer to any particular method of communication.

(Paragraphs 4.2–4.3; clause 1(1), (2))

4.4 Even if new offences were to be given the scope that we have just suggested,

1. Para 3.7 above.

there would remain the question whether they should be expressed in a way that would catch every form of unauthorised access or only those where the access was obtained with some ulterior and undesirable purpose in mind. This distinction arises by virtue of the fact that in many instances hackers, who are often quite young and possibly still at school, attempt to gain access to other people's computers simply because of the intellectual and technical challenge which that activity presents. They are, it is said, uninterested in any data which they may see as a consequence of successful hacking, and certainly have no intention of using such information for improper purposes. By contrast, others who seek to obtain unauthorised access to computers do so because they are anxious to use information which they may come upon for purposes of personal gain, or because, for a variety of possible reasons, they hope to manipulate or alter data or programs to someone's disadvantage.

4.5 Initially we were inclined to disregard such distinctions, partly on the basis that the unauthorised obtaining of access to a computer can be regarded as undesirable in any circumstances, and partly on the basis that a simply expressed offence, covering all forms of unauthorised access, might offer advantages in terms of clarity and ease of proof. We have not, however, proceeded with that approach.

4.6 On further reflection we identified a major disadvantage of a somewhat technical nature in an offence expressed simply in terms of unauthorised access of any kind. The disadvantage is that, on conviction of an offence expressed in that way, a court might find it impossible to pass a more severe sentence in a case where it was shown that the unauthorised access had, for example, been part of a deliberate act of industrial or commercial espionage or sabotage. The reason for that is that the offence would itself be described in purely objective terms without reference to the actual or intended consequences, and accordingly the proper sentencing practice would be to ignore any such consequences for the purpose of sentencing. That is the practice which has been judicially approved in, for example, cases of careless driving where it has been held[1] to be improper for a court to impose a more severe sentence than would be justified by reference simply to the quality of the driving in circumstances where that driving has resulted in a death. It seems to us that a simple offence of obtaining unauthorised access to a computer, without any reference to the purpose or consequences thereof, would fall to be dealt with in the same way.

4.7 In our opinion it would not be acceptable that an offence which, as we have suggested, can have very undesirable consequences should in all cases be subject to broadly the same penalty regardless of whether or not such consequences were present or intended; and we doubt whether the business community or the public at large would find that state of affairs acceptable.

4.8 It then seemed to us that the foregoing considerations pointed to the creation of an offence or offences expressed in terms of intention or result. This was in fact a suggestion made to us by several of our consultees. Such an approach would avoid the sentencing problem that we have just described. Additionally, it would mean that the activities of a hacker would not come within the ambit of an offence unless these activities were with the stated intention or the stated result. Although we are not sympathetic to the view that unauthorised hacking should be encouraged so long as it is only a kind of intellectual game, we recognise that, as a matter of public policy, it is probably preferable to express any new offence or offences in terms which actually draw attention to the real mischief at which they are aimed. We would only add that, since in many instances unauthorised access will itself, we expect, be proved by evidence of subsequent activities such as the inspection or corruption of data, hackers who go on to engage in such activities may find it difficult to escape the inference that their original access to a computer was for one of the prohibited purposes.

1. *McCallum* v *Hamilton* 1985 SCCR 368 per LJC Ross at 371; *R* v *Krawec* [1985] Crim LR 108.

The expression of new offences

4.9 We now turn to consider how a new offence or new offences might best be expressed. So far as the obtaining of access itself is concerned, we suggested in the Memorandum that, rather than use the word 'access', the offence should be expressed in terms of 'to communicate with' a computer. One reason for making this suggestion was that we were reluctant to use the word 'access' as a verb, although such use is common in much American legislation on the subject. However, some consultees pointed out that 'communicate with' may carry a sense of a two-way interchange which is not really what is intended in the essentially unilateral activity that this new offence is meant to penalise. It was also pointed out that the word 'access' is familiar to computer users, and can in any event be used as a noun in phrases like 'obtain access to' or 'gain access to'. We are persuaded by these arguments and accordingly conclude that the new offence should be expressed in terms of obtaining access to a computer.

4.10 We have also considered whether, if the word 'access' is to be used, it should be further defined. When, as mentioned earlier, we were considering the creation of an offence that would penalise all forms of unauthorised access we took the view that some definition, in terms of operating or instructing the computer, would be necessary so that the offence would not strike at possibly accidental contacts. For example, we would not have wished such an offence to strike at a person who, possibly through misdialling, made preliminary contact with a remote computer but did nothing more, or at a person, such as an employee, who merely laid his fingers on a computer keyboard. Since we are now proposing that it should be an offence to obtain unauthorised access to a computer only when that is done with an intention to go on to certain other activities, or with certain results, it seems to us that any definition of 'access' would be unnecessary. Moreover, although we have talked thus far in this Report about obtaining unauthorised access to 'a computer', it seems to us that any real mischief will occur only when a person obtains such access to a program or data stored in a computer. If any new offence were to be expressed in these terms, that would in our view diminish still further the need to provide any definition of 'access'.

4.11 Turning now to the intent or result which should be required to make any unauthorised access an offence, it seems to us that one can identify certain kinds of activity which are undesirable if they are engaged in with one or other of two, possibly overlapping, purposes. The activities in question are the inspection of data, and the insertion, alteration or corruption of data or programs. The purposes are the obtaining of an advantage for the unauthorised obtainer of access or another person, and the damaging of some other person's interests. In our opinion, therefore, it should be an offence for a person to obtain unauthorised access to a program or data with the intention of achieving one or other of these purposes by means of any of these activities. There is, however, in our view another element which should be taken into account where the insertion, alteration or corruption of data are involved: that is the element of recklessness. In some instances a person may obtain access to a program or data without any intention of causing harm or damaging anyone's interests, but may in fact produce that result through recklessness in the way in which he instructs the computer or uses its resources. We can see no reason why this should not also be an offence. We recognise that such an offence may in some circumstances duplicate the existing statutory offence of vandalism; but, as we have previously pointed out,[1] that offence can be tried only summarily, and the common law crime of malicious mischief (which can be tried on indictment) may not extend to conduct which is merely reckless as opposed to deliberate. In the circumstances we think that the new offence which we are proposing will serve a useful purpose.

4.12 In these circumstances we accordingly **recommend:**

(6) It should be an offence for a person, without authorisation to do so, to obtain access to a program or data stored in a computer in order to inspect such data

1. Para 2.21 above.

or program, or to add to, alter or corrupt any such data or program for the purpose of—

(*a*) obtaining an advantage for himself or another person; or

(*b*) damaging another person's interests.

(Paragraphs 4.9–4.11; clause 1(1))

(7) It should also be an offence for a person, without such authorisation, to obtain access to a program or data, and to damage another person's interests by recklessly altering, corrupting, erasing, or adding to such a program or data.

(Paragraphs 4.9–4.11; clause 1(2))

4.13 There is one further point which we should mention here. Although, in most cases where access is obtained to a program or data, the program or data in question will be exhibited in visual form, it is, we understand, possible for data to be made available in other ways—for example, aurally. We therefore **recommend:**

(8) The offence proposed in recommendation 6 above should be expressed in such a way that any reference to the inspection of a program or data should not be restricted to inspection by visual means.

(Paragraph 4.13; clause 1(1))

4.14 It is to be noted that, because the new offences which we are proposing (and in particular the first of them) are to be expressed in terms of obtaining access to a program or data stored in a computer rather than to a computer itself, the first of these offences will also extend to the activity which we have earlier described as eavesdropping, that is to say looking in from a distance, and by the interception of radiation emissions, on data being displayed on an authorised user's terminal and screen. While, as noted earlier,[1] we would not have been disposed to recommend the creation of an offence to deal solely with that activity, we can see no objection to its being dealt with under an offence which is primarily designed to deal with a wider range of activities.

Overcoming of a security device

4.15 One possibility which we have also considered is that the offences could be expressed in terms of obtaining access by overcoming a security device, such as a password or an identification number. That would certainly provide an extra element which might assist in establishing the intent which we have proposed. On reflection, however, we have come to the conclusion that such a solution suffers from several disadvantages. First, it may not be possible in some cases to say with certainty whether or not a security device has been overcome. If, for example, a hacker had been told the password by a confederate in the business concerned, could it be said that he had overcome a security device simply by using a password which he already knew? We think there may be some doubt about that. Second, it seems to us that to concentrate on the overcoming of a security device would be to discriminate unfairly against computer owners who do not have any security system. No doubt it is unwise, and possibly negligent, for a computer owner not to seek to protect his data by some sort of security system or device but, just as the law of theft does not distinguish between householders who lock all their doors and those who do not, so too, in our opinion, it would be inappropriate to distinguish between owners with and without security devices or systems. Third, an employee who gains unauthorised access to a computer may be able to do so without going through any entry procedures at all. He may simply seize an opportunity to take access to a colleague's computer which has not been switched off during a tea-break. A requirement of overcoming a security system or device would allow such cases to escape unpunished. For these reasons we do not favour this approach.

1. Para 3.15 above.

Meaning of 'unauthorised'

4.16 Hitherto we have spoken, in relation to the offences which we have been considering, of obtaining 'unauthorised' access to a program or data. The term 'unauthorised' probably requires no further explanation but, in the interests of completeness, we should perhaps set out what we mean by the term. We accordingly **recommend:**

(9) For the purpose of offences of unauthorised access, 'unauthorised' should mean not having authority granted by the person or persons entitled to control access to the program or data in question.

(Paragraph 4.16; clause 1(3))

Further definitions

4.17 We have already dealt with some of the terms which will require to be defined for the purpose of the new offences. There remains, however, the term 'computer' itself. In the Memorandum we suggested that it might be preferable not to offer any definition of that word on the basis that, since computer technology is advancing so rapidly, any definition, even if expressed in terms of function rather than construction, would rapidly become obsolete. This suggestion was approved by most of our consultees, and we see no reason to change our original view.

Partial authorisation

4.18 There remains one further problem in relation to an offence of obtaining unauthorised access. It is that in certain circumstances a person may be authorised to have access to some parts of a computer's data or programs, but not to others. For example, an employee who works in the personnel division of an organisation may be authorised to have access to computer records relating to staff matters, but will probably not be authorised to have access to other records such as those dealing with corporate finance or corporate strategy. As another example mention may be made of those computers which allow a limited amount of public access. We understand that some companies, particularly in the manufacturing field, permit potential customers to obtain access to their computers in order to examine computerised lists or catalogues of products which are available for sale. In some such cases orders for goods may be placed through the computer. In all of these cases one plainly does not wish to penalise the obtaining of access to the program or data in question in so far as that is authorised either explicitly or implicitly. In our view a way of dealing with this problem will be to refer, in the offences, not simply to a program or data but also to any part of a program or data to which the person concerned is not authorised to obtain access. We accordingly **recommend:**

(10) In the offences of unauthorised access references to the obtaining of such access should be expressed as the obtaining of access to a program or data, or to a part of such program or data, to which the person in question is not authorised to obtain access.

(Paragraph 4.18; clause 1(1), (2))

Part V Miscellaneous matters

(1) Attempted offences

5.1 Some consultees, in considering new offences which might be created, urged us to ensure that it will also be contrary to law to attempt to commit any such offence. We simply note that special provision for this is unnecessary since general provision already exists[1] to the effect that an attempt to commit any crime or offence is itself a crime or offence, as the case may be.

(2) Penalties

5.2 In the Memorandum we suggested, in relation to an offence of unauthorised access, that the offence should be triable either summarily or on indictment, and that in the former case the maximum penalty might be 3 months imprisonment or a fine up to the statutory maximum,[2] and in the latter case the maximum might be 2 years imprisonment or an unlimited fine. Many consultees did not address the matter of penalty but, of those who did, some suggested that our proposed maximum sentences were too low. Those consultees were of the view that a maximum sentence of 2 years imprisonment would not deter a person who was really determined to try to gain access to secret and confidential information of great value. We can see some force in that view. In many instances, of course, if the person concerned goes on to perpetrate activities such as fraud or theft, he will be liable to very severe penalties for these offences quite apart from any penalty which might arise for the unauthorised access offence. However, there will not always be further activities of that sort, and in the circumstances we consider that some increase above our original proposal is justified. We accordingly **recommend:**

(11) The offences recommended in recommendations 6 and 7 above should be triable either summarily or on indictment. In the former case the maximum penalty should be 6 months imprisonment or a fine up to the statutory maximum, or both: in the latter case the maximum penalty should be 5 years imprisonment or an unlimited fine, or both.

(Paragraph 5.2; clause 3)

5.3 Before leaving the subject of penalties we should mention that some consultees suggested to us that, in addition to a power to imprison or fine, courts should also be empowered to order forfeiture of any computers or other equipment used in the commission of the offence. We can readily understand that on occasions courts might wish to do this. However, we consider that it is unnecessary to confer this power expressly since it already exists as a general power.[3] In our view the existing power is expressed in sufficiently wide terms to include the kinds of forfeiture which our consultees were contemplating.

(3) Official authorisation for obtaining access to a computer

5.4 When we considered in the Memorandum the possibility of introducing an unauthorised access offence, we also raised the possibility[4] that there might be circumstances where official investigating authorities, such as the police, should be authorised to obtain access to a computer without the knowledge or authority of the computer owner. In raising this matter we were mindful of the analogy to be found in the Interception of Communications Act 1985. Under that Act it is an offence to engage in the practice commonly referred to as 'telephone tapping',[5] but the Act

1. Criminal Procedure (Scotland) Act 1975 ss 63(1), 312(*o*).
2. At present £2,000.
3. Criminal Procedure (Scotland) Act 1975 ss 223, 436.
4. The Memorandum para 6.9.
5. s 1. As we observed in the Memorandum this provision, as it is expressed, will also strike at the interception of communications between computers where these are effected by means of a public telecommunications system.

specifically empowers the Secretary of State to issue a warrant requiring the person to whom it is addressed to intercept such communications as are described in the warrant. The Secretary of State is not to issue such a warrant unless he considers that it is necessary (*a*) in the interests of national security, (*b*) for the purpose of preventing or detecting serious crime, or (*c*) for the purpose of safeguarding the economic well-being of the United Kingdom.[1]

5.5 Although the direct accessing of a computer probably raises somewhat different considerations, since it will not be effected clandestinely and will normally take place under the authority of a conventional search warrant, remote accessing (hacking) is sufficiently analogous to telephone tapping, particularly by reason of its clandestinity, that we invited consultees to let us know whether any new unauthorised access offence should be subject to some special provision for official authorisation. Of the consultees who addressed this question almost all were in favour of such provision being made. Having now reconsidered this matter we are of opinion that there should be provision for official authorisation. No doubt the occasions may be few and far between when such authorisation will be required, but it would, we think, be unfortunate if the police or other investigating authorities were to be at risk of committing an offence by covertly accessing programs or data stored in a computer even where that was, for example, necessary for the purpose of preventing or detecting serious crime. We accordingly **recommend:**

(12) The offences of unauthorised access to a program or data stored in a computer should not be committed where the person concerned has official authorisation for what he is doing.

(Paragraphs 5.4–5.5; clause 1(4))

5.6 In the Memorandum we suggested that, if there were to be provision for official authorisation, this might be achieved in a manner similar to that to be found in the Interception of Communications Act. Most consultees agreed with that proposal, but a few considered that it might be sufficient if authorisation were to be granted under a simple court procedure, rather similar to that used when a search warrant is being applied for. In our view such a procedure would be inadequate for this purpose. In the first place it would be difficult to justify a relatively simple court procedure in respect of the clandestine accessing of computer data or programs when the authorisation of the Secretary of State is required in respect of the clandestine interception of telephone conversations and indeed the clandestine interception of communications passing between computers: as we have pointed out, the two activities are closely analogous. In the second place, it seems to us that an important reason for entrusting the granting of warrants to the Secretary of State under the 1985 Act is that he will be in the best position to judge whether the grounds on which a warrant may be granted[2] do in fact exist. It would, we think, be inappropriate to entrust to a judge the task of determining whether, for example, the grant of a warrant would be 'in the interests of national security'. We accordingly conclude that provision for what we have termed 'official authorisation' to obtain remote, and therefore clandestine, access to a program or data stored in a computer should be made in a similar manner to that provided in the 1985 Act. Moreover, since in our view such authorisation should be granted only in exceptional circumstances, we consider that it should be available only in the same circumstances as justify the grant of a warrant under the 1985 Act. We accordingly **recommend:**

(13) Provision, similar to that contained in the Interception of Communications Act 1985, should be made for official authorisation to be granted by the Secretary of State.

(Paragraph 5.6; clause 2(1), (3) to (6), Schedule)

(14) The grounds upon which authorisation may be granted should be the same as in section 2(2) of that Act, namely that it is necessary (a) in the interests of national security, (b) for the purpose of preventing or detecting serious

1. s 2(1) and (2).
2. See para 5.4 above.

crime, or (c) for the purpose of safeguarding the economic well-being of the United Kingdom.

(Paragraph 5.6; clause 2(2))

5.7 Having reached the foregoing conclusions we next considered how the provisions of the 1985 Act could, or should, be modified so as to apply to the officially authorised obtaining of access to programs or data stored in a computer. Plainly parts of section 2 and the whole of sections 4 and 5 are relevant to what we are proposing, as also are the provisions relating to safeguards (section 6), to the Tribunal (section 7), and to the Commissioner (section 8), as well as certain ancillary provisions in sections 9 and 10. What has caused us some difficulty is to find, in relation to computer programs and data, some provision which is comparable to section 3 of the 1985 Act. That section limits the scope of warrants issued under section 2 of the Act by reference to certain premises, persons, communications or material described or specified in the warrant. Some comparable limitation is clearly desirable in respect of the warrants which we envisage; but the extensive provisions of section 3 of the 1985 Act are of course expressed in terms which are inappropriate for the essentially unilateral activity of obtaining access to a program or data stored in a computer. Moreover, it seems to us to be likely that the precise wording of section 3 may well have been influenced by confidential advice given by, among others, the security services.[1] It would not, we think, be appropriate for us to seek to obtain such advice. Consequently, what appears in clause 2 of the Bill annexed to this Report, and in particular what appears in clause 2(5), is in our view the minimum that may be required to introduce a warrant procedure in respect of the obtaining of access to programs or data stored in a computer: some amplification, particularly of our clause 2(5), may however prove to be desirable should our proposals be enacted. Consequential amendments to the 1985 Act are dealt with in clause 2(6) and in the Schedule to the draft Bill.

(4) Duty to disclose incidents of computer crime

5.8 In the Memorandum[2] we sought views on whether or not computer users should be under a statutory duty to disclose incidents of computer crime of which they had been the victims. We said at that time that we were not persuaded that there is a case for the imposition of such a duty.

5.9 Most of our consultees took the same view, but some have argued strongly that such a duty should be imposed. We have also heard calls for the introduction of a duty of disclosure at conferences, seminars and meetings which some of us have attended. The arguments advanced by those who favour compulsory disclosure appear to be as follows:

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

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

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

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

5.10 The principal contrary arguments are as follows:

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

1. See the Report for 1986 of the Commissioner appointed under the Interception of Communications Act 1985, March 1987, Cm 108, from which it appears that the security services are involved in several of the interceptions authorised under that Act.
2. Para 6.17 *et seq.*

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

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

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

5.11 In our opinion the arguments against imposing a duty of disclosure are quite unanswerable. We accordingly **recommend:**

(15) There should be no statutory duty to disclose incidents of computer crime.

(Paragraphs 5.8–5.11)

(5) A statutory code of practice

5.12 A final possibility which we examined in the Memorandum[1] was that there should be a statutory code of practice setting out, in particular, minimum security measures that should be taken by all computer users. We were not attracted by this proposal when we considered it in the Memorandum, and it attracted no support on consultation. We accordingly **recommend:**

(16) A statutory code of practice for computer users should not be introduced.

(Paragraph 5.12)

(6) Jurisdiction

5.13 The final matter considered in the Memorandum[2] was that of jurisdiction. We examined this subject because, in the context of long-range unauthorised accessing of computer data or programs, there may be jurisdictional problems where the offender is in one country and the target computer where the data or programs are stored is in another. In relation to Scotland the offender could be in Scotland and the target computer elsewhere, or vice versa.

5.14 We took the view, as a matter of policy, that in both such cases the Scottish courts should have jurisdiction. Of course, in the case where the target computer is in Scotland and the offender is elsewhere, it will not be possible to charge and try the offender unless he can physically be brought within the jurisdiction of the Scottish courts; but that is a different problem from having, or not having, jurisdiction to try the actual offence. Our policy on this matter was supported by consultees. In the circumstances we **recommend:**

(17) Where the offences recommended in this Report are committed partly in Scotland and partly in another country, the Scottish courts should have jurisdiction to try the offender irrespective of whether at the material time he was himself in Scotland or in that other country.

(Paragraphs 5.13–5.14; clause 4)

1. Para 6.21 *et seq.*
2. Part VII.

Part VI Summary of recommendations

Unauthorised access to a computer

1. Provision should be made for it to be an offence to obtain unauthorised access to a computer.

(Paragraphs 3.6–3.7; clause 1(1), (2))

Other possible offences

2. There should be no new offence directed at the unauthorised use of computer time or facilities.

(Paragraphs 3.13–3.15)

3. Except in so far as the following activities may be linked to, or form part of, a new offence or new offences relating to the unauthorised obtaining of access to a computer:

(*a*) there should be no new offence directed expressly at what we have described as eavesdropping on a computer;

(*b*) there should be no new offences directed expressly at computer-related fraud or theft, or the malicious or reckless corruption or erasure of data or programs; and

(*c*) there should be no new offence directed expressly at the unauthorised taking of information stored in a computer.

(Paragraphs 3.13–3.17)

4. There should be no new offence directed at the temporary appropriation of discs, tapes, or other data storage articles used in conjunction with a computer.

(Paragraphs 3.13, 3.14, 3.18)

Formulation of unauthorised access offences

5. The offences should be expressed in terms which do not refer to any particular method of communication.

(Paragraphs 4.2–4.3; clause 1(1), (2))

6. It should be an offence for a person, without authorisation to do so, to obtain access to a program or data stored in a computer in order to inspect such data or program, or to add to, alter or corrupt any such data or program for the purpose of:

(*a*) obtaining an advantage for himself or another person; or

(*b*) damaging another person's interests.

(Paragraphs 4.9–4.11; clause 1(1))

7. It should also be an offence for a person, without such authorisation, to obtain

access to a program or data, and to damage another person's interests by recklessly altering, corrupting, erasing, or adding to such a program or data.

(Paragraphs 4.9–4.11; clause 1(2))

8. The offence proposed in recommendation 6 above should be expressed in such a way that any reference to the inspection of a program or data should not be restricted to inspection by visual means.

(Paragraph 4.13; clause 1(1))

9. For the purpose of offences of unauthorised access, 'unauthorised' should mean not having authority granted by the person or persons entitled to control access to the program or data in question.

(Paragraph 4.16; clause 1(3))

10. In the offences of unauthorised access references to the obtaining of such access should be expressed as the obtaining of access to a program or data, or to a part of such program or data, to which the person in question is not authorised to obtain access.

(Paragraph 4.18; clause 1(1), (2))

Penalties

11. The offences recommended in recommendations 6 and 7 above should be triable either summarily or on indictment. In the former case the maximum penalty should be 6 months imprisonment or a fine up to the statutory maximum, or both: in the latter case the maximum penalty should be 5 years imprisonment or an unlimited fine, or both.

(Paragraph 5.2; clause 3)

Official authorisation for obtaining access to a computer

12. The offences of unauthorised access to a program or data stored in a computer should not be committed where the person concerned has official authorisation for what he is doing.

(Paragraphs 5.4–5.5; clause 1(4))

13. Provision, similar to that contained in the Interception of Communications Act 1985, should be made for official authorisation to be granted by the Secretary of State.

(Paragraph 5.6; clause 2(1), (3) to (6), Schedule)

14. The grounds upon which authorisation may be granted should be the same as in section 2(2) of that Act, namely that it is necessary (a) in the interests of national security, (b) for the purpose of preventing or detecting serious crime, or (c) for the purpose of safeguarding the economic well-being of the United Kingdom.

(Paragraph 5.6; clause 2(2))

Duty to disclose incidents of computer crime

15. There should be no statutory duty to disclose incidents of computer crime.

(Paragraphs 5.8–5.11)

A statutory code of practice

16. A statutory code of practice for computer users should not be introduced.

(Paragraph 5.12)

Jurisdiction

17. Where the offences recommended in this Report are committed partly in Scotland and partly in another country, the Scottish courts should have jurisdiction to

try the offender irrespective of whether at the material time he was himself in Scotland or in that other country.

(Paragraphs 5.13–5.14; clause 4)

Appendix A

COMPUTER CRIME (SCOTLAND) BILL

ARRANGEMENT OF CLAUSES

Clause

Schedule

DRAFT

OF A

BILL

TO

AD 1987

Create offences as respects Scotland relating to the obtaining of unauthorised access to a program or to data stored in a computer.

BE IT ENACTED by the Queen's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:—

Offences of unauthorised access to a program or data stored in a computer.

1.—(1) A person commits an offence if, not having authority to obtain access to a program or data stored in a computer, or to a part of such program or data, he obtains such unauthorised access in order to inspect or otherwise to acquire knowledge of the program or the data or to add to, erase or otherwise alter the program or the data with the intention—

(*a*) of procuring an advantage for himself or another person; or

(*b*) of damaging another person's interests.

(2) A person commits an offence if, not having authority to obtain access to a program or data stored in a computer, or to a part of such program or data, he obtains such unauthorised access and damages another person's interests by recklessly adding to, erasing or otherwise altering the program or the data.

(3) For the purposes of this section, a person does not have authority to obtain access to a program or data stored in a computer, or to a part of such program or data, if he does not have the authority of a person entitled to control such access.

(4) Notwithstanding the foregoing provisions of this section, a person shall not commit an offence under this section if he obtains such access as aforesaid in pursuance of a warrant issued by the Secretary of State under section 2 of this Act.

Access under warrant of Secretary of State.

2.—(1) Subject to the provisions of this section, the Secretary of State may issue a warrant requiring the person to whom it is addressed to obtain access to a program or data stored in a computer, or to any part of such program or data, for the purpose of acquiring information; and such a warrant may also require the person to whom it is addressed to disclose any information so acquired to such persons and in such manner as are described in the warrant.

(2) The Secretary of State shall not issue a warrant under this section unless he considers that the warrant is necessary—

(*a*) in the interests of national security;

(*b*) for the purpose of preventing or detecting serious crime; or

(*c*) for the purpose of safeguarding the economic well-being of the United Kingdom.

(3) The matters to be taken into account in considering whether a warrant is necessary as mentioned in subsection (2) above shall include whether the information which it is considered necessary to acquire could reasonably be acquired by other means.

(4) A warrant shall not be considered necessary as mentioned in subsection (2)(*c*) above unless the information which it is considered necessary to acquire is information relating to the acts or intentions of persons outside the British Islands.

(5) A warrant under this section shall specify or describe an address or addresses, being an address or addresses used, or likely to be used, to accommodate a computer containing a program or data the examination of which the Secretary of State considers necessary as mentioned in subsection (2) above.

1985 c. 56.

(6) Sections 4 to 10 of the Interception of Communications Act 1985 and Schedule 1 to that Act shall, subject to the adaptations set out in the Schedule to this Act, apply in relation to a warrant under this section.

Penalties.

3.—A person guilty of an offence under this Act shall be liable—

(*a*) on summary conviction, to imprisonment for a term not exceeding 6 months or to a fine not exceeding the statutory maximum, or both; or

(*b*) on conviction on indictment, to imprisonment for a term not exceeding 5 years or to an unlimited fine, or both.

Clause 1 implements the general policy of the Report that there should be new offences to penalise the unauthorised obtaining of access to a program or data stored in a computer. See Recommendations 1, 6 and 7.

Subsection (1) implements Recommendations 5, 6, 8 and 10. It makes it an offence to obtain access to a program or data stored in a computer, or to a part of such program or data, (not having authority to do so) in order to inspect or otherwise to acquire knowledge of the program or data, or to add to, erase or otherwise alter the program or data with the intention of procuring an advantage or of damaging another person's interests. Expressed in this way the offence will not be committed by a person who obtains unauthorised access to a program or data but who does so without the stated purpose or intention.

Subsection (2) implements Recommendations 5, 7 and 10. It creates a parallel offence to deal with the situation where a person obtains unauthorised access to a program or data without the purpose or intention in the offence in subsection (1), but who damages another person's interests by recklessly adding to, erasing or otherwise altering the program or data.

Subsection (3) implements Recommendation 9, and in effect defines the words "not having authority" as used in subsections (1) and (2).

Subsection (4) implements Recommendation 12. It provides that neither of the offences in subsections (1) and (2) will be committed by a person who obtains access to a program or data in pursuance of a warrant issued by the Secretary of State. The circumstances in which such a warrant may be granted are dealt with in clause 2 and in the Schedule annexed to the Bill. See discussion in paragraph 5.4 and 5.5.

Clause 2 sets out the circumstances in which the Secretary of State may grant a warrant for the obtaining of access to a program or data stored in a computer. The provisions in the clause are modelled on those in the Interception of Communication Act 1985 ("the 1985 Act"), and much of that Act will, with modifications, apply to warrants issued under this clause.

Subsection (1) implements Recommendation 13, and permits the Secretary of State to issue a warrant requiring the person to whom it is addressed to obtain access to a program or data stored in a computer, or to any part of such program or data, for the purpose of acquiring information. This is analogous to section 2(1) of the 1985 Act.

Subsection (2) implements Recommendation 14, and sets out the grounds upon which a warrant may be issued. These are the same as the grounds expressed in section 2(2) of the 1985 Act.

Subsections (3) and (4) are in further implementation of Recommendation 13, and apply to the issuing of a warrant on the same considerations as are to be found in section 2(3) and (4) of the 1985 Act.

Subsection (5) provides that a warrant must specify or describe an address or addresses used, or likely to be used, to accommodate a computer containing a program or data the examination of which the Secretary of State considers necessary. This subsection is intended to perform a limiting function in relation to the scope of a warrant comparable to that achieved by section 3 of the 1985 Act.

Subsection (6) applies sections 4 to 10 and the Schedule of the 1985 Act to a warrant issued under subsection (1) above, subject to the adaptations set out in the Schedule to the Bill.

Clause 3 implements Recommendation 11, and prescribes the maximum penalties which may be imposed on summary conviction, and on conviction on indictment, in respect of the offences in clause 1(1) and (2).

Jurisdiction.

4.—A court in Scotland shall have jurisdiction to entertain proceedings for an offence under this Act if at the time the offence was committed—

(*a*) the accused was in Scotland; or

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

Short title commencement and extent.

5.—(1) This Act may be cited as the Computer Crime (Scotland) Act 1987.

(2) This Act shall come into force at the end of the period of 2 months beginning with the day on which it is passed.

(3) This Act extends to Scotland only.

Clause 4 implements Recommendation 17. It provides that a court in Scotland is to have jurisdiction in respect of an offence under the Bill if, at the relevant time, the accused was in Scotland, or the program or data in relation to which the offence was committed was stored in a computer in Scotland.

Section 2(6)

SCHEDULE

Adaptations of provisions of the Interception of Communications Act 1985 in their application to warrants under section 2 of this Act.

1. Any reference to a warrant under section 2 of the Interception of Communications Act 1985 shall, unless the context otherwise requires, include a reference to a warrant under section 2 of this Act.

2. In section 5—

(*a*) in subsection (1)(*a*) after the word "above" there shall be inserted the words "or which he considers is used, or is likely to be used, as mentioned in section 2(5) of the Computer Crime (Scotland) Act 1987";

(*b*) in subsection (2) after the word "above" there shall be inserted the words "or is no longer used, or is no longer likely to be used, as mentioned in section 2(5) of the Computer Crime (Scotland) Act 1987".

3. In section 6—

(*a*) in subsection (1)(*a*) after the word "material" there shall be inserted the words "or, as the case may be, the information acquired in pursuance of the warrant under section 2 of the Computer Crime (Scotland) Act 1987";

(*b*) in subsections (2) and (3)—

(i) after the words "intercepted material" there shall be inserted the words "or acquired information";

(ii) after the words "the material" wherever they occur there shall be inserted the words "or information".

4. In section 7—

(*a*) after subsection (2) there shall be inserted the following subsection—

"(2A) Any person who believes that access has been obtained to a program or data stored by him in a computer may apply to the Tribunal for an investigation under this section.";

(*b*) at the end of subsection (3)(*b*) there shall be added the words "or, as the case may be, of section 2 of the Computer Crime (Scotland) Act 1987 or section 4 or 5 above in relation to the warrant.";

(*c*) in subsection (4) after the word "certificate" there shall be inserted the words "or, as the case may be, of section 2 of the Computer Crime (Scotland) Act 1987 or section 4 or 5 above in relation to a relevant warrant";

(*d*) at the end of subsection (5)(*b*) there shall be added the words "or of copies of the information acquired in pursuance of the warrant under section 2 of the Computer Crime (Scotland) Act 1987";

(*e*) at the end of subsection (7) there shall be added the words "or, as the case may be, of section 2 of the Computer Crime (Scotland) Act 1987 or section 4 or 5 above in relation to a relevant warrant.";

(*f*) at the end of subsection (9) there shall be added the following paragraph—

"(*c*) a warrant under section 2 of the Computer Crime (Scotland) Act 1987 is a relevant warrant in relation to an application if an address used by the applicant to accommodate a computer is specified or described in the warrant.".

5. In section 8—

(*a*) in subsection (1)(*a*) after the words "sections 2 to 5 above" there shall be inserted the words "and by section 2 of the Computer Crime (Scotland) Act 1987";

(*b*) in subsection (5)(*a*) after the words "sections 2 to 5 above" there shall be inserted the words "or, as the case may be, of section 2 of the Computer Crime (Scotland) Act 1987 or section 4 or 5 above".

The *Schedule* is provided for in clause 2(6). It set out the adaptations which are necessary so that sections 4 to 10 of the Interception of Communications Act 1985 will apply to a warrant issued under clause 2 of the Bill.

6. In section 9, in subsections (1)(*a*), (3)(*b*) and (4)(*a*) after the word "above" there shall be inserted the words "or under section 1 of the Computer Crime (Scotland) Act 1987".

7. In section 10(1) in the definition of "copy"—

(*a*) after the words "intercepted material" there shall be inserted the words "or information acquired in pursuance of the warrant";

(*b*) after the words "the material" in both places where they occur there shall be inserted the words "or information".

EXPLANATORY NOTE

Appendix B

List of those who submitted written comments on Memorandum No. 68

(Note: In the case of some of the organisations listed below the views which were expressed were those of individuals, or groups of individuals, within the organisation in question, and were not necessarily the views of the organisation itself.)

Association of Chief Police Officers (Scotland)
Association of Scottish Chambers of Commerce
Association of Scottish Police Superintendents
Audit Commission for Local Authorities in England and Wales
BIS Applied Systems Ltd
D J Blackwell
British Computer Society
British Telecom
Building Societies Association
Commission for Local Authority Accounts in Scotland
Committee of London and Scottish Bankers
Committee of Scottish Clearing Bankers
Confederation of British Industry
Crown Office
Digital Equipment Co Ltd
Cliff Dilloway
Faculty of Advocates
General Accident Fire and Life Assurance Corporation
HM Customs and Excise
Dr H J Highland, New York
Dr John Hulbert, Devon and Cornwall Constabulary
Institute of Chartered Accountants in England and Wales
Institute of Chartered Accountants of Scotland
K M G Thomson McLintock, Chartered Accountants
Law Society of Scotland
Legal Technology Group
Professor A M McCosh
Professor Michael C Meston
Rt Hon Lord Murray
National Computing Centre Ltd
National Council for Crime Prevention, Sweden
John Pringle
Fu Rui, Director-General, Computer Inspection Bureau, People's Republic of China
Professor Doctor B de Schutter, Brussels
Scottish Convention of Women
Scottish Law Agents Society
Sheriffs Association
Dr Ulrich Sieber, Freiburg, West Germany
Society for Computers and Law
Society of Writers to HM Signet
University of Aberdeen Law Faculty

Printed by HMSO, Edinburgh Press
Dd 0287084/HF4716 C14 7/87 (246802)