Scottish Law Commission

CONSULTATIVE MEMORANDUM NO. 68

Computer Crime

MARCH 1986

This Consultative Memorandum is published for comment and criticism and does not represent the final views of the Scottish Law Commission

The Commission would be grateful if comments on this Consultative Memorandum were submitted by 30th September 1986. All correspondence should be addressed to -

Mrs A M Cowan
Scottish Law Commission
140 Causewayside
Edinburgh
EH9 1PR

(Telephone: 031-668 2131)

Note In writing its Report with recommendations for reform, the Commission may find it helpful to refer to and attribute comments submitted in response to this Consultative Memorandum. Any request from respondents to treat all, or part, of their replies in confidence will, of course, be respected but if no request for confidentiality is made, the Commission will assume that comments on the Consultative Memorandum can be used in this way.

CONTENTS

SCOTTISH LAW COMMISSION

CONSULTATIVE MEMORANDUM NO. 68

COMPUTER CRIME

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 It is perhaps not unfair to say that in recent years scarcely a day has passed without there being some sort of reference to what is called "computer crime" in newspapers, periodicals, television, or the like. For example, The Times of 14 March 1985 carried an article headlined "Computer fraud costing companies '£2m. a day'". The writer of the article went on to claim that the marketing director of a firm of international insurance brokers had said that four British banks have budgeted £85 million against computer frauds this year. In the Sunday Times, on 9 December 1984, an article urged that the Department of Trade and Industry and the Home Office should, as a matter of urgency, prepare guidelines for computer abuse legislation. A programme shown on television early in 1985 demonstrated that, with the use of relatively inexpensive equipment, it is possible to eavesdrop from long range on the activities of a computer or word-processor by intercepting the electro-magnetic

radiation which surrounds all such machines while they are in operation, and which can be detected if the machines are not adequately shielded.

1.3 Apart from media interest in such matters, there has for some time now been considerable professional interest both in the United Kingdom and abroad. In the United Kingdom many large companies and corporations have addressed the problem within their own organisations. Professional bodies representing, for example, accountants and auditors have set up committees to examine computer crime. The Audit Commission for Local Authorities in England and Wales published Computer Fraud Surveys in 1981 and in 1985. Outside the United Kingdom the American Bar Association has campaigned for federal legislation on computer crime in the USA. Within Europe the subject is under review by, among others, the Commission of the EEC, the Council of Europe, the Justice Ministry of the Federal German Republic, and the National Swedish Council for Crime Prevention. The scope for international co-operation is being examined by the OECD. Further afield, the whole subject is presently under review by the Law Reform Commissions of, respectively, Hong Kong and Tasmania, to take but two examples.

1.4 All of this world-wide interest and activity provides, in a sense, the background against which we were invited to examine the problems of computer crime. In all parts of the world there seems to be a growing awareness that modern computer technology, and the opportunities which it presents for criminal behaviour, may have outrun the effectiveness of the criminal law to control and regulate such behaviour. But, simply to say

that is in fact to beg one of the major questions which it is the purpose of this Memorandum to explore. That question is: what is meant by the term "computer crime"? Since much of the present world-wide concern centres on the fact that certain computer-related activities are not, or may not be, crimes according to national systems of law, it is in a sense something of a misnomer to use the term since it may prejudge the question of what should be a crime. That in turn involves, among other things, moral and economic judgments on which opinions may differ.

1.5 To deal with the whole subject of what for convenience we shall at present continue to call computer crime it will be necessary to attempt some sort of analysis of the scope and range of computer technology, and of the ways in which that technology can be used, abused, or misused, in order to see what sort of activities could, or should, be made subject to the criminal law. Since we in this Commission are not ourselves computer experts, and have only a limited experience of computers in operation, we have in this instance engaged in substantial consultation prior to preparing this Memorandum. The purpose of this consultation was, firstly, to enable us to assess whether those more experienced in the world of computers than ourselves considered that a review of the relevant criminal law was desirable or necessary at all; secondly, to seek advice on the range of activities which are causing concern; and thirdly, to discover how any perceived problems are being, or have been, tackled elsewhere in the world. For that purpose we contacted a wide range of individuals, companies and organisations

both in the United Kingdom and abroad. While some of those contacted felt unable to assist us at this stage, the majority were able to offer us considerable advice and assistance. All of those who did so were of the view that an examination of computer crime in this country was both timely and highly desirable. We are most grateful to all who have given us help towards the preparation of this Memorandum. A full list of all those who did so is to be found in Appendix B at the end of the Memorandum.

1.6 Despite all the help which we have received, we remain, in a sense, amateurs in relation to computer operations. Consequently any descriptions which we give of such operations may appear somewhat simplistic to those who are more experienced and knowledgeable than ourselves. We hope, however, that any such descriptions are accurate; and we take comfort in the thought that some of the readers of this Memorandum may be as unfamiliar with computers as ourselves, and may find it easier to follow certain parts of the Memorandum if they are expressed in a reasonably simple way. That said, however, it has to be acknowledged that computer technology has accumulated a great deal of jargon, most of which now has a precise, and well understood, meaning. While we have attempted to keep to a minimum our use of such jargon, it has in some cases been necessary in the interests of accuracy.

1.7 In Part II of the Memorandum we examine the nature and scale of the problem of computer crime; in Part III we consider the suitability of existing criminal law for dealing with that problem; in Part IV we ask whether our examination of existing law reveals a need

for reform; in Part V and in Appendix A we examine the approaches to law reform that have been adopted in other jurisdictions; in Part VI we set out some possible reform of Scots criminal law; and in Part VII we consider some consequential problems affecting the jurisdiction of the Scottish courts. Finally, in Part VIII we set out a summary of the questions and provisional proposals to which consultees are invited to respond.

1.8 There are two matters which we have not addressed in this Memorandum. One is the abuse of telecommunications systems in isolation from computers and computer systems. Although the terms of the proposal which we received from the Law Society[1] appear to direct us to this topic, our understanding is that telecommunications systems are mentioned there simply to take account of the fact that such systems play a crucial role in enabling computers to communicate with each other. It was not, as we understand it, the intention of the Law Society that we should, for example, embark on a study of the improper uses that may be made of the ordinary telephone system. The second matter which we have not addressed here is the law of evidence. We are aware that computer-generated evidence presents many problems for the law, and that, in criminal proceedings, these problems may be increased rather than diminished if computer-related offences were in future to be prosecuted with any regularity in the courts. We are, however, presently engaged in a separate study of the whole law of

---

1 See para.1.1 above.

evidence and we intend to deal with the topic of computer-generated evidence in the course of that study.

PART II - THE NATURE AND SCALE OF THE PROBLEM

A brief history of the computer

2.1 The computer, as a device for storing and processing data, has been in existence since about the end of World War II. The first computers were physically bulky, were operated by an unreliable system of thermionic valves, and were comparatively slow in the speed with which they performed calculations. Gradually, however, semiconductor technology replaced the earlier valve systems; and with the growth of the science of micro-electronics, and the growth of micro-chip technology, computers rapidly became smaller, more efficient, more reliable, and, simultaneously, less expensive. Some universities are now experimenting with optical techniques which may in the future replace electronic technology as a means of operating computers.

2.2 When computer technology was in its infancy there were very few people who knew anything about how computers worked; their possible use and application was thought to be very limited; and there were very few of them in existence. Today school children are, as a matter of course, taught computer use and computer programming, as well as something of computer technology, from an early age. The existing and future uses and applications of computers are virtually without number, and millions of computers have been sold, and are in use, throughout the world. The range of computers available today is very large. At one extreme large corporations, and some Government departments, may have mainframe computers, and related networks, costing hundreds of thousands, or even millions of pounds. On the other hand

a small business can acquire a mini-computer powerful enough to perform many functions for a few thousand pounds. And at the other extreme a micro-computer, small enough to stand on a desk or a table in a person's home, can be purchased for, at most, a few hundred pounds.

What does a computer do?

2.3 Essentially a computer is a device for storing and processing data, by which is meant information of any kind - numbers, words, scientific formulae, or whatever. At its simplest a computer may be used as little more than an electronic filing cabinet, that is to say a receptacle in which data can be stored for instant recall as required. Even at this level a computer has certain advantages over a conventional manual filing system. The data can be stored much more compactly on magnetic tape, or on a disc; it can be retrieved much more quickly than is normally possible with a manual system; and it can be altered or amended easily and speedily without, for example, the necessity of removing some pieces of paper and replacing them with others.

2.4 A computer has, however, a further advantage over a manual filing system which is of virtually immeasurable potential: that is its ability to process the data stored in or fed into it. In response to a set of logical instructions (known as a program) a computer can be given the ability to collate or retrieve required parts of data stored in it, to perform calculations based upon that data, or to transmit data and instructions to other computers which may be geographically distant by hundreds, or even thousands, of miles.

2.5 To take a simple example, if the data in a computer consisted of the personnel files of all the employees in a business, the computer could be programmed so as to produce, in response to a single instruction, a list of all the employees above a certain age, or who had worked for the business for more than a certain number of years, or who earned more than a given sum of wages or salary. At a rather more sophisticated level the computer in that same business could be programmed to calculate the weekly or monthly payments due to all the employees, making the necessary calculations for tax, national insurance, and any other deductions, and at the end of the process producing the requisite pay slips, and possibly even the pay cheques themselves.

2.6 As mentioned above, computers may also be separated geographically but remain in contact with each other. This sort of network may be no more than several computers within the same building, which are linked to each other by electric cables; or it may commonly involve computers in different parts of the country, or even abroad, where contact between them is achieved through the public telecommunications system, or through a privately owned or leased telecommunications line.

2.7 The use of public telecommunications systems is common where it is necessary for long range contact to be maintained. For example, a large company manufacturing consumer goods which are sold throughout the country may have a computer which has been programmed to process orders from salesmen. On receipt of such an order the computer will, possibly by communicating with another computer within a network, determine the despatch

warehouse which should handle the order, list the necessary instructions for employees in that warehouse, make the necessary amendments on the stock control file, and prepare an appropriate invoice for submission to the customer. None of that, however, can happen until the salesman can communicate his order to the computer which may, of course, be many hundreds of miles distant from him. To enable that to be done the salesman will have, in his local office or possibly even in his home, a computer terminal consisting of a keyboard and a screen, an ordinary telephone, and a device such as an acoustic coupler or a modem which provides the link between his terminal and the public telephone system which in turn is linked to the central computer with which he wishes to make contact. Having dialled the appropriate telephone number, and having used any password or other access procedures that may be necessary, he can then communicate his instructions direct to the central computer by typing them out on his terminal keyboard.

Hardware and software

2.8 The materials used for data processing are usually described as being either "hardware" or "software". By "hardware" is meant the physical objects such as keyboards, screens, central processing units, and the like. "Software" on the other hand is the general term for computer programs and data. While many of the larger computer users, and those engaged in particularly sensitive activities, may write their own programs, there is also a considerable market in ready-made software packages designed for a variety of business applications.

Security of computers and computer systems

2.9 For obvious reasons it is customary for most computers, other perhaps than those used at home, to have some sort of security device incorporated into them. Even where authorised users are concerned this may be desirable where it is considered that certain users should be permitted access only to certain sections of the computer's stored data. And, because of the widespread use of public telecommunications systems as a means of making contact with computers at long range, it is obviously desirable to have some means of preventing access by those who are not authorised to use the computer at all.

2.10 Varying degrees of security can be achieved in different ways. For a start, every authorised user may be given some form of identification which the computer will recognise. Like the personal identification number given to users of bank cash cards, this may be supplied by the organisation operating the computer, though in such a case the particular number may be randomly chosen by the computer itself, and may be unknown to any of the other employees of the organisation concerned. Alternatively, an authorised user of a computer may, as it were, invent his own identification: he will personally give the appropriate instructions to the computer so that it will thereafter recognise that identification whenever it is used.

2.11 Apart from personal identification, the computer system itself, or particular files within it, may require some form of password to be used before access can be

gained. This may be a simple combination of digits or, commonly, it may be an alphanumeric password consisting of a combination of digits and letters of the alphabet. On the other hand, a password may simply be the name of the company chairman's daughter!

2.12 As an additional security measure a computer, as well as being programmed to recognise and to respond to the correct personal identifications and passwords, may also be programmed specifically to deny access when an incorrect identification or password is supplied to it. To allow for ordinary human error a few false attempts may be permitted, but thereafter the computer will simply not respond even if the correct information is supplied.

2.13 Yet another form of security involves the encryption of data so that, even if an unauthorised person manages to access the computer, any data which he sees will be meaningless. While encryption may be necessary where highly sensitive information is involved, it can prove less than convenient for those who actually have to make use of that data.

2.14 Further security can be obtained in some cases by using fixed lines, or privately leased lines, as a means of communication between computers rather than the public telecommunications network; but that is expensive, and may not be practicable where international, as opposed to purely local, communication is required.

2.15 Another form of security which has to be considered by some computer users is a form of shielding to prevent eavesdropping on computers which they are operating. As was mentioned in paragraph 1.2 above, it has been shown to be possible to intercept the radiation which surrounds any computer while it is in use and to reproduce, on the interceptor's screen, the same images as are being seen by the authorised user of the computer.[1] Expensive screening is necessary to avoid this risk.[2]

2.16 Computers are, of course, subject to other risks such as fire, flood, power failures, and the like. It is not, however, necessary to dwell on these for the immediate purposes of this Memorandum.

Uses and applications of computers

2.17 Mention has been made earlier of the fact that the uses and applications of computers may be virtually limitless; and some examples of the ways in which computers may be used have already been given by way of illustration. It may, however, be helpful to set out rather more extensively some of the major uses to which computers are presently put. This may assist in an assessment of the likely scale and importance of the various activities described later in this Part of the

---

1 See Wim van Eck, Electromagnetic Radiation from Video Display Units; publ: PTT Dr Neher Laboratories, Leidschendam, Holland, 1985.

2 The British Government uses a system known as Tempest for the screening of military and defence computer installations. The details of that system are not publicly available.

Memorandum. It should be stressed that the examples which follow are no more than examples. They are certainly not a comprehensive list of all the possible uses and applications of a computer.

2.18 **Data storage and retrieval**. This is one of the simplest uses to which a computer may be put though, as mentioned earlier, the computer offers the means of easily amending or up-dating the data, as well as the means of collating and presenting the data in a variety of ways. As an example of this kind of computer operation with which many lawyers are now becoming familiar, mention may be made of legal information retrieval systems which store Acts of Parliament, law reports, and the like, and which can, for example, in response to a simple instruction provide a list of all the cases dealing with a particular legal subject-matter. Relatively simple data storage systems may also be used by, for example, travel agents in order to have ready access to timetables, or information about the availability of holidays offered by tour companies.

2.19 **Word processing**. Increasingly familiar in offices everywhere, word processors are a form of computer which can store texts that have been fed into them, make corrections, additions, and deletions, and print a fully edited version of any chosen text.

2.20 **Business uses**. In a business context a computer may be used to perform a whole range of routine operations which would otherwise require to be performed manually. It may be used for stock control, book keeping, accounting, customer invoicing, pay roll

calculation and preparation, and the like. It may also, for example, be used to make future projections on a range of activities so as to assist forward planning. Operations of the kind just described are not confined to commercial users of computers. Government departments such as the Department of Health and Social Security make extensive use of computers in connection with the calculation and payment of pensions, social security benefits, and the like.

2.21 **Banking**. Banks are now among the largest computer users. Customers' accounts are held on computers which automatically record every transaction, including those initiated by customers using cash dispensing machines. Computers can be used for the automatic clearing of cheques between different banks, or for the instantaneous transfer of funds from one bank to another or from one country to another.[3] Some banks are beginning to introduce home banking systems whereby a customer can carry out a limited range of transactions using a small computer in his own home.

2.22 **Point of sale funds transfer**. Although not yet widely available in this country, some retailers are beginning to instal computerised check-outs in stores. These will be linked to major banks and will enable the

---

3 Some of these systems are commonly known by acronyms. BACS (Bankers Automated Clearing Services) is a system used by clearing banks for the clearing of cheques. SWIFT (Society for Worldwide Interbank Financial Telecommunications) performs a somewhat similar function on a worldwide basis, connecting over 100 banks in 53 countries.

cost of a customer's purchases to be immediately debited against his bank account.

2.23 **Electronic mail.** Systems such as Prestel and British Telecom Gold provide to subscribers an electronic system for passing messages. Messages are transmitted instantaneously and will be stored in a "mail box" until the recipient subscriber reads them through the medium of his own terminal.

2.24 **Robotics.** Many manufacturing processes, particularly of a repetitive kind, are now performed by robots which in turn are controlled by computers.

2.25 **Medical treatment.** Apart from storing and processing patients' records computers can also be used directly in connection with treatment. For example a computer may measure and apply the appropriate dosage of radiotherapy to a cancer patient.

2.26 **Research and development.** Computers are widely used in a whole range of research and development activities from pure scientific research to advanced product design.

2.27 **Defence systems and forms of transport.** Many of the sophisticated defence systems which the world knows today are dependent on computers in very large measure. This is so not only in relation to the analysis of intelligence but also in relation to the control and guidance of many forms of weapons. In addition many forms of transport - ships, aircraft and spacecraft - are

increasingly dependent on computers for their operation and control.

The possibilities for misuse

2.28 Given the very large number of computers in use throughout the world, and given the enormous range of uses to which they can be put, it is not surprising that they are susceptible to some forms of use which may be thought to be objectionable on moral, social or economic grounds. Although there are no official classifications of computer crime or computer misuse, at least in the United Kingdom, writers on the subject[4] have identified several kinds of activity which are thought to merit concern.

2.29 For the purposes of this Memorandum it will be desirable to attempt some sort of classification of these different kinds of activity. This is, we think, essential if the adequacy of the existing law is to be properly examined. Whatever method of classification one uses, however, it is clear that to a greater or lesser extent some of the chosen categories will in fact overlap with each other. Subject to that, we think that the

---

4 See, for example, Computer Crime, Criminal Justice Resource Manual, US Department of Justice, 1979; Computer Technology and Computer Crime, Artur Solarz, for the National Swedish Council for Crime Prevention, 1981; Sieber, Gefahr und Abwehr der Computerkriminalität, Betriebs-Berater 1982, p.1433; A.R.D. Norman, Computer Insecurity, 1983; Computer Fraud and Crime Casebooks, Wong and Farquhar for BIS Applied Systems Ltd., 1983; Research Paper on Computer Misuse, Law Reform Commission of Tasmania, 1984.

different kinds of computer misuse may usefully be categorised as follows--

(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.

For the moment the foregoing categories have deliberately been expressed in rather neutral terms and without attaching to them any specific criminal labels since part of the purpose of this Memorandum is to explore the extent to which such activities may already be subject to the criminal law and, in so far as they are not, to seek views on whether, and if so how, they should be made subject to that law. We now turn to examine each of these categories in greater detail.

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

2.30 This sort of activity is most commonly engaged in by those who have some sort of legitimate access to the computer in question. For convenience, both here and later in the Memorandum, we simply use the two terms "erasure" and "falsification" but in fact we intend to embrace any sort of interference with data or programs

carried out with the given purpose. Examples are to be found in the most recent Computer Fraud Survey published by the Audit Commission for Local Authorities in England and Wales.[5]

2.31 In one case recorded in that survey[6] a sales manager fed spurious purchases invoices into his employer's accounts department for input to the computer-based purchase ledger system. The sales manager was able to authorise the opening of new supplier accounts on the purchase ledger master file, to originate purchase orders, to authorise the completion of goods received notes, and to approve invoices for payment. Cheques, automatically produced by the computer and signed using a cheque-signing machine, were sent to the fictitious suppliers' addresses created by the sales manager. The total amount involved in this case was £80,000. As can be seen the misuse of the computer in this case was no more than consequential upon the other activities being carried on by the sales manager. That, however, is not always the case.

2.32 In another case recorded by the Audit Commission[7] a cashier in a banking organisation managed to discover another cashier's password. She then waited for the innocent cashier to complete a withdrawal and leave a transaction displayed on the visual display unit (VDU), though instructions were that cashiers should

---

5 H.M.S.O. 1985.

6 Case 9, p.29.

7 Case 53, p.46.

clear the screen on completion of a transaction. She noted the details of this account and later that day effected a second withdrawal from this account and made an investment for the same amount into her own personal account, each time using the innocent cashier's password. The double transaction of course meant that the offending cashier's till still balanced. To cover her trail she backdated the effective investment date on her own account. The matter only came to light when an investor from whom an unlawful withdrawal had been made queried the balance on her account (the balance in her passbook disagreeing with that appearing on the organisation's database). At first it was assumed that there had simply been a cashier's error, but further investigations, aided by the fact that auditors had previously insisted, when the systems were developed, on the production of an audit log with all transactions timed, brought the whole affair to light.

2.33 The two foregoing examples are typical of many instances where employees have, to a greater or lesser extent, made use of their employers' computer systems in order to obtain some financial benefit for themselves. Very often the amount involved is relatively small.[8] Sometimes, however, computers can be used in order to obtain financial advantage on a much more spectacular scale. One such case which has become something of a legend is the Equity Funding case which occurred in the

---

8 In the example given in para.2.32 the amount was only £150.

USA in the early 1970s.[9] As subsequent investigations revealed, the Equity Funding Corporation of America had for years been in a very shaky financial state. It was originally formed to sell mutual funds (the American equivalent of unit trusts) and life insurance policies, the plan being that customers would buy unit trusts, borrow money against the security of these shares to purchase a life assurance policy, and then pay for the borrowed money and the life policy from the gains in the shares. Perhaps inevitably stock market prices did not make the anticipated gains and Equity Funding became short of cash. By inflating its own share values Equity Funding began to buy, with its own inflated shares or with money raised against them, genuine corporations with real cash income, trading the real assets of these subsidiaries for the worthless (but apparently valuable) securities of Equity Funding.

2.34 When income still continued to fall below what was required to support Equity Funding's fictitious share value, it began, through its insurance subsidiary, to sell some of the future income due on the life policies to co-insurance or re-insurance companies. Gradually, however, Equity Funding began to run out of genuine lives to sell to re-insurers and, to meet that problem, it resorted to inventing fictitious lives. It was at this stage that its computers began to play a central part.

2.35 Computers were used to create the details of the bogus insured lives, and all the records of these

---

9 For a full description of this case see Parker, Crime by Computer, 1976, Chap.13; and see also Norman, Computer Insecurity, 1983, p.119.

fictitious insurance policies were recorded and stored only on the computers. Accordingly, when re-insurers or others sought details of the policies and the lives that were being sold, they were supplied only with computer output, and accepted that output as evidence of the existence of the lives and of the policies.

2.36 By the time this deception was eventually uncovered 64,000 of the 97,000 policies which Equity Funding claimed to have in force were in fact bogus. Prior to that date the computers were used to record cancellations, deaths and lapses in the fictitious policies so that apparently authentic output could be produced for the actuarial department. It seems clear that, while this sort of fraud could have been perpetrated without the use of computers, it could never have been perpetrated on anything like the same scale, nor could it have been concealed for anything like such a long time. The end eventually came in 1973 when an employee, who had become suspicious, contacted the New York State Insurance Department and a Wall Street investment analyst. A snap audit was carried out; Equity Funding's share value tumbled; dealing on stock exchanges was eventually suspended; and a few days later the corporation filed a petition for bankruptcy. In the result shareholders lost $600 million and insured persons lost policies with face values of $1 billion.

(2) <u>Obtaining unauthorised access to a computer</u>

2.37 This may occur where an employee, who is not authorised to use his employer's computer, evades any physical security measures that there may be, and makes use of the computer facility. It may also occur as a

result of a form of wire tapping where communications between computers can be intercepted in transit. These can be recorded on a tape or disc and subsequently displayed at leisure on the wire tapper's own computer screen. Much more commonly, however, this category of misuse is applied to those who indulge in the activity known as "hacking". This term, which originated in the USA, describes the activity whereby an organisation's computer is accessed from long range by a person who has no connection whatever with the organisation, and who certainly has no authorisation to make such access. What happens is that the hacker will have, probably, a micro-computer and an acoustic coupler or modem which enables him to link his computer to the public telecommunications network. He may also already know the computer telephone numbers of public companies or other organisations who operate computers. Alternatively he may have to guess such numbers, or discover them by trial and error. Thus equipped, he will then be able to make primary contact with one of these remote computers. At that stage he will probably be required to give some sort of identification or password before he can proceed further into the system, but again he may have prior knowledge of that, or may obtain it by guesswork. Alternatively he may have programmed his own computer to run through, in a matter of seconds, a very large number of, for example, names, or sequences of numbers or letters: with luck one of these will secure the desired entry.

2.38 Hacking is probably the activity which has generated the most media interest in recent years, and it has provided the basis for at least one film in which several young people were shown hacking their way into

the US defence system computers. Certainly hacking seems to be a widespread activity, and some hackers maintain their own computerised "bulletin boards" by means of which they can exchange information about telephone numbers, user IDs, passwords, and the like. But is hacking a real problem?

2.39 One writer has claimed that "hacking is a recreational and educational sport ... the process of 'getting in' is much more satisfying than what is discovered in the protected computer files".[10] This is apparently a view taken by many who see the activity as no more than an intellectual challenge, rather like solving a crossword puzzle. Not surprisingly, however, this view is rarely shared by those organisations who have been, or who may be, hacked. While most such organisations which have been identified as victims in the past have claimed that any information obtained by the hacker has only been routine or of low level security, it is not difficult to conceive of more sensitive information being obtained in some cases, and of that information being put to dubious use. Suppose, for example, that a hacker were to succeed in gaining access to an insurance company's files containing the names and addresses of persons with high value property insurance: in the wrong hands such information could be very valuable. Moreover, it seems likely that some, if not indeed most, of those who engage in the activity of hacking would regard it as morally reprehensible to break into people's homes or offices in order to inspect their contents. If so, it is not immediately clear why a

---

10 Cornwall, The Hacker's Handbook, 1985.

similar stigma should not attach to what is upon one view simply an electronic form of house-breaking.

2.40 The potential damage which can be caused by a hacker need not be measured only in economic terms. A few years ago a group of teenage hackers, known as the Milwaukee "414",[11] gained access to the computer records of, among others, the Los Alamos Nuclear Weapons Research Laboratory and the Sloan-Kettering Cancer Clinic in New York.[12] In the latter instance it appears that the perpetrators inadvertently altered patients' files controlling radiation treatment. It requires little imagination to recognise the havoc that could be caused by activities of that kind.

(3) Eavesdropping on a computer

2.41 Although the obtaining of access to a computer by means of the telecommunications network is probably the most common form of hacking, it is clear that another, and distinct, form of eavesdropping is also now possible. This occurs when, by means of suitable (and apparently quite inexpensive) equipment, the radiation field which surrounds any computer in use can be picked up from a distance with the result that whatever is displayed on the legitimate user's VDU screen will also appear on the eavesdropper's screen.[13] In this case, however, the

---

11 So called from the telephone exchange code for Milwaukee.

12 Source: American Bar Association, Report on Computer Crime, June 1984, pp.46-49.

13 See para.2.15 above.

eavesdropper cannot himself determine what data will be displayed nor, so far as we understand, is it possible for him to alter or corrupt it in any way. On the other hand, if encryption techniques are in use, and sensitive data is being typed into the computer, the eavesdropper will be able to read that data in clear since encryption normally takes place only after data has been fed into the computer.

(4) Taking of information without physical removal

2.42 Information in any intelligible form can be taken by a person who has access to it in the sense that he can commit it to memory, or can copy it down in a notebook, or can photograph it, or can record it into a tape recorder. In all of these instances the critical feature is that there need be no taking of the actual medium on which the information is recorded or stored: for this purpose the information has, in a sense, an existence of its own. Information in this sense can, of course, be taken by anyone who sees it displayed on a computer screen.

2.43 Frequently, however, information will be regarded as secret or confidential, and those with such information will not wish it to come into the hands of those who are not authorised to have knowledge of it. If the information is recorded in a conventional manner on paper, this can be achieved by placing the paper in a locked drawer or in a safe. Increasingly, however, as has been seen, information of all kinds is stored in computers and can be read off a VDU screen just as easily as it can be read off a piece of paper. However, the taking of such information is in reality no different

from the taking of information recorded by more conventional means. The security of such information can be achieved by making it accessible only to those who have been supplied with a certain password which is the electronic equivalent of a key to open the drawer or the safe. The main differences where data is stored in a computer, and is taken (perhaps by someone who has without authorisation discovered the password) are that the taking may be more likely to escape detection, and that, if the terminal being used has a printing facility, it will be possible to obtain a copy of the information speedily and easily.

(5) Unauthorised borrowing of computer discs or tapes

2.44 Thus far it has been assumed that any taking of data has occurred directly by displaying the data on a VDU screen linked to the computer where the data is stored. It would, of course, equally be possible to "borrow" a tape or a disc containing stored data or a program with a view to copying it and returning the original. Once again that is really no different from "borrowing" a piece of paper, making a photocopy, and restoring the original to the place from which it was taken. The main difference between this and the previous category of misuse is that the present one involves physical appropriation whereas in the other there is no physical thing to be taken.

(6) Making unauthorised use of computer time or facilities

2.45 This occurs when a person, normally an authorised user of a computer, uses it for a purpose of his own

which is not authorised. Once again the computer fraud survey by the Audit Commission gives some illustrative examples.

2.46 In one example[14] a supervisor used a file interrogation package to produce name and address labels for commercial organisations. These were to be used for fund raising purposes for a body which was not part of the organisation. In another example[15] an employee, who sold gramophone records in his spare time, developed software on his employer's computer to create a mailing list of records which he had for sale. The list showed the album title, the grade of the record and the price.

2.47 While these examples are relatively trivial, and are not significantly different from cases involving the use of an employer's typewriter and paper, it is not difficult to envisage cases which would be much more serious. If, for example, a computer had, at considerable cost, been programmed to carry out advanced scientific research and development work, an employer would no doubt be less than pleased if an employee were to use these facilities for his own private work.

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

2.48 This can be achieved either by an authorised user of a computer or by a hacker.[16] It may, of course,

---

14 Case 63, p.50.

15 Case 72, p.53.

16 See, for example, the Sloan-Kettering example mentioned in para.2.40 above.

occur inadvertently, but it may also be done deliberately. The main difference between this and the first category of misuse outlined above is that in this case the corruption or erasure is an end in itself and not merely an element in a fraudulent scheme.

2.49 A simple alteration of stored data is probably the most straightforward version of this activity, but more sophisticated procedures, involving tampering with a program, are not uncommon. In one case recorded by the Audit Commission[17] a programmer, prior to his resignation from the company which employed him, made an unauthorised amendment to the language parameter in the program library. This modification was post-dated and only became effective after the employee had left. The consequence of the amendment was that system error messages were thereafter displayed in French, Dutch or German rather than English.

2.50 It appears that in that case the unauthorised activity was undertaken simply as a prank, and no great harm was caused. But much more serious cases have been recorded. In one of these[18] the credit controller of a major tyre distributor had sole responsibility for setting up and maintaining his employer's computerised data files. When the company made him redundant he told the company that they would pay dearly if his severance terms were not improved. The company did not take him

---

17 Case 65, p.51.

18 Reported in Sunday Telegraph, 27 March 1983; and see Wong and Farquhar, Computer Crime Casebook, p.68.

seriously. He had, however, kept a spare set of keys and, after leaving his employment, re-entered the premises and obtained access to the computer. He then destroyed the record of all invoices (relating to some £1 1/4 million of goods) and planted "logic bombs"[19] within the wages and other systems. It required two weeks' work to list all the invoices by hand, and to sort out the problems; and a considerable amount of chaos was caused.

2.51 Although logic bombs are often the weapons used by those who wish to sabotage a computer system out of malice or ill-will, it appears that they are sometimes used for what might be regarded as legitimate commercial reasons. Mention was made earlier in this Memorandum[20] of the fact that, although large computer users may write their own programs, many users rely on off-the-shelf programs prepared by commercial software houses. Sometimes such programs will be purchased outright, but often they will simply be leased, possibly on a year-to-year basis. It appears that, in order to ensure prompt payment of the rent, some software houses place logic bombs in their leased programs which, on an appointed date, will cause the programs to cease to function if the rent is not paid.

---

19 "Logic bombs" is the popular name given to corruption of a program the effect of which is, at some future date, to cause a system to malfunction or even to cease to operate completely.

20 para.2.8.

(8) Denial of access to authorised users

2.52 With so much reliance currently being placed on computer systems for all sorts of activity, it is evident that any denial of access to these systems on the part of authorised users could be an event of major importance. Such access could be denied in a number of ways.

2.53 It could, of course, be achieved by purely physical means, as by cutting off a power supply, or cutting a telephone wire. Apparently, however, there are also some electronic means whereby an unauthorised person, using a variety of hacking technique, can in effect cut in on an authorised user who is starting to make contact with the computer, and thereafter deny him access for so long as the hacker remains on line.

2.54 It is also to be noted, of course, that authorised users can themselves deny their employers the use of their computer, notably by a withdrawal of labour. It is unlikely, however, that this would be thought to be a fit subject for the criminal law.

Explanations for incidents of misuse

2.55 Why do incidents like those described in the preceding paragraphs occur? There can be a variety of possible explanations. Sometimes security measures for controlling access to a computer may be inadequate, or may not be conscientiously enforced. Within an organisation there may be insufficient precautions to deny physical access to computers by those who are not authorised to use them: for example, computer rooms may be unlocked or inadequately supervised. At an electronic

level insufficient attention may be given, firstly, to devising appropriate levels of password security, thus making life easy for hackers and other unauthorised users, and, secondly, to maintaining the confidentiality of such security measures as there are. On a purely organisational level insufficient attention may be paid to good management techniques or to internal audit controls.

2.56 Of course, effective security measures are likely to be expensive. To take but one example a private telecommunications line will cost more than using the public telecommunications system. Security measures may also be time-consuming and unpopular with staff. Consequently every computer user will have to balance the cost and inconvenience of improved security measures against the amount of loss or damage which he is likely to suffer by not taking them. While it is probably true that no computer system can ever be made totally secure, it seems clear from the vast number of books, articles and reports on the subject that a considerable number of computer users have failed to get the balance right. But just how serious is the problem of computer misuse, and how important is it that the law should be able to deal adequately with those who engage in such activity?

The extent of computer misuse

2.57 As was mentioned in paragraph 1.2 of this Memorandum the news media frequently suggest that the financial losses caused by computer misuse are of awesome proportions. Mention has been made of the report in The Times of 14 March 1985 that computer fraud is costing

companies £2 million a day. A number of professional surveys have painted an equally gloomy picture. Some years ago a survey conducted by the Stanford Research Institute in California estimated that the annual cost of computer misuse in the United States was 300 million dollars. More recently the American Bar Association, which has been campaigning for federal computer crime legislation in the USA, conducted a survey of its own. The report[21] on that survey claims that, among those who responded and reported losses attributable to computer crime, the average loss ranged between two million to over ten million dollars per year. The report goes on to state:[22]

> "Given the small number of organizations reporting these large known and verifiable annual losses (total and per respondent), the total annual loss figures nationwide would appear to be enormous."

2.58 Some preliminary words of caution are, we think, desirable in respect of reports of the kind mentioned in the previous paragraph. Most importantly, perhaps, since "computer crime" and "computer fraud" are terms which have no legal significance, at least in the United Kingdom, it would be helpful to know precisely what sort of activities newspaper reporters and others have in mind when they use such words. It seems at least possible that in some cases they may be referring to activities which simply have some kind of connection with a computer, however remote. Thus, the passing of a stolen

---

21 Report on Computer Crime, American Bar Association, June 1984.

22 p.38.

cheque to pay for goods might be classed as a computer crime or a computer fraud simply because in due course the cheque will be processed through a bank's computer system for payment. So too, if a fire is deliberately started in a computer room, that may be classed as a computer crime by some writers though, of course, the legal nature of the act, namely fire-raising, would be no different if the contents of the room had been simply desks and tables.

2.59 Criticisms on this score, as well as on the basis that much of its research data was derived from no more than newspaper reports, have been levelled[23] at the study carried out by the Stanford Research Institute. In turn the survey carried out by the American Bar Association has been characterised as "criminologically rather naive" by Martin Wasik of Manchester University.[24] Wasik points out that the ABA survey elicited only a 28 per cent response from those approached, and so may not be representative of the country as a whole. He goes on to observe that an average figure of loss may be rather misleading since in the great majority of cases the actual loss is comparatively small while in a few cases each year it is massive. This, of course, has a distorting effect on any average figure.

2.60 Another problem about estimating the scale of computer misuse by reference to financial loss is that in

---

23 J.K. Taber, "A Survey of Computer Crime Studies", Computer Law Journal, 1980, Vol.II, p.275.

24 "Surveying Computer Crime", Computer Law and Practice, March/April 1985, p.110, at p.113.

some cases such an exercise may be quite impossible and in others it may produce quite unreliable results. If a computer system is accessed by a hacker who simply reads some of the data which he discovers there, it may not be possible to say that any loss has occurred thereby, far less to put a figure on it. And if, say, a software system has been corrupted, or data has been falsified or erased, it may be difficult to put any accurate figure on the loss which this has caused. Probably in such a case any loss should be calculated by reference to the time and expense involved in putting matters right, but there may be a tendency in some cases to express such loss by reference to the face value of, say, the data involved. Thus, for example, some writers might designate as a "£1 1/4 million pound computer crime" the incident described in paragraph 2.50 above when in fact that sum represented no more than the face value of the invoices which were erased from the computer's stored data.

2.61 So far as the United Kingdom is concerned the most authoritative survey relating to computer misuse is probably the Computer Fraud Survey[25] produced by the Audit Commission for Local Authorities in England and Wales, to which some reference has already been made in this Memorandum. The authors of that survey extended an invitation to participate to local authorities in England, Wales and Scotland, to health authorities, to a number of Government departments, and to commercial organisations in a variety of fields such as manufacturing, retailing, distribution, construction,

---

25 H.M.S.O. 1985.

catering, finance, and leisure and travel. 943 replies were received which represented a 55% response rate.

2.62 Recognising the difficulties of definition to which reference has just been made, the Audit Commission defined computer fraud as "any fraudulent behaviour connected with computerisation by which someone intends to gain dishonest advantage". In settling on that definition the Commission acknowledged that there may be a narrow dividing line between frauds which could only have occurred because of the involvement of a computer, and frauds where the computer played a lesser, though not insignificant, part. Since the Audit Commission's purpose in conducting its survey was not to examine the need for law reform but rather to draw to the attention of commercial and other organisations that the involvement of computers in business "may have introduced an additional risk of financial loss", the chosen definition was of necessity somewhat wide.

2.63 Standing the stories circulated by the news media, and the figures suggested by the American surveys mentioned earlier, the results of the Audit Commission's survey are quite revealing. Of the 943 replies received 92% said they had not suffered a computer fraud in the last five years. Of the 77 cases of computer fraud which were notified, 13 had no financial loss ascribed to them, and the total loss relating to the remaining cases amounted to £1,133,487. The highest individual losses (of which there were three) averaged just over £200,000.

2.64 These figures are of course significantly lower than might have been expected on the basis of press and other survey reports. It has to be borne in mind, however, that even with a guarantee of anonymity (which was given by the Audit Commission) some organisations may, for commercial reasons, prefer not to disclose any losses which they have suffered. The Commission itself acknowledges that "evidence of the full extent of the scale of the subject cannot be readily determined. The evidence by its very nature can only relate to reported cases which must be less than the total number of discovered cases which by inference must also be less than the total number of fraudulent acts committed". The Commission went on to urge that "the lack of published evidence should not be regarded as the excuse for failing to initiate and maintain adequate precautions".

2.65 So far as the detail of the Audit Commission's survey is concerned, perhaps the most striking feature is that almost all of the reported frauds were perpetrated by employees or ex-employees of the organisations concerned; and certainly none seem to have been perpetrated by hackers. Moreover, no less than 58 of the 77 reported frauds were what are described as "input frauds", that is to say frauds involving the unauthorised submission and alteration of data. Few of these required any particularly sophisticated manipulation of computer procedures but rather took advantage of weaknesses in fairly basic control procedures, encouraged perhaps by the knowledge that false data held in a computer may be much more difficult to detect than information which is recorded and stored by more conventional means.

Conclusion

2.66 In this Part of the Memorandum we have endeavoured to describe in relatively simple terms the possibly undesirable activities in which computers can play a part, and we have given some indication of the possible consequences which some of these activities may produce, particularly in terms of financial loss. What we have not tried to do so far is to consider the legal implications of such activities so far as the criminal law is concerned. We attempt that task in the next part of the Memorandum.

PART III - THE SUITABILITY OF EXISTING CRIMINAL LAW

3.1 In this Part of the Memorandum we shall examine those parts of the existing law which seem to be relevant in an attempt to see whether, and if so in what circumstances, they may be able to deal with the various types of misuse in question. For this purpose it will be convenient to examine the law by reference to each of the categories of misuse identified in Part II of the Memorandum.

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

(a) Fraud

3.2 Clearly the crime of fraud is the one which is most immediately relevant to this sort of activity. According to Macdonald[1] fraud "involves a false pretence made dishonestly in order to bring about some definite practical result". Applying this definition it seems clear that at least some of the examples given in Part II of this Memorandum, together with some of the other examples to be found in, for example, the Audit Commission Survey, would amount to the crime of fraud in Scotland. If a person supplies false written, or oral, information to a computer operative so that he will feed that information into a computer which will in turn record, for example, a higher level of salary than the first person is entitled to, there will have been a false pretence followed by a definite practical result, and the crime of fraud will have been committed.

---

1 Criminal Law of Scotland (5th ed.), p.52.

3.3 Indeed, in the example just given the fraud would probably be complete as soon as the false information was fed into the computer by the data processor. That in itself would be a sufficient practical result even if the next step of actually processing that data and producing the false salary level did not occur. And, if the pretence were to be discovered before the false information was ever fed into the computer, the making of the pretence might of itself amount to attempted fraud.

3.4 Similarly a fraud would probably be committed if the perpetrator himself fed the false data into the computer intending that another, say a wages clerk, would thereafter act upon that data and prepare an inflated salary cheque. That example and the preceding one, however, both share this common feature, namely that in both cases the false pretence was made, whether directly or indirectly, to another person. But that feature need not be present in all cases. Even in a case of simple salary inflation there may be no human intervention between the perpetrator and the final result. In other words the perpetrator may simply supply the false data to the computer himself, and thereafter the computer itself may carry out all the subsequent processes including, finally, the issue of the inflated salary cheque. In such a case the question is: Can there be a false pretence when the pretence has been made only to the computer, and when no person has acted upon it?

3.5 So far as we have been able to discover the courts in Scotland have not yet been asked to answer this question. The closest analogy of which we are aware

occurs in cases where a person, by the use of a stolen banker's card, obtains cash from an automated cash dispenser. On one view such a person obtains the cash by means of the false pretence that he is the person authorised to use the banker's card, that pretence being made to the dispenser, or to the computer which controls it. However the interesting questions to which this approach could give rise have not had to be addressed by the courts since such cases have been successfully prosecuted as theft.

3.6 Some attention has been given to the problem in England. The Theft Acts of 1968 and 1978 contain a number of offences relating to the obtaining of property or services by deception. Section 15(4) of the 1968 Act defines "deception" as meaning:

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

3.7 The courts in England have held in a number of cases that offences of deception require some person to be deceived. In D.P.P. v. Ray[2] (which was admittedly not a case involving a computer or any other sort of machine) Lord Morris said[3] that "for a deception to take place there must be some person or persons who will have been deceived". More recently, in the unreported case of

---

2 [1973] 3 All E.R. 131.

3 at p.137.

R. v. Moritz[4] it was held that deception requires a human mind to be deceived, and that, given the computer assisted nature of the processing of VAT returns, there was in that case no satisfactory evidence to put to a jury that an admittedly false VAT return, which had secured unwarranted repayments, had "deceived" in the required sense.[5]

3.8 It may be arguable that "deception", as used in English legislation and interpreted by the English courts, is different from "false pretence", as used in the common law of Scotland. Such a difference was suggested by the Criminal Law Revision Committee, whose Eighth Report, "Theft and Related Offences",[6] formed the basis for the 1968 Theft Act. Prior to the passing of that Act, English law used the words "false pretence" by virtue of their appearing in section 32(1) of the Larceny Act 1916. In recommending the replacement of these words by the word "deception" the Criminal Law Revision Committee suggested[7] that the new word has "the advantage of directing attention to the effect that the offender deliberately produced on the mind of the person deceived,

---

4 (1981) unrptd, referred to in Report of the Committee on Enforcement Powers of the Revenue Departments, Vol.2, 18.3.17.

5 Generally on this matter, see Smith, "Some Comments on Deceiving a Machine", (1972) 69 Law Soc. Gaz. 576; see also R v. Laverty [1970] All E.R. 432; R v. Royle [1971] 3 All E.R. 1359; R. v. Kovacs, [1974] 1 All E.R. 1236.

6 1966, Cmnd.2977.

7 para.87.

whereas 'false pretence' makes one think of what exactly the offender did in order to deceive".

3.9 The foregoing distinction suggests that, while the English courts have been correct in holding that "deception" requires a human mind to be deceived, "false pretence" does not involve any such requirement since the latter words are merely descriptive of what someone has done. We are disposed to accept that distinction as valid and to conclude that the use of a computer would not present problems for the Scots law of fraud, even in cases where it could not be said that a human mind had been deceived. In many such cases, of course, even if a charge of fraud were thought to present problems, a charge of theft would be available, at least where the end result was the obtaining of some tangible benefit such as money.

(b) Uttering

3.10 According to Macdonald[8] the crime of uttering "consists in uttering as genuine writings known by the utterer to be forged". This definition presents an immediate difficulty as to whether false data fed into, or stored in, a computer could ever be a "writing" for this purpose. Leaving that difficulty aside for the moment, the crime of uttering appears at first sight to offer certain advantages in the present context since the crime is complete when the writing is dishonestly used towards the prejudice of some person, but "it is not necessary that any person should actually have been injured, or that any definite practical result should

---

8 p.59.

have been attained, by the use".[9] This appears to suggest that the crime of uttering might be appropriate in some cases if it were thought that a charge of fraud or attempted fraud could be frustrated by the absence of any human mind to be deceived.

3.11 Macdonald goes on, however, to say:[10]

> "Only those writings which bear to be authenticated by some person can become the subject matter of a charge of uttering .... The essence of uttering is that it involves a false pretence as to the genuineness of the signatures .... If there is no false representation in that respect, then however untrue may be the statements contained in the document, it cannot become the subject matter of a charge of uttering ...."

3.12 The crime, then, applies only in the case of a very limited class of documents and, whether computer input can be regarded as "writing" or not, it seems likely, at least for the present, that it will not consist of something which bears a signature. It is doubtful, therefore, that uttering would be relevant to the kinds of activity with which we are presently concerned.

3.13 It may be worth noting here that the English equivalent of uttering is to be found in sections 1 and 3 of the Forgery and Counterfeiting Act 1981, though these sections take a very different approach from the Scots

---

9 Macdonald, ibid.

10 Ibid.

common law, and are, in some respects, similar to the Scots crime of fraud. The sections provide:

> "1. A person is guilty of forgery if he makes a false instrument, with the intention that he or another shall use it to induce somebody to accept it as genuine, and by reason of so accepting it to do or not to do some act to his own or any other person's prejudice.
>
> 3. It is an offence for a person to use an instrument which is, and which he knows or believes to be, false, with the intention of inducing somebody to accept it as genuine, and by reason of so accepting it to do or not to do some act to his own or any other person's prejudice."

"Instrument" is defined[11] as meaning, inter alia, "any disc, tape, sound track or other device on or in which information is recorded or stored by mechanical, electronic or other means". Although we are not competent to express a firm view on a matter of English law, these provisions appear to avoid some of the restrictions which attach to the Scots crime of uttering. Moreover, section 10(3) of the 1981 Act provides:

> "In this part of this Act references to inducing somebody to accept a false instrument as genuine ... include references to inducing a machine to respond to the instrument ... as if it were a genuine instrument ...."

This provision would appear to meet some of the possible problems which we have already discussed in relation to "deception" and "false pretence". We understand that sections 1 and 3 of the 1981 Act have recently been invoked in England in the prosecution of persons who are alleged to have obtained access to a computer system by

---

11 s.8(1).

the use of false identifications. The outcome of these proceedings is not yet known.

(c) Embezzlement

3.14 Embezzlement, again according to Macdonald,[12] is "the felonious appropriation of property which is in the possession of the offender as trustee, agent, factor or other administrator". It is embezzlement "where what is appropriated is an amount for which [the offender] is ... bound to account".

3.15 So defined, embezzlement would possibly be an appropriate crime with which to charge, for example, the deviant bank cashier mentioned in paragraph 2.32 of this Memorandum. However, a central feature of the crime of embezzlement is that the person who feloniously appropriates the funds in question must have been in a position of trust in respect of them. It may be doubtful if the crime would be appropriate for a case where a person, albeit an employee, falsified data so as to acquire some of his employer's funds, where he himself exercised no fiduciary function in respect of any of these funds. Such behaviour would be either fraud or theft.

3.16 The precise borderline between theft, fraud and embezzlement - and indeed uttering - is not always easy to draw.[13] We do not think, however, that it is

---

12 p.45.

13 See, e.g. the analysis of embezzlement in Gordon, Criminal Law, (2nd ed.), Chap.17.

necessary for our present purposes to explore that topic. Our present purpose is simply to determine, in relation to cases involving the erasure or falsification of data or programs so as to obtain a pecuniary or other advantage, whether the existing law is adequate to deal with all the computer-related cases that could arise. Our conclusion is that, existing Scots law, with its inherent flexibility, should provide a satisfactory solution to such cases.

(2) Obtaining unauthorised access to a computer

3.17 As was observed earlier in this Memorandum[14] a person may obtain unauthorised access to a computer in any one of several ways. Although an employee of a computer owner, he may not be authorised to have access to the computer, but may do so without permission. If not connected with the computer owner in any way, he may gain access to the computer by physically breaking into the premises where the computer is kept. He may obtain access to computer transmissions by means of an unauthorised wire tap. Lastly, he may be a hacker, that is to say he may obtain unauthorised access to a computer by electronic means through the medium of a remote telecommunications link. It is, of course, the last of these methods which has attracted the greatest interest in recent times.

3.18 Although for the moment we are looking at the problems associated with unauthorised access on their

---

14 para.2.37 above.

own, it is as well to bear in mind that some form of unauthorised access may precede many of the other activities with which we are concerned, for example, the falsification of data, the taking of information, and the unauthorised use of computer time and facilities. Accordingly, unauthorised accessing may well be seen as a subject which merits particular attention when we come to consider possible reform of our criminal law.

3.19 This may be particularly so since, so far as we can see, the sorts of activity in question would not, with one possible exception, contravene our existing criminal law. So far as the common law is concerned this is not altogether surprising since that law, in the main, developed in a pre-computer age. Certainly housebreaking is known as an element in that law, and so might be thought to be appropriate for a case where an outsider breaks into the premises where a computer is kept by physical means. But housebreaking is not a crime by itself. It acquires a criminal character only when it occurs with intent to steal, or when it is an aggravation of a completed theft.

3.20 There are several statutory provisions which are, or could be, related to the obtaining of unauthorised access to a computer, but only one of them appears to deal with that matter directly. For example, the eighth Data Protection Principle set out in Schedule 1 to the Data Protection Act 1984 requires of certain data users that "appropriate security measures shall be taken against unauthorised access to ... personal data". The Data Protection Act does not, however, contain any provision affecting those who, obtain, or attempt to

obtain, unauthorised access to such data, whether protected by appropriate security measures or not.

3.21 The one possible exception to which we referred above is the Interception of Communications Act 1985. Section 1(1) of that statute provides:

> "... a person who intentionally intercepts a communication in the course of its transmission ... by means of a public telecommunication system shall be guilty of an offence....

The word "communication" is not defined in the statute and we can see no reason why it should not include a communication between computers as well as a purely oral communication between humans using conventional telephones. Accordingly, it seems to us that this offence would be appropriate in certain circumstances where a computer communication was intercepted by tapping the line down which the communication was passing. However, that would be so only where the line in question formed part of a public telecommunication system: it would not be so if the line was a private one. Moreover, the 1985 Act would not, in our view, catch the conventional hacker since, although making use of a public telecommunication system, he would be initiating rather than intercepting a communication.

3.22 If unauthorised access is taken by one who is an employee of the computer owner, then of course he can be made subject to internal sanctions, including possibly dismissal from his employment; but these remedies would not be available where the person concerned was an outsider. It is perhaps worth observing that the criminal law is capable of dealing with certain invasions

of privacy. If someone who has no right to do so peers through another's curtains in order to observe what is taking place within, he may be guilty of a breach of the peace. In such a case, however, the criminality of the behaviour will arise because of the alarm which it is likely to cause, and not because the offender might thereby, for example, be gaining access to secret information. Despite its great flexibility, we do not see the crime of breach of the peace as providing an answer to the activity of obtaining unauthorised access to a computer. Our view on the whole matter is that at present, and apart from the limited remedy provided by the Interception of Communications Act 1985, our criminal law contains no provision which is appropriate for such activity.

(3) Eavesdropping on a computer

3.23 Although somewhat similar in character to certain forms of hacking, eavesdropping on the contents of a computer screen is different in that it involves no physical or electronic contact between the eavesdropper and the computer in question. As has been shown elsewhere in this Memorandum it occurs from a distance when the electro-magnetic radiation surrounding a computer screen is picked up by a television receiver. In a sense this sort of activity is no different from reading the contents of a person's papers by the use of a powerful telescope, and in legal terms we suspect that the position is the same in both cases. That is to say that the conduct in question might amount to a breach of the peace, on the analogy of peeping between a person's curtains, if it were of a kind that caused, or was likely

to cause alarm. Since, however, the kind of conduct which we are presently considering will often be carried on at a considerable distance,[15] and in circumstances which may be undetectable by the computer user, we doubt whether the crime of breach of the peace will often be appropriate. If that is right, it is our view that there is no other offence that would be appropriate for such activity.

(4) Taking of information without physical removal

3.24 Information can be "taken" or "obtained" (to use, for the present, rather neutral words) in a variety of ways. A person who reads a textbook obtains information by doing so. In the same way a person who reads data displayed on a computer screen obtains information, and does so regardless of whether he is an unauthorised hacker or a person authorised to have access to that data. By somewhat different means information can be obtained by a person who takes, albeit temporarily, a tape or a disc or, for that matter, a piece of paper on which information is stored or recorded, and who thereafter reads the information concerned. The question in such cases is whether the obtaining of that information is in any circumstances a crime. Later in this Memorandum[16] we shall consider the position where an article containing information is taken for a limited period. For the present we consider the position of information by itself.

---

15 We understand that the kind of eavesdropping presently under consideration can occur up to several miles distant from the target computer.

16 para.3.34 et seq.

3.25 Since its earliest days Scots law has recognised the existence of incorporeal property, that is to say property which has no physical substance.[17] Examples commonly given in the textbooks include decrees of court, rights under contract, some rights in security, and various rights under wills and trusts. The absence of any physical substance means that incorporeal property cannot be possessed: it exists only in the form of rights or claims. These rights or claims can be disposed of but only in prescribed ways, normally by assignation or by transmission on death.

3.26 At first sight information is quite different from the kinds of property that have just been given as examples of incorporeal property. It is neither a right nor a claim. Moreover, it does not exist, as do such rights and claims, by virtue of some sort of relationship between the owner of the incorporeal property and the person against whom the right or claim can be exercised. In a sense it can be said that information has an existence of its own, and can be, and frequently is, shared by a great many people quite independently of each other.

3.27 On the other hand, information can in certain circumstances have a degree of uniqueness attaching to the totality of the information rather than to its component parts. A list of AB's customers is unique not because of the individual names on it, any of which could probably be found by consulting a telephone directory,

---

17 Erskine, II,2,7; Bell, Comm.I, 100; Prin. paras.1338 and 1476-1505.

but because, taken as a whole, it discloses specialised information about AB's business activities. Moreover information can have value, and can be sold. At a fairly basic level it is commonplace today for certain organisations to sell lists of customers or subscribers to other organisations who may be seeking a potential market for their own product. In such cases it is not just pieces of paper which are being purchased but the information which they contain. At a more sophisticated level agreements for the sale or exchange of manufacturing "know how" are far from uncommon.

3.28 All of this tempts one to say that, if information can, at least when assembled in a certain way, have a unique existence of its own, and if it can be bought and sold, then surely it should attract some sort of right of property. In the context of the civil law, however, Professor Walker says:[18]

> "No exclusive or proprietary right is, however, legally recognised in trade secrets as such, except in so far as they are the subject of trade marks, patents, registered designs, copyright, or plant breeders' rights, and there is no appropriation of property by discovering or annexing or publishing another's trade secrets."

3.29 If the civil law had recognised information as being something which could, even in certain circumstances, attract proprietary rights, then it seems likely that the law relating to trade secrets, which we

---

18 Principles of Scottish Private Law (3rd ed.) Vol.III, p.526.

describe briefly later,[19] would have developed rather differently.[20]

3.30 We think that it is clear that, if no proprietary right in information is recognised by the civil law, then no such right can be recognised by the criminal law. Hume, commenting on the case of Dewar[21], where an apprentice was charged with taking a book of recipes in order to copy them, observes[22] that the apprentice took the papers "at first with the intention to detain them; and if, caught with them in his possession, he could not well have pleaded that there was not a complete theft in the case". Hume continues, however:

> "On the other side, it may be observed, that still the main substance of theft is wanting in such a case, viz. the owner's loss of the corpus in question, the possession, use and disposal thereof: that he suffers only in a certain abatement of the value of his subject; and the offender appropriates only a sort of incorporeal right or privilege, which is not the subject of theft." (our emphasis)

We are not aware that Scots law on this matter is any different today from what it was in the time of Hume.

---

19 paras.3.88 to 3.90.

20 It appears that no right of property in information is recognised by English law either: see, e.g., Phipps v. Boardman, [1966] 3 W.L.R. 1009, per Lord Upjohn at 1070; Malone v. Commissioner of Police of the Metropolis (No.2), [1979] 2 All E.R. 620, per Megarry V.-C. at 630.

21 (1777) Burnett, 115, described in greater detail in para.3.38 below.

22 i.75.

As Gordon has put it,[23] "there must in theft be a 'thing' to which one can point and say 'That is what A stole'".

3.31 The non-recognition by the criminal law of information as an object of theft is not confined to Scots law but is also to be found in some continental systems and in English law. The leading English case on that matter is Oxford v. Moss.[24]

3.32 In that case an undergraduate at Liverpool University dishonestly obtained the proof of an examination paper for an examination which he was due to take some months later. He returned the paper after he had read its contents. He was charged with the theft of confidential information, contrary to section 1 of the Theft Act 1968, it being asserted by the prosecutor that the confidential information was intangible property within the meaning of section 4(1) of the Act. The prosecution was dismissed at first instance, a decision which was upheld by the Divisional Court on appeal, it being held that confidential information is not "property" for the purposes of the 1968 Act. In a commentary on the case[24] Professor Smith suggests that the prosecutor might have fared better had he concentrated on the theft of the paper rather than the information, and had he prayed in aid section 6(1) of the 1968 Act which deals expressly with "borrowing". That view may, however, be open to question now standing a

---

23 para.14-29.

24 (1979) 68 Cr. App. Rep. 183; and see commentary by Professor J.C. Smith in [1979] Crim.L.R. 119.

recent decision of the Court of Appeal in relation to the temporary borrowing of films for the purpose of copying them.[25]

3.33 As we see it there are two main difficulties about treating the taking of information as theft. One involves the question whether information is truly property at all. The other involves the question whether, even supposing that information can be classed as property, there is any deprivation of that property when information is merely committed to the mind of another. In such a case the "owner" of the information still has it, to do with as he wishes. All that he has lost is a particular advantage attaching to the information, namely its exclusive character. That loss may have considerable financial consequences for him, but it is not the same as the loss of the information itself. We therefore conclude that Scots criminal law, probably like English law, does not penalise the taking of information as distinct from the taking of that on or in which the information is stored or recorded.

(5) Unauthorised borrowing of computer discs or tapes

3.34 Apart from the situation which we have just been considering, where information in the pure sense has been taken or obtained, information may also be obtained as the result of the physical taking, albeit for a limited period, of that on or in which the information is recorded or stored. Subsequent to any such article being taken the information concerned can be read, and perhaps

---

25 R. v. Lloyd and Others, [1985] 2 All E.R. 661; and see para.3.49 below.

even copied, at leisure. If the article in question is taken with the intention of depriving the owner permanently of it, there is no doubt that such a taking would amount to the crime of theft; and in such a case the nature of the contents of the article might have an effect on sentence. But the question is whether the mere temporary taking, or borrowing, of such an article can be treated as theft under Scots law.

3.35 So far as we can judge several slightly different, though to an extent overlapping, lines of development have occurred in Scots law in relation to this problem. These lines involve, first, cases where the temporary removal or retention of an article have been in issue; second, cases where an article has been taken and used; and third, cases where some element of breach of trust has been involved. Each of these will be examined in turn.

(a) Temporary removal of articles

3.36 According to Macdonald:[26]

> "It is no defence to a charge of theft that the person charged had no intention of totally depriving the owner of the article. The crime is properly one of theft if the owner of property is clandestinely deprived of possession of it even although the deprivation be temporary, and so the taking of a book to copy its contents for an illegitimate purpose was held to be theft, although there might be no intention to retain the book."

3.37 If accurate, that passage would provide authority for the view that if, say, a computer tape were

---

26 p.20.

taken for a few hours so that its contents could be copied, and was then replaced, the person concerned would have committed the crime of theft. However, the passage in question has been challenged by Gordon[27] who doubts whether it is supported by the authorities on which Macdonald relies.[28]

3.38 In Dewar an apprentice at a printing works broke into his master's office, carried off a book containing recipes for mixing colours, had them copied, and returned the book. He was indicted for theft and housebreaking and particularly for "the feloniously carrying away [a man's] pocket book, and papers containing the secret knowledge whereby he carries on a valuable part of his trade, and the fraudulently copying such papers ... to the prejudice of the proprietor thereof". After a debate on relevancy the court pronounced an interlocutor finding the libel relevant to infer an arbitrary punishment. Burnett[29] construes this as meaning that "the Court did not hold this as a proper theft, the paper having been fraudulently abstracted with a view merely to take a copy of it and then to return it".

3.39 Dealing with the same case Hume[30] is a little ambivalent, and seems uncertain whether the facts

---

27 para.14-72 et seq.

28 Dewar, (1777) Burnett, 115; Hume, i.75; John Deuchars, (1834) Bell's Notes 20; H.M.A. v. Mackenzies, (1913) 7 Adam 189.

29 supra.

30 In the passage quoted in para.3.30 above.

amounted to theft or not. Alison,[31] when he came to consider the case of Dewar, does not seem to have entertained any doubts. He says that "the Court ... did not consider this as a case of proper theft ... but they held it an irregular and punishable act".

3.40 The case of John Deuchars[32] is of less assistance. The facts were similar to those in Dewar, but with two differences: the book was still in the accused's possession at the time of his arrest, and, on being charged, he tendered a plea of guilty. As Gordon suggests,[33] it may be that, since he still had possession at the time of his arrest, his advisers may have felt that it would be impossible to redargue the factual presumption of theftuous intent. Such a view would be consistent with what was said by Hume in the passage referred to above.

3.41 The case of Mackenzies[34] was rather more complex. An employee of a chemical manufacturer was charged with stealing a book containing recipes of value relative to secret processes. He was also, but in a separate charge, charged with making copies of the recipes in the book with intent to dispose of them for valuable consideration. For the present the point of interest is that the first charge, while clearly relevant simply as a charge of theft of a book, provoked several comments,

---

31 i.271.

32 supra.

33 para.14-31.

34 supra.

albeit obiter, from the court on the question whether taking for a limited purpose can be theft.

3.42 In particular the Lord Justice Clerk said:[35]

> "The indictment seems to hint at the book having been taken, not to appropriate the actual article itself, but in order to obtain the opportunity of copying part of its contents for an illegitimate purpose. That such a taking, although there is no intention to retain the article, may be theft, is, I think, clear. The article is taken from its owner for a serious purpose of obtaining something of value through the possession of it."

No authority is cited in support of these propositions but, since the Lord Justice Clerk at the time was Lord Macdonald, the author of the textbook on criminal law, it may be that he was relying on the views in that book which bear to be supported by the authority of Dewar and Deuchars.

3.43 Had the matter rested simply on the authority of the three cases already mentioned, one might fairly have said that the question whether temporary appropriation can, in Scots law, amount to theft was, at best, not free from uncertainty. However, a series of recent cases suggests that the views of Lord Justice Clerk Macdonald are gaining acceptance.

3.44 In Herron v. Best,[36] which was the first of these cases, the tide seemed to be going the other way. In that case a mechanic received a bad cheque in payment

---

35 at p.194.

36 1976 S.L.T. (Sh.Ct.) 80.

of work done by him on a van which he had handed back to the owner on receipt of the cheque. When he discovered that the cheque was bad, he took the van back. Having reviewed the authorities, including Mackenzies, Sheriff Macphail concluded that an intention to deprive permanently is crucial to the crime of theft, and acquitted the accused.

3.45 In Milne v. Tudhope,[37] on the other hand, the outcome was different. In that case a builder, who was carrying out work on a house on a fixed price contract, and who had received payment of that price, refused to carry out remedial work unless he received further payment. The client refused whereupon the builder removed doors, radiators, and other parts from the house. He told the client that he would return them if he received more money. He was convicted of theft, and the conviction was sustained on appeal. In delivering the opinion of the court the Lord Justice Clerk (Wheatley) said:[38]

> "We agree with the Sheriff's statement of the law to the effect that 'in certain exceptional cases an intention to deprive temporarily will suffice' and disagree with Sheriff Macphail that 'an intention to deprive permanently' is essential."

3.46 Unfortunately the Lord Justice Clerk did not expand on what might amount to "exceptional cases" for this purpose, though in the case in question the exceptional feature appears to have been that, as the

---

37 1981 J.C. 53.

38 at p.57.

Sheriff put it, the builder was trying to hold his client to ransom. A somewhat similar consideration was present in the later case of Kidston v. Annan[39] where a person had been given a television set to estimate the cost of repairing it. Without, as the Sheriff found, receiving any instructions he proceeded to carry out a repair, and then refused to return the set to the owner until he received payment for the repair. Remarking on the similarities between this case and Milne v. Tudhope, the High Court refused an appeal against conviction for theft. Finally mention should be made of Sandlan v. H.M.A.[40] In that case there was an allegation that stock and books had been temporarily removed from a company's premises by its director in order to prevent auditors discovering shortages. In charging the jury Lord Stewart told them[41] that, where goods are removed clandestinely, "such a taking ... aimed at achieving a nefarious purpose, constitutes theft even if the taker intends all along to return the things taken when his purpose has been achieved".

3.47 The recent trend of authority, then, clearly seems to support the view that an intention permanently to deprive the owner of the article in question is not a necessary ingredient of theft, and that, where a temporary taking is effected for a nefarious purpose, such actings will amount to theft. If one applies that proposition to the kind of activity with which we are

---

39 1984 S.C.C.R. 20.

40 1983 S.C.C.R. 71.

41 at p.83.

concerned in this Part of the Memorandum, it would appear to follow that a temporary taking of a tape or other computer-related article may amount to theft, but apparently that will be so only where, to use Lord Stewart's words, the taking is "aimed at achieving a nefarious purpose". But is the reading of the contents of a tape a "nefarious purpose"?

3.48 It is not entirely clear what these words mean, but in the context of the recent cases which have been described above they seem to mean a purpose which is unlawful in the sense of involving a form of extortion or promoting the furtherance of a fraudulent scheme. But, merely to read something which somebody else has written, or committed to a tape, is not in itself unlawful. This suggests that, in such cases, the temporary taking may not amount to theft unless it can be shown to be part of, or a preliminary to, some other activity which is itself unlawful. But this, of course, is in turn linked to the question whether the taking, or the subsequent disposal, of information is itself unlawful. In this context, of course, "unlawful" does not necessarily just mean "criminal". A given act may be unlawful in the sense of constituting a civil wrong; but whether that is what is intended by "nefarious purpose" must, we think, be uncertain. In short, we are uncertain as to whether the recent restatements of the law on temporary appropriation are necessarily apt to cover a case where the taking is merely for the purpose of reading a document, or the contents of a tape, or some similar article.

3.49 In this connection we note with interest that the Court of Appeal in England has recently held[42] it not to be theft where a film projectionist clandestinely removed films from the cinema where he worked so that they could be copied, and pirated versions thereafter marketed. The films were only out of the cinema for a few hours for this purpose, and were returned in time for advertised performances. The decision of the court in this case proceeded on a construction of section 1, and particularly section 6, of the Theft Act 1968. These statutory provisions, of course, have no counterpart in Scots law, and expressly provide, subject to a reference to borrowing in section 6, that an "intention of permanently depriving the other" is necessary for theft. The court held that the "borrowing" provision in section 6 was for exceptional cases only and that, as "the goodness, the virtue, the practical value of the films to their owners"[43] had not gone out of them, there had been no intention of permanently depriving the owners of them, and consequently no theft. Although this case proceeds, as we have observed, on a law of theft which is quite different from that in Scotland,[44] it is, we think, of interest not only as an indication of how English law tackles the matter of temporary appropriation but also as illustrating that what might be called the "reading and copying problem" can extend to many classes of articles other than those related to computers. This, we think,

---

42 R. v. Lloyd and Others, [1985] 2 All E.R. 661.

43 per Lord Lane C.J. at 667.

44 At least as explained in Milne v. Tudhope, supra.

may be of some significance when we come to consider possible reforms of the law.[45]

(b) Taking and using another's property

3.50 According to both Burnett[46] and Alison,[47] Scots law does not admit of the furtum usus vel possessionis of the Roman law. Macdonald,[48] by contrast, asserts that the crime of furtum usus is recognised by the common law. He makes this assertion solely upon the authority of Strathern v. Seaforth,[49] and it may be that he was confusing furtum usus, which strictly involves no more than the improper use of another's property, with the crime dealt with in Strathern v. Seaforth which also involves a preliminary taking of that property.

3.51 The facts of Strathern v. Seaforth are that the respondent was charged in the sheriff court that he "did ... clandestinely take possession of a motor car ... well knowing that [he] had not received permission from, and would not have obtained permission from [the owner] to [his] so doing, and did drive and use said motor car in the streets of Glasgow ...." Objection was taken to the relevancy of the complaint on the ground that the species facti libelled did not infer any crime known to the law of Scotland. The objection was sustained in the sheriff

---

45 See Parts IV and VI below.

46 p.115.

47 i.271.

48 p.20.

49 1926 J.C. 100.

court, but the Crown appeal against that decision was successful.

3.52 The argument for the respondent was essentially that furtum usus is not a crime against the law of Scotland, and that the complaint was simply an attempt to introduce such a crime. In rejecting that argument the Lord Justice Clerk (Alness) said:[50]

> "... speaking for myself, I should not have required any authority to convince me that the circumstances set out in this complaint are sufficient, if proved and unexplained, to constitute an offence against the law of Scotland."

He went on:

> "The matter may be tested by considering what the contention for the respondent involves. It plainly involves that a motor car, or for that matter any other article, may be taken from its owner, and may be retained for an indefinite time by the person who abstracts it and who may make profit out of the adventure, but that, if he intends ultimately to return it, no offence against the law of Scotland has been committed. I venture to think that, if that were so, in these days when one is familiar with the circumstances in which motor cars are openly parked in the public street, the result would be not only lamentable but absurd. I am satisfied that our common law is not so powerless as to be unable to afford a remedy in circumstances such as these."

3.53 In a concurring judgment Lord Anderson[51] identified three points which would entitle a court to convict of a crime according to the law of Scotland. He expressed these as follows:

---

50 at p.102.

51 at p.103.

"The first is that the prosecutor libels and offers to prove that possession of the motor car was taken clandestinely. This implies a certain degree of secrecy, and certainly implies that it was done without authority. The second is that this possession was taken in the knowledge that permission to take would not be granted; and the third is that, possession having thus been taken, the car was used."

3.54 Only a year later, Strathern v. Seaforth came under the scrutiny of the court in the case of Murray v. Robertson.[52] In that case the accused was a fish merchant in Ardrossan who was charged with clandestinely taking possession of a number of fish boxes belonging to other merchants and using them to transport his own fish to Glasgow. The accused's conviction was quashed on appeal. In doing so the court drew attention to the requirement of clandestinity as noted in Strathern v. Seaforth, and observed that there was no evidence of that in the present case. Indeed, there seems to have been no evidence even of a taking in the case of Murray since it appears that the boxes had simply been left by someone in the accused's yard. Founding on that fact Gordon[53] argues that it was unnecessary for the court in Murray to place reliance on the clandestine character of a taking: the case could have been decided simply on the basis that there was no evidence of a taking. Consequently, Gordon goes on to suggest that, despite Murray v. Robertson, it is a crime at common law to take and use the property of another without his consent, and that the crime is committed whether or not the taking is secretive.

---

52 1927 J.C. 1.

53 paras.15-31, 15-32.

3.55 While this is an attractive argument, it is not supported by authority and, in our view, a court, at least of first instance, would be likely to consider itself bound to apply the "clandestine" requirement which was stipulated in Strathern v. Seaforth. It is perhaps surprising that there has apparently been no need, since 1927, to reconsider the ratio of that case, but no doubt the main reason is that the particular mischief which the complaint in that case was designed to penalise has, for many years now, been the subject of express provision in road traffic legislation.[54]

3.56 Before leaving the case of Strathern v. Seaforth we should observe that some years ago, in a Consultative Memorandum on Confidential Information,[55] we expressed the view[56] that the basis of the decision in that case could be extended "to cover the case where a person surreptitiously reads a document belonging to another, without permission, and in circumstances where he knows that if permission had been asked it would not have been granted". We went on to suggest that this would be so if he not only read the document, but copied it or made notes from it. On further reflection we do not now support these views. Whatever difference of opinion may be open regarding the need for clandestinity, it seems perfectly clear that, to constitute the crime that was held to be relevant in Strathern v. Seaforth, there must at least be a taking of the article in

---

54 Now to be found in Road Traffic Act 1972, s.175.

55 Consultative Memorandum No.40, 1977.

56 at para.69.

question. Merely to read a document does not involve any taking of it, and on that ground alone we do not now consider that the criminality, or non-criminality, of such behaviour can be determined by reference to that authority.

3.57 Notwithstanding that, it appears to us that the common law crime established by Strathern v. Seaforth could have relevance to some of the computer-related activities with which we are presently concerned. On one view the clandestine taking of a tape or disc, and the subsequent reading of its contents or its use for recording data, appear to possess all the necessary elements of the offence as set out by Lord Anderson in Strathern v. Seaforth.[57] It is not clear whether the courts would follow Strathern but we consider that case to be good law which should apply in such circumstances.

(c) Breach of trust

3.58 Having observed that "breach of trust and embezzlement" is a composite name for what is now regarded as the single crime of "embezzlement", Gordon[58] goes on to say:

> "It may be possible to commit breach of trust with regard to things other than corporeal moveables or money, for example by revealing secrets imparted to one in confidence, but if such a form of breach of trust does exist it is undeveloped and virtually unformulated, except in those cases in which it comes under the category of breach of duty by public officials."

---

57 See para.3.52 above.

58 para.17-01.

3.59 Hume,[59] Burnett,[60] and Alison[61] all deal with breach of trust in contexts which we would now recognise as constituting the crimes of fraud or embezzlement, and the case referred to by Gordon in the passage quoted above seems to be the only relatively modern authority for the existence of a separate crime of breach of trust. That case is H.M.A. v. Mackenzies.[62]

3.60 We have already considered[63] the case of Mackenzies in connection with the charge of theft which was brought against the first accused. He faced a second charge, however. It was in the following terms:

> "You ... being engaged in a confidential capacity as an assistant ... in the service of [a company] and being bound by your agreement of service with them not to make known ... to anyone, so long as you remained in said service, or at any time after its termination, the secrets of your said employers, or of their manufactures, trade, or business, or of or connected with any of the processes used by them ... nevertheless did, in breach of your said agreement and obligation above set forth, and of the trust reposed by your said employers in you as their assistant, make copies ... of the recipes for the preparations ... set forth, and that with intent to dispose of said copies for valuable consideration to trade rivals of the said [company]."

3.61 This charge was dismissed as irrelevant. That decision was reached, however, upon the basis that the

---

59 i.60.

60 pp.111-113.

61 i.354-357.

62 (1913) 7 Adam 189.

63 para.3.41 above.

charge did not set forth a completed crime or an attempted crime, but only acts preparatory to the commission of a crime. Accordingly, while that case did not decide that a breach of trust involving the taking and copying of secrets for disposal and gain is not a crime, it is, in our view, far from being a convincing authority for the proposition that such behaviour is a crime. We would hesitate to suppose that a court today would happily endorse a charge of breach of trust in circumstances where, for example, a computer operator borrowed and then copied, for his own purposes, some of the data to which he quite properly had access.

(6) Making unauthorised use of computer time or facilities

3.62 Earlier in this Part of the Memorandum we considered the case of a hacker who obtains unauthorised access to a computer either for reasons of idle curiosity or in order to read the data stored in that computer. What we are now concerned with is the case where a person, having gained access (whether authorised or not), proceeds to use the computer for his own purposes. These two cases obviously overlap to a certain extent, but the distinction which we are seeking to draw may be expressed as being comparable to, on the one hand, a person who gets into a motor car simply to see what the interior looks like and, on the other hand, a person who, without authority, actually drives the car for his own purposes. Some simple examples of unauthorised use have been given in Part II of this Memorandum.[64] It was also suggested

---

64 See para.2.46.

there[65] that more significant cases could be visualised as, for example, where a computer had been programmed, at considerable cost, to carry out advanced research and development work and was used, without authority, by an employee in connection with his own private work.

3.63 An example of an attempt to invoke the criminal law in a case of this nature is to be found in the Canadian case of R. v. McLaughlin.[66] In that case a student at the University of Alberta made unauthorised use of the university's mainframe computer having gained access through a remote terminal on the university campus. The remote terminals were connected to the various components of the computer by electric wires. The student was charged with a contravention of section 287(1) of the Criminal Code which provides:

> "Every one commits theft who fraudulently, maliciously, or without colour of right, ...
>
> (b) uses any telecommunication facility or obtains any telecommunication service."

3.64 This case eventually reached the Supreme Court of Canada where the quashing of the student's conviction by the provincial Court of Appeal was upheld. Put shortly the ground of the decision was that the computer system was not a "telecommunication facility" within the meaning of the section. As Estey J. put it:[67]

---

65 para.2.47.

66 (1980) 2 S.L.R. 331; (1981) 113 D.L.R. 386.

67 113 D.L.R. at 394.

> "The Court would not be expected by Parliament to glean from words generally associated with the communications industry an intent to attach penal consequences to the unauthorised operation of a computer."

3.65 The provision in the Canadian Criminal Code which was under consideration in the case of McLaughlin may be contrasted with the comparable United Kingdom provision which is to be found in section 42 of the Telecommunications Act 1984. That provision is even more expressly directed towards dishonest use of the telecommunication system itself rather than of what may lie at the end of it. It is in the following terms:

> "A person who dishonestly obtains a service provided by means of a licensed telecommunication system with intent to avoid payment of any charge applicable to the provision of that service shall be guilty of an offence."

3.66 We have, with one exception noted below, been unable to find any provision of the criminal law, in statute or at common law, which would penalise the unauthorised use of computer time or facilities. Once again, as with unauthorised access, an employer may have contractual or other sanctions which he can use against an employee, but that is not what we are concerned with at present. The only provision of the criminal law which we have been able to find, which could be of relevance to the kind of activity presently under consideration, is the apparently established doctrine of Scots common law that electricity is something which is capable of being

stolen.[68] Accordingly it would in theory be possible to prosecute the unauthorised user of a computer with theft of the electricity which was thereby consumed. However, apart from the fact that such a charge might seem rather unrealistic as a way of dealing with the activity in question, the charge could also, we think, present some technical difficulties. Not least among these would be the question of who was the owner of the electricity involved. Was it the occupier of the premises where the computer was kept, or was it the Electricity Board who provided the supply? If it were the latter, then a charge of theft of electricity would seem even more remote and inappropriate for an incident of computer misuse.

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

3.67 Once again, as was shown by the examples given in Part II of this Memorandum,[69] this is an activity which can be perpetrated either by a person who is normally authorised to use the computer in question or by an outsider like a hacker. For the present, however, we are concerned to see whether the activity, however perpetrated, is subject to our criminal law.

---

68 See Gordon, para.14-34. For obvious reasons the theft of electricity is not dealt with by the institutional writers. For many years, however, it seems to have been the unchallenged practice of prosecutors to treat electricity as an appropriate object of theft.

69 Para.2.49 et seq.

3.68 Apart from crimes like fire-raising, which are not relevant for present purposes, Scots law recognises two offences relating to damage to property. These are the common law crime of malicious mischief, and the statutory offence of vandalism created by section 78 of the Criminal Justice (Scotland) Act 1980.

3.69 In the time of the institutional writers malicious mischief was seen as an offence involving great and wilful damage to the property of another, done "with circumstances of tumult and disorder".[70] Over the years, however, the need for these features has disappeared, and Macdonald[71] describes the offence as applying to "injuries to, or destruction of, property where there is no taking, but only the indulgence of cruelty or malice, or an attempt to concuss others by injuring their property". The offence is committed "if the damage is done by a person who shows a deliberate disregard of, or even indifference to, the property or possessory rights of others".[72]

3.70 Standing the foregoing definitions it seems clear that the offence of malicious mischief would be appropriate in respect of the corruption or erasure of data or programs where that was achieved by some sort of physical interference with, or destruction of, the tapes or discs containing the data or programs in question. In such a case what occurred would be similar in kind to a

---

70 Hume, i.122; Alison, i.449.

71 p.84.

72 per L.J.C. Aitchison in Ward v. Robertson, 1938 J.C. 32, at 36.

case where a person defaced or destroyed a book or a manuscript. But what if the corruption or erasure is achieved simply by electronic means?

3.71 In that event it could be argued that the tape or disc will itself be undamaged, and will still be as fit for its purpose of storing data as it was before the corruption or erasure occurred, much as would happen if writing were rubbed off a blackboard. It will simply be the data or program which has sustained damage; but to say that is to raise the question whether data, or a program, can properly be regarded as "property" for the purposes of the offence of malicious mischief. This could be seen as a parallel to the question which we have already considered, namely whether information is something which is capable of being stolen. Arguably, if it is not capable of being stolen, it is not capable of being damaged.

3.72 There is, however, a counter-argument. The main difficulty about any concept of stealing information is that there is no taking away of the information if it is merely memorised, or photographed, or copied. In such a case the owner of the information does not lose any of the information: he merely loses its exclusive or private character. If, however, the nature of that information is altered by its being corrupted or erased, then different considerations must apply since in that case the substance of that which is owned has been changed. Indeed if total erasure has occurred, the information may have ceased to exist. Looked at from a slightly different point of view a parallel argument is also possible. Information stored on a tape or a disc is

represented by magnetic impulses or whatever on the tape or disc itself. Any corruption or erasure of the data which these impulses represent must involve in a sense some damage to the tape or disc since in such a case the tape or disc is not merely an empty receptacle waiting to receive such impulses but one which already has them imprinted on it. On that approach any corruption of the data is a form of damage to the disc or tape itself.

3.73 We ourselves are persuaded by the arguments in the last paragraph. To argue otherwise would, we think, be like arguing that it is not malicious mischief to dissolve an oil painting with a chemical solvent since in that event the canvas is still capable of being used for another painting. In our opinion the crime of malicious mischief is sufficiently wide, and sufficiently flexible, to deal with new technologies, and in particular to deal with the corruption or erasure of data or programs.

3.74 This view derives some support from the majority decision in the recent case of H.M.A. v. Wilson.[73] In that case the accused, who was employed at Hunterston nuclear power station, maliciously activated an emergency stop button thereby causing the power station to shut down and to remain inoperative for 28 hours. During that time the electricity authorities were obliged to supply the national grid from other sources at a cost of around £147,000. A plea to the relevancy of a charge of malicious mischief was sustained by the sheriff on the ground that that crime necessarily involves some physical damage or injury to property. The sheriff's

---

73 1984 S.L.T. 117.

view was supported in a powerful dissenting judgment delivered by Lord Stewart, but the majority of the Court (Lord Justice-Clerk Wheatley and Lord McDonald) concluded that the indictment was relevant. The Lord Justice-Clerk put his opinion in this way:[74]

> "If the malicious intention improperly to stop the production of electricity is established, and the achievement of that had the effect of rendering inoperative a machine which should have been operating productively and profitably, then in my view that is just as much damage to the employer's property as would be the case in any of the more physical acts of sabotage. To interfere deliberately with the plant so as to sterilise its functioning with resultant physical loss ... is in my view a clear case of interference with another's property which falls within Hume's classification of malicious mischief."

It is not quite clear to us what the Lord Justice Clerk meant by "physical loss" in that passage since, as we understand it, the loss was a loss of productive capacity with consequential financial loss. We suspect that the meaning of the passage would have been just as appropriate had the word "physical" been omitted.

3.75 As mentioned above, a second offence relating to damage to property is the offence of vandalism which was created by section 78 of the Criminal Justice (Scotland) Act 1980. That section provides that:

> "... any person who, without reasonable excuse, wilfully or recklessly destroys or damages any property belonging to another shall be guilty of the offence of vandalism."

---

74 at p.119.

3.76 This new statutory offence is at first sight similar to the common law offence of malicious mischief. However, the High Court has recently stated[75] that section 78 is not simply an echo of the common law offence, but stands on its own language. By that we take the court to mean that the section must be construed on its own terms and not by inference from any principles applicable to the common law crime. That may, of course, result in the statutory offence being found in some respects to be identical with the common law offence, but need not do so. Indeed we note that the statutory offence uses the word "reckless" but we are not aware that recklessness has ever been seen as an element in the crime of malicious mischief.

3.77 In relation to our present concern the words which are principally of interest are "any property belonging to another" which describe the object of the prohibited activity. If our view were to be accepted, namely that property in a tape or a disc includes the contents then, in our view, the statutory offence would also cover cases of electronic corruption or erasure.

(8) Denial of access to authorised users

3.78 This is the final category of computer misuse which we described in Part II of this Memorandum. It is perhaps fair to say that it is rather more speculative than the others in the sense that, although it is, we understand, technically possible to deny access to a computer by electronic means, we are unaware of any

---

75 Black v. Allan, 1985 S.C.C.R. 11.

recorded instances where it has actually occurred. If, of course, the denial of access is achieved by purely physical means, such as by cutting a wire, there is probably no problem since that activity by itself could constitute either the offence of malicious mischief or the statutory offence of vandalism. Alternatively, the cutting of an electric wire could also be an offence under section 51 of the South of Scotland Electricity Order Confirmation Act 1956 and section 36 of the North of Scotland Electricity Order Confirmation Act 1958.[76] If, however, any denial of access was achieved by purely electronic means, then the position is, we think, far from clear. Depending on the precise circumstances of a given case, it is, we suppose, just possible that the highly flexible charge of breach of the peace might be appropriate; but such a charge would, in our view, have in contemplation the likely human and physical, as opposed to the economic, consequences of the behaviour in question. In many cases, however, only the economic consequences would be of real relevance. We doubt whether any part of our existing common law is appropriate for such cases.

Existing statutory offences

3.79 There is a variety of statutory offences which could indirectly involve some misuse of a computer. For example there are several offences which, in one context or another, involve the giving of a false statement:[77]

---

76 As amended respectively by Criminal Justice Act 1982, Sched.15, paras.9 and 11.

77 For example, Prevention of Fraud (Investment) Act 1958, s.13; Bankruptcy (Scotland) Act 1985, s.67.

in any of these cases the false statement could be based on, or derived from, false data stored in a computer. There is also a range of offences relating to information and its unauthorised disclosure. These include offences under the Official Secrets Act 1911, the Atomic Energy Act 1946, the Radioactive Substances Act 1960, the European Communities Act 1972, and the Legal Aid (Scotland) Act 1967. In all of these cases the information the disclosure of which is prohibited could well be stored in, or recovered from, a computer.

3.80 In the result many of these statutory provisions could be appropriate for the prosecution of what might loosely be referred to as computer crime or computer fraud. However, they would not in any way address, far less solve, the particular problems which we have sought to identify in this part of the Memorandum, and that for the simple reason that in all these cases the use of a computer would be entirely incidental to the activity in question. In other words the computer in these cases could just as well have been replaced by a conventional, manual, system of record-keeping or whatever without making any difference to the nature of the offence in question. So far as we have been able to discover there are at present, with only one exception,[78] no statutory provisions in this country which directly deal with any of the problems with which we are presently concerned.

---

78 Interception of Communications Act 1985; see para.3.21 above.

Civil remedies

3.81 In this Memorandum we are concerned to examine the adequacy of our existing criminal law in relation to computer misuse in order to determine whether reform of that law is either necessary or desirable. It seems to us, however, that it would be inappropriate to consider any reform of our criminal law in this area without at least taking a brief look at the extent to which our civil law may provide remedies for some of the activities with which we are concerned. What we may require to contemplate, after all, is not simply the reform of the legal description of activities which are presently regarded as criminal, but the possible criminalisation of activities which at present do not attract the attention of the criminal law at all. Such a course must involve a consideration of whether or not it is necessary in the public interest that certain activities should be regarded as criminal, and that in turn must inevitably involve a consideration of whether or not such activities can be adequately controlled in some other way.

3.82 Rights in various kinds of incorporeal subjects are recognised, and protected, by various branches of statute law, and in some instances by the common law. Those branches of statute law which are of particular relevance here are copyright, patent and registered design legislation. In relation to the common law the area which is probably of most interest is that relating to the protection of trade secrets. This is by no means the place to attempt a full description of these areas of law, but it may be helpful to note briefly the more salient features which seem to be relevant to the subject matter of this Memorandum.

(a) Copyright law

3.83 The statutory expression of British copyright law is to be found in the Copyright Act 1956, as subsequently amended. The types of subject which are covered by copyright law are, generally, literary, dramatic, musical and artistic works, together with certain sound and visual recordings. Additionally, under the Copyright (Computer Software) Amendment Act 1985, copyright protection is to be extended to certain computer programs, though not to computer data. Again stating the matter very generally, the protection which is afforded by copyright law is a protection against unauthorised reproduction of the work in question, it being axiomatic that "the copyright protects the expression of an idea rather than the idea itself".[79] The rights which are created by copyright law are not absolute rights of property since they can only be protected in the limited manner mentioned above, and since in any event they have only a limited duration (normally 50 years).

3.84 In the context of the present Memorandum we think that copyright law has some relevance. If data stored in a computer happens to be of a kind which attracts the protection of copyright law, then that law will provide a remedy should a person take the data without authority, and subsequently reproduce it. But in practice the kind of data that will be stored in a computer may often not fall under copyright law at all.

---

79 W.R. Cornish, Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights, p.319.

(b) Patent law

3.85 British patent law is now regulated by the provisions of the Patents Act 1977. Under that Act a patent may be granted for "an invention"[80] which satisfies certain conditions as to novelty, inventiveness, and industrial application. In Scotland a patent is incorporeal moveable property[81] and may be assigned either outright or in security.[82] Once granted, however, a patent does not endure for ever but expires after a period of 20 years.[83] Where it is alleged that a patent has been infringed, civil proceedings may be brought against the alleged wrongdoer.[84]

3.86 Patent law seems to have little direct relevance to the subject matter of this Memorandum. The technical details of an invention may be stored in a computer, but if the data in question is taken and used by an unauthorised person the existence of a civil remedy will depend on whether or not a patent has been granted for the invention in question, and not on the nature of the medium in which the technical details are recorded.

(c) Registered designs

3.87 The Registered Designs Act 1949 provides for the registration of designs which are "new or original",

---

80 s.1.

81 s.31(2).

82 s.31(3).

83 s.25(1).

84 s.61.

and which involve "features of shape, configuration, pattern or ornament" which appeal to the eye rather than being dictated solely by the function which the article in question has to perform.[85] The author of a design is treated for the purposes of the Act as its proprietor,[86] and upon registration acquires the copyright in the design[87] for, normally, a period of five years.[88] The copyright can be protected by civil proceedings.[89] So far as its relevance to the subject matter of this Memorandum is concerned, registered designs law is in much the same position as copyright and patent law.

(d) Trade secrets

3.88 It has been said[90] that:

> "Trade secrets are bodies of knowledge, whether relating to customers, markets, sources of supply or methods of manufacture or otherwise, which a person in business or trade regards as and seeks to preserve as peculiarly his own."

Taking this as a useful working definition, it is clear that, in modern times, computers will be used not merely as a means of recording and storing such secrets but also as a means of seeking to preserve them from the eyes of others.

---

85 1949 Act, s.1.

86 s.2.

87 s.7(1).

88 s.8.

89 s.9.

90 Walker, Principles of Scottish Private Law, (3rd ed.) Vol.III, p.526.

3.89 The use and disclosure of confidential information of any kind, including trade secrets, may be regulated by the terms of a contract.[91] Thus a contract of employment may provide expressly or impliedly that any secret information, or information of specified kinds, obtained by an employee is not to be disclosed to other parties, and, quite apart from contract, there may in certain circumstances be an implied obligation of confidence as between master and servant.[92] English law has also for many years recognised a general obligation of confidence in certain other circumstances, and in our recent Report on Breach of Confidence[93] we suggested ways in which a statutory obligation of confidence might be introduced into Scots law.

3.90 While this branch of our law is still to some extent undeveloped, we consider that it has the capacity to provide a useful range of sanctions and remedies in cases where there is an obligation to respect the secrecy or confidentiality of certain classes of information. In particular it should, in our view, operate as a useful restraint in cases where an employee, whether with or without authorisation, becomes aware of information stored as data on a computer. The civil law, however, strikes at the dissemination of such data and can do

---

91 Fraser, Master and Servant (3rd ed.) p.95; and see, e.g., Exchange Telegraph Co. v. Giulianotti, 1959 S.C. 19.

92 Faccenda Chicken Ltd. v. Fowler and Others, The Times, 11 December 1985.

93 1984, Scot. Law Com. No.90.

nothing about the taking of it in the first place.[94] Moreover, unless effect were to be given to the possible scheme of reform suggested in our Report on Breach of Confidence,[95] any civil remedies would be available only in a limited number of circumstances.

(e) Trespass

3.91 Our civil law recognises trespass as a delict involving an infringement of an occupier's right of exclusive possession of heritable property.[96] In the event that a person broke into, or even simply entered, another's premises in order to gain access to, or to interfere with, a computer located in these premises, the occupier of the premises might have available to him the remedies of damages or interdict, and would also be entitled to order or conduct the intruder off the premises. It seems unlikely, however, that this civil remedy would often be appropriate for the kinds of computer misuse with which this Memorandum is primarily concerned.

3.92 Looking to civil remedies as a whole our conclusion is that, while they may have a part to play in regulating some forms of computer misuse, they are likely to do so by accident as it were rather than by tackling the particular problems directly.

---

94 Except, perhaps, where the unauthorised accessing of a computer can be treated as a disciplinary offence under a contract of employment.

95 See above.

96 Walker, Delict (2nd ed.), p.938.

PART IV - A NEED FOR REFORM?

4.1 Our survey of existing law in Part III of this Memorandum has, we think, highlighted two features in particular. One is that, if our assessment of existing law is correct, many forms of computer misuse should be capable of being dealt with by that law without the need for any reform. The second is that, even where existing law is, or may be, defective for dealing with particular computer-related activities, any such defects are not necessarily related to these activities alone: they may often be of much wider application. Before turning to consider possible reforms to our law it may be helpful to consider these points in slightly more detail. Once again we do so by reference to the various categories of misuse which we have previously used for the purposes of analysis.

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

4.2 It is clear that, in many of the cases where this sort of activity occurs, the use of a computer will be no more than incidental to a course of criminal conduct which our law would readily characterise as amounting to fraud, embezzlement or theft. Even where the use of a computer is more central to the activity in question, the only possible difficulty that we have been able to identify is that there may be thought to be some conceptual difficulty about making a false pretence to a machine. Our own opinion is that our law of fraud in particular is sufficiently flexible to be able to accommodate that concept. Consequently, our provisional view is that there is no need to reform our law of fraud in order to deal expressly with cases where data is

erased or falsified in order to obtain a pecuniary or other advantage.

4.3 In paragraph 3.13 above we drew attention to the difference which exists between the Scots crime of uttering and the offences created for England and Wales by sections 1 and 3 of the Forgery and Counterfeiting Act 1981. We observed that, under that Act, it might be possible to prosecute a person who supplied false data to a computer, whereas the same facts would not support a prosecution for uttering in Scotland. Had this been a problem in isolation it might have been necessary to consider some comparable reform of Scots law. If, however, we are correct in concluding that our law of fraud (and in appropriate cases embezzlement or theft) are capable of dealing with cases where data is falsified, then in our view no provision comparable to sections 1 and 3 of the 1981 Act is required for Scotland. If, in a given case, no more occurred than the supply of false data to a computer, such activity could, in our opinion, be prosecuted as an attempted fraud.

(2) Obtaining unauthorised access to a computer

4.4 This activity, particularly when it takes the form of hacking, is the one which has attracted the greatest media interest in recent years. It is also an activity which in our view is not subject to any effective control by our criminal law.[1]

---

1 See para.3.17 *et seq* above.

4.5 As we have seen[2] there are those who argue that hacking is no more than a harmless sport engaged in simply for the intellectual challenge which it presents. Indeed even the media sometimes cannot avoid a certain note of admiration when reporting the exploits of some, and particularly young, hackers.[3] We, for our part, can understand this attitude since any technological feat is clearly worthy of some admiration. This is particularly so when the feat is, at least in this country, not contrary to the law.

4.6 On the other hand hacking, or any other form of unauthorised access to a computer, can quite properly, we think, be regarded as an unjustified and objectionable invasion of privacy. Apart from civil remedies based, for example, on the delict of trespass, our criminal law already recognises a right to privacy in certain circumstances. If someone peeps between the curtains in order to see what is going on inside a room, he will be guilty of a breach of the peace. Certainly in such a case the primary rationale for that crime is that the conduct in question is likely to cause alarm rather than

---

2 For example, para.2.39 above.

3 In one case which was widely reported in the summer of 1985 a number of young American hackers in the State of New Jersey had for a considerable period been penetrating the supposedly secure computers of government departments and large corporations. One of the youngsters had been chided by his parents for the very large telephone bill which his "computer activities" had run up. He made amends by penetrating the telephone company's computer and reprogramming it so that his parents' next bill was suitably reduced. Very few press reports sought to condemn this exploit in any way.

that an invasion of privacy has taken place, but it is not, we think, too fanciful to suggest that in part at least it will be the invasion of privacy which gives rise to the alarm in the first place. In the area of statute law the Interception of Communications Act 1985 will make it an offence, except with express authority, to intercept telephone conversations and communications between computers using a public telecommunication system, and section 58 of the Post Office Act 1953 makes it an offence for an employee of the Post Office to open any postal packet in course of transmission by post. These analogies suggest that an offence of taking unauthorised access to a computer would not be out of place in our law.

4.7 It may, of course, be argued that to take unauthorised access to a computer is more nearly analogous to taking unauthorised access to a store cupboard or a filing cabinet, and that neither of these activities is a crime according to our law. It is perfectly true that these activities are not crimes in themselves, but if the security of the objects in question is overcome, the person concerned may well find himself facing a charge of opening a lockfast place with intent to steal, which is a crime; and if he overcomes the security of a building he may find himself facing a charge of housebreaking with intent to steal. No doubt it may be said that a hacker who overcomes the electronic security of a computer is not doing so with the intention of stealing the computer's contents, but in part that is so only because of the conceptual difficulties surrounding a "theft" of information: he is very likely to be doing so with the intention of acquiring knowledge

of the data concerned and, in so far as that data is secret or confidential, that may, we think, be regarded as a form of dishonest taking.[4]

4.8 Obviously in a matter of this sort precise comparisons or analogies are not really possible. What we have said so far, however, persuades us that hacking, and other forms of unauthorised access, are not only objectionable on social and economic grounds but also constitute an activity which at least has several points of resemblance to other activities which already fall under our criminal law. On that basis we conclude that there is a case for devising a crime to deal with the obtaining of unauthorised access to a computer.

(3) Eavesdropping on a computer

4.9 The kind of eavesdropping that was described in paragraph 2.41 of this Memorandum would probably be regarded by most people as being undesirable and, if one was the victim of such an activity, most unwelcome. The fact that it is happening may be completely unknown to the victim, and as a consequence secret or confidential information may pass unnoticed into the hands of persons who are not authorised to have such information.

4.10 All of this tends to suggest that such behaviour, which is not at present, so far as we can tell, subject to the criminal law, should be made subject to that law without delay. While we would not necessarily dissent from that view, we are, however, conscious that the kind

---

4 para.3.57 above.

of activity being considered here is but one example of what may well be a much wider problem. While we are far from being expert in modern surveillance techniques we understand that it is, for example, possible to listen in to a conversation at long range using directional microphones. That, it seems to us, is really no different in character from the computer eavesdropping which we have described; and we would doubt whether it is really a sensible or an acceptable approach to law reform to legislate, in the absence of a good reason for doing so, for one specific kind of abuse while ignoring others which, in a legal sense, are really more or less similar in character. Hacking, and perhaps some other forms of unauthorised accessing of a computer, are not activities of this kind since, so far as we can tell, they are computer specific and do not have a counterpart in other fields of technology. Eavesdropping on computers, on the other hand, does not appear to us to possess any special features which would justify a new crime directed solely at that activity.

4.11 If that view were to be accepted, it would follow that any reform of the law should not be undertaken without a full survey of all the surveillance and espionage techniques which are currently in use, and without a careful analysis of the circumstances, if any, in which the criminal law should be used to control such behaviour. That is all beyond the scope of this Memorandum, and accordingly we do not for the present propose to consider any law reform to deal with computer eavesdropping.

(4) Taking of information without physical removal

4.12 As has been mentioned elsewhere in this Memorandum,[5] information may be "taken" in many ways, none of which is at present a crime. It may be read off a computer screen (either by one authorised to use that computer or by a hacker); it may be obtained by reading a piece of paper; or it may be acquired by overhearing a conversation. Any information so acquired may, of course, be used thereafter in a perfectly proper fashion, but equally it may be misused, for example by being passed on, or sold, to a business competitor. The question then is whether the taking of information, at least when unauthorised or for an improper purpose, should be made a crime. Our view is that the present Memorandum is not the appropriate place to answer that question.

4.13 We have several reasons for holding this view. The first, and perhaps the most important, is that to make information the object of theft would involve conferring on information some kind of property status which at present it possesses neither in the criminal nor the civil law. In other words any problems regarding the legal status of information are very much wider than our present concern in this Memorandum. Apart from the undesirability of having different concepts of property in civil and criminal law (even if that were possible), we think in any event that information is something which should not be capable of exclusive ownership. Dealing

---

5 para.2.42 above.

with this very matter a committee of the Canadian House of Commons has said:[6]

> "For reasons of public policy the exclusive ownership of information which, of necessity, would flow from the concept of 'property', is not favoured in our socio-legal system. Information is regarded as too valuable a public commodity to have its ownership vest exclusively in any particular individual."

4.14 A second reason stems from the fact that in many cases where information is taken and used for some improper purpose the taker will be an employee of the person whose information it is. As such, he will be liable to internal disciplinary procedures including, perhaps, dismissal. This may have some deterrent effect in relation to such activities.

4.15 A third reason is that if, as we have previously suggested, the unauthorised accessing of a computer, including in particular hacking, were to become a crime, then the result would be that there would be a criminal sanction available for a significant range of cases where, as a result of the unauthorised accessing, information is in fact acquired by someone who has no entitlement to do so. Any such new offence would, of course, be concerned only with the unauthorised accessing itself rather than with the consequences of that activity but, as such, it would provide an effective means of protecting information even if it did not directly address its taking.

---

6 Canadian House of Commons, Standing Committee on Justice and Legal Affairs, Report of the Sub-committee on Computer Crime, June 1983, p.14.

4.16 A final reason is that, even if the property problems mentioned above could be overcome and an offence of theft of information created, it would, we think, be difficult if not impossible to frame such an offence in a way which would satisfactorily distinguish between what one might call the ordinary and proper acquisition of information and acquisition of a kind which ought to be regarded as improper and therefore criminal. The infinite variety of ways in which information can be acquired would in our view pose immense problems if any attempt were made to legislate on this matter.

(5) **Unauthorised borrowing of computer discs or tapes**

4.17 Although this activity may be undertaken in order to gain access to the information which a disc or tape may contain, it is quite different from the kind of "theft" of information which we have just been considering in that in this case there is a tangible thing which has been taken. Moreover, that thing will normally be in the ownership or possession of someone, and will accordingly be capable of being stolen.

4.18 As we have seen, however, the difficulty which may arise in such cases is that the owner may be deprived of the article only temporarily rather than permanently, and there may be some uncertainty about the extent to which our law will recognise such a deprivation as amounting to theft. In our opinion the line of recent cases which was described in Part III of this Memorandum[7] could in fact be found to provide sufficient authority for treating

---

7 paras.3.43 et seq.

such behaviour as theft, but there may be a case, if only in the interests of achieving certainty, for seeking to reform the law so as to encompass the temporary removal of discs or tapes. But that immediately presents a major problem.

4.19 Although, no doubt, the temporary removal of tapes or discs, possibly in order to acquire information or to copy programs, is seen as a highly undesirable activity by computer users, the plain fact is that, if there is any defect or shortcoming in our existing law, it is by no means confined only to articles associated with computers. It can, as we have seen,[8] arise in relation to films which are temporarily removed for the purpose of illicit copying. It could equally well arise in relation to a wide range of other articles such as books, papers and sound recordings, to name but a few.

4.20 It is not, of course, unknown for there to be legislation dealing with very specific forms of undesirable behaviour: examples are to be found in legislation dealing with road traffic, food and drugs, weights and measures, and so on. As presently advised, however, we do not see the temporary borrowing of computer tapes and discs (even if it is not covered by the existing law of theft) as being so distinguishable from other forms of borrowing, such as those mentioned in the preceding paragraph, as to justify specific legislative intervention. If there is a need to make such behaviour criminal, then in our view the proper

---

8 R. v. Lloyd and Others, [1985] 2 All E.R. 661; and see para.3.49 above.

course would be either to create a new offence of much wider application, or alternatively to revise the common law of theft so as to expand the range of cases where temporary, as opposed to permanent, deprivation will suffice. We do not examine either of these possibilities in this Memorandum.

(6) Making unauthorised use of computer time or facilities

4.21 Although this sort of activity is in some ways similar to the second category of misuse mentioned above, namely obtaining unauthorised access to a computer, - and may indeed follow on from that - what we are primarily concerned with here is the use for computing purposes of a person's computer facilities both by a person who is not authorised to use these facilities at all and by a person who is authorised to use them, but not for his private purposes or private gain.

4.22 In Part III of this Memorandum we came to the conclusion that this kind of activity is probably not subject to our criminal law save, perhaps, in so far as it may be regarded as involving a theft of the electricity consumed. As presently advised we can see arguments both for and against changing that state of affairs.

4.23 In favour of making this sort of activity subject to the criminal law it can be said that many computer installations involve a very substantial investment in stored data and sophisticated programs, not to mention the associated hardware, and that it is wrong in principle that a person should be permitted with impunity

to use all of these for his own private purposes. This will particularly be so if, as may be the case, these private purposes are in conflict with the business and commercial interests of the person whose computer is involved.

4.24 On the other hand it can be argued that the sort of activity in question is really no different in substance from many other kinds of unauthorised use of a person's property, none of which are subject to the criminal law. If a person goes into his neighbour's garage and, without authorisation, uses his bench saw to cut up some wood, he commits no crime. If, in an office, an employee uses his employer's typewriter to type personal letters, or his employer's telephone to make personal telephone calls, he equally commits no crime, except perhaps in the latter case a theft of the cost of the telephone call. So far as we are aware there is no clamour to make these activities criminal, and in that event it may be questioned why special attention should be given to the unauthorised use of a computer.

4.25 A further consideration is that most often, as we understand it, unauthorised use of a computer for private purposes will be made by one who is in the employment of the person whose computer it is. That being so, the employer will have disciplinary sanctions available to him, and it may be thought that in most cases they will be sufficient without the need to invoke the criminal law as well.

4.26 For the moment we have no firm view as to whether or not the unauthorised use of a computer's facilities should be a criminal offence.

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

4.27 In Part III of this Memorandum we have expressed the view that this sort of activity could be dealt with either as the common law crime of malicious mischief or as the statutory offence of vandalism. If that view is correct, it follows that in our opinion no reform of the law is required here.

(8) Denial of access to authorised users

4.28 Although it has been suggested to us that this can be achieved by purely electronic means as opposed to physical means such as cutting telephone cables etc., we have at present no clear information to suggest that it is either a widespread activity or one which is likely to present major problems in the long term. Moreover, we would see major disadvantages in a crime which simply penalised those who denied access to the authorised users of a computer. Such a crime would be much too wide and would, for example, strike at any person who, for whatever reason, waylaid a computer operator on his way to work.

4.29 It may be that there are problems here which in fact require a solution but which for the present we do not fully appreciate. No doubt consultees will draw any such problems to our attention. In the meantime, however, we do not propose to consider any law reform in relation to this activity.

4.30 So far in this Memorandum we have endeavoured to describe the various forms of misuse to which, as we understand it, computers and computer systems may be

prone. We have examined the law which is, or may be, relevant to deal with such activities, and we have considered, in the light of that examination, the need for reform. There are many matters in all of this on which we would welcome the views of consultees both in relation to technical matters and in relation to our analysis of the legal position. Before passing on to consider the shape that any reforms of our law might take, it may be helpful to summarise in question form the points on which we particularly seek the views of consultees.

Summary of questions on which the views of consultees are sought

4.31 (1) Do you consider that we have correctly and adequately identified the main categories of computer misuse which are causing, or are likely to cause, concern?

(2) Do you agree with our assessment of the present law in Part III of this Memorandum? If not, on what points do you disagree?

(3) In particular -

(a) Do you agree that the making of a false pretence to a computer as opposed to a person should not present problems for our crime of fraud?

(b) Do you consider that our law of theft would penalise the temporary taking of computer discs or tapes?

(4) Do you agree that reform of the law is unnecessary in respect of:

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

(b) Taking of information;

(c) Malicious or reckless corruption or erasure of data or programs; and

(d) Denial of access to authorised users?

(5) Do you agree that the following, in so far as they may not be adequately dealt with under existing law, are part of a wider problem so that any reform of the law should not be specific to computers but should be of wider application:

(a) Eavesdropping on a computer; and

(b) Unauthorised borrowing of computer discs or tapes?

(6) Do you agree that there should be appropriate legislation to make it an offence to obtain unauthorised access to a computer?

(7) Do you consider that it should be an offence to make unauthorised use of computer time or facilities?

Conclusion

4.32 We are conscious of the fact that the way in which we have dealt with the need for reform in this Part of the Memorandum has disclosed a number of unresolved problems, particularly in relation to the law of theft and the legal nature of information. In some instances - as in the case of temporary appropriation - these problems are unresolved for the present because in our view any defect or uncertainty in the present law is of much wider application than just in relation to

computer-associated articles. Possibly a comprehensive review of our whole law of theft would be advantageous, but the present Memorandum is not, we think, the place for that. So far as the legal nature of information is concerned, this is something which goes far beyond the criminal law. The advent of widespread computerisation in particular has had the effect of transferring to the realm of incorporeal property many things such as files, records, plans or designs which in the past inevitably took a corporeal form. We strongly suspect that the time will soon come, if it has not already arrived, when there will be a need for a thorough reappraisal of the whole concept of corporeal and incorporeal property, including information. That, however, will require a careful examination not only of many parts of our civil and criminal law, but also a wide-ranging consideration of social, political, economic and moral factors.

4.33 We are also conscious that it may appear a little curious to some readers of this Memorandum that certain manifestations of twentieth century technology can (if our assessment is accurate) be adequately dealt with by a common law which is based on principles enunciated by institutional writers of the eighteenth and nineteenth centuries, and even earlier. While some may feel that the time is ripe for a modern restatement of these principles, we have no doubt that many others will say that it is no more than a reflection of the great flexibility and adaptability of Scots common law that it is generally able to keep pace with contemporary developments of all kinds. For the present we are content to leave the common law to deal with problems of computer crime where, in our view, it is capable of doing so.

PART V - APPROACHES TO REFORM IN OTHER JURISDICTIONS

5.1 If the provisional views which we have formed about the need for reform of Scots law were to be accepted, the result would be that we would recommend an offence to deal with the taking of unauthorised access to a computer and, possibly, an offence to deal with the unauthorised use of computer time or facilities. For such an exercise only limited guidance is to be found by examining the ways in which other jurisdictions have tackled the subject of computer crime. On the other hand, it may be that consultees will disagree with our assessment of the current position, and in that event we may require to contemplate a more extensive reform of our law. If that were to be so, the approach of other systems of law might offer considerable guidance.

5.2 In considering the various matters on which views are sought in this Memorandum consultees may find it of assistance to have some indication of the approaches to law reform that have been taken around the world. Rather than fill up a large part of the text with this material, a survey of recent reforms in other jurisdictions has been set out in Appendix A.

PART VI - POSSIBLE REFORMS

6.1 From our consideration of existing law in Part III of this Memorandum, and our assessment of the need for reform in Part IV, it emerges that some forms of computer misuse can reasonably confidently be expected to fit within parts of our existing criminal law, such as those involving the crimes of fraud or malicious mischief. Some, on the other hand, such as the temporary removal of tapes or discs, and the unauthorised use of computer time or facilities, may present problems for the existing law but, if they do, are part of a wider problem the solution of which lies beyond the scope of the current exercise. In the result the only form of computer misuse which, as presently advised, we think should be made the subject of a new offence is the obtaining of unauthorised access to a computer or computer systems, particularly in the form of hacking. We have noted that, if this activity were to be an offence, then not only would that penalise the particular mischief in question but also it would in some instances provide a useful deterrent against the unauthorised taking of information and unauthorised tampering with data or programs. We now consider how such an offence might best be formulated.

Obtaining unauthorised access to a computer

6.2 The first question which we think requires to be addressed when considering an offence to deal with this kind of activity is how wide such an offence should be. On the one hand there can be no doubt in our view that a criminal offence must be framed in such a way that, so far as possible, there can be no room for

uncertainty as to when the offence is or is not being committed. On the other hand an offence which is directed largely at a technological activity should not, we think, be expressed in terms which are so precise as to run the risk that the offence will cease to be effective in perhaps a year or two simply because what is essentially the same mischief is by then being perpetrated by somewhat different, and possibly more sophisticated, means.

6.3 In relation to the obtaining of unauthorised access to a computer we see the problem in this way. At present, as we understand it, the activity of hacking necessarily involves the use of a public telecommunication system in order to make contact with the target computer. On that basis it would be possible to frame an offence simply in terms of obtaining unauthorised access by means of such a system. But, if it were, or if it were to become, possible to obtain unauthorised access by means of a private, as opposed to a public, telecommunication system, such an offence would be ineffective in a possibly significant number of cases. And, if it were to become possible in the future to obtain access to a computer by means other than a conventional telecommunication system, then any offence expressed in terms of using such a system, even if not limited to a public one, would likewise cease to be effective in some cases.

6.4 It may be that we over-estimate the possibilities for technological development in this area. If so, we hope that our more technically skilled consultees will bring this to our attention. If,

however, changes of the sort that we have envisaged are indeed possible, there would appear to be a case for making it an offence simply to obtain unauthorised access to a computer, that is to say without specifying in any way the manner in which such access is achieved. The difficulty about that sort of formulation, however, is that the offence would then affect not only hackers but also, for example, an employee who, without authorisation, operated the keyboard at one of his employer's terminals. It may be that this ought to be a criminal offence but, standing the availability of internal disciplinary sanctions in such cases, some people may take a different view. Moreover, an offence expressed in the wide manner suggested above would, we think, create some risk of uncertainty as to whether it did or did not cover certain activities. For example, would the words "obtain unauthorised access" be construed so as to cover only cases where the person concerned caused the computer to operate in some way, or might they also cover the case where a person simply obtained access to a room where a computer was situated?

6.5 We are clearly of the view that the last example given above should not be the subject of an offence, but apart from that we have at present reached no firm conclusion as to precisely how, and in particular how widely, a new offence should be formulated. To some extent a final decision must await the technical advice of some of our consultees. Subject to that, it seems to us that there are several possible options. These may be summarised as follows:

(a) It should be an offence to obtain unauthorised access to a computer by means of a public telecommunication system. This formulation would exclude cases where an employee obtained unauthorised access directly to his employer's terminal (or to a room where the computer was situated) but may be expressed too narrowly to cater for technological developments in years to come.

(b) It should be an offence to obtain unauthorised access to a computer by means of a telecommunication system. This takes a wider view of the technology, but still may not go far enough.

(c) It should be an offence to obtain unauthorised access to a computer by any form of telecommunication. If the method of obtaining access is to be specified at all, this is perhaps the widest possible formulation. Subject to further consideration of the word "access",[1] this formulation could also strike at the long-range eavesdropper who has been described elsewhere in this Memorandum.[2] Notwithstanding our view that that particular activity should not itself be the subject of an offence for the reason that it is but one example of a whole range of possibly unacceptable surveillance techniques, it may be that there would be no objection to its being

---

1 See para.6.6 below.

2 See, e.g., para.2.41.

drawn into the net, as it were, in a wide hacking offence.

(d) It should be an offence to obtain unauthorised access to a computer. This formulation, by not specifying any required technique, would apply not only to a conventional hacker but also to an employee, or anyone else for that matter, who obtained unauthorised access to a computer by direct physical means. To avoid the risk, mentioned in paragraph 6.4 above, that this formulation could also cover simply going into a computer room without authority, it would, we think, be necessary to define "access" in an appropriate way or to use a different word in place of it, so as to make the scope of the offence clear.

6.6 However widely or narrowly a new offence may come to be formulated (and there may well be other possibilities beyond those suggested in the last paragraph), it will, we think, be necessary to give some attention to the precise words which are used in it. Thus far we have for convenience spoken only in terms of "to obtain unauthorised access", but it may be that other words would be preferable or even, as we suggested in (d) above, necessary. The point is that what we are seeking to penalise by the new offence presently under consideration is primarily the activity which puts a person in a position where, having made electronic contact with a computer, he can instruct it to display data or to carry out computing operations. We are not necessarily seeking to penalise the actual giving of such instructions because that could make this offence overlap

with the activity of making unauthorised use of computer facilities, which we are not at present disposed to make the subject of a criminal offence. And, of course, as previously observed, we may require to ensure that the new offence does not cover the mere obtaining of access to a place where a computer is situated.

6.7 One possibility to meet these points might be to use the words "communicate with" in preference to "obtain access to". Such words would at least exclude mere presence in the vicinity of a computer. On the other hand they would not, without further elaboration, necessarily exclude using the services of a computer; and furthermore they might be seen as being rather passive words for an offence which is intended to strike at a deliberate act. An alternative would be to use the word "access", but to use it as a verb. It is regularly used in that form by persons who themselves are computer users and, as such, it conveys, as we understand it, precisely the meaning which we think would be appropriate for the new offence. Against that, the use of the word as a verb is plainly a neologism with its origins in technical jargon, and for that reason it is probably inappropriate for a statute. Indeed, we note with interest that even where the word is used as a verb in American statutes, it has generally been thought necessary to define it as meaning, among other things, "communicate with".[3]

---

3 See, e.g. the Florida statute reproduced in Appendix B, s.815.03(10).

6.8 On balance we are inclined to think that the best course will be to use the words "communicate with" in preference to any of the other options that have been considered. Since in any event we consider that the offence should also include the word "intentionally", if only to exclude cases where contact is made accidentally, we think that the two concepts of "intention" and "communication" taken together will sufficiently indicate the active rather than passive behaviour which the offence is meant to deal with. There remains, of course, the possibility that these words could also cover the case of a person making unauthorised use of a computer's facilities. Probably that will not be a major problem if the final formulation of the offence were to retain some reference to "telecommunication", or indeed if that particular activity were itself to come within the scope of the criminal law. Until the views of consultees are known, we doubt whether it is profitable to pursue this point further at this stage.

6.9 A further point of detail is the concept of "without authorisation". In the normal case the authorisation, if any, will come from the owner of the computer in question, and we would not anticipate that such words would create problems. It occurs to us, however, that there might be cases where official investigating authorities, such as the police, might wish to communicate with a computer without the knowledge or authorisation of the person or company concerned. We are not competent to say whether such cases could occur, nor what considerations should apply in determining whether or not such access should be permitted without it amounting to an offence. If, however, there is a problem

here we suspect that the proper way to deal with it would be by making provision for express authorisation, possibly along lines similar to those contained in the Interception of Communications Act 1985. Some of our consultees may wish to address themselves to this matter.

Definitions

6.10 If any new offence were to be formulated in terms of communication being achieved by means of a "public telecommunication sytem", it would probably be desirable to define these words. As in the Interception of Communications Act 1985[4] this should probably be done by reference to the definition in the Telecommunications Act 1984.[5] If, however, these words were not to be used, we would doubt whether any of the words in the offence would require express definition with the possible exception of the word "computer". Many other systems of law which have enacted computer legislation in recent years have gone to considerable lengths to define words such as "computer". Some of these definitions are full of technical details while others are expressed more in terms of function. At a time when technology itself can develop and change with great rapidity we are in no doubt that, if any definition of "computer" were thought to be necessary, that should be expressed in terms of function rather than technology. We note, however, that in the computer evidence provisions[6] which are contained in the recent Police and Criminal Evidence Act 1984 it was not

---

4 s.10(1).

5 s.9(1).

6 ss.69 and 70.

thought necessary to provide any definition of "computer" at all. We are disposed to think that this is a wise course to follow.

Summary

6.11 It may be helpful at this stage to summarise the proposals and questions on which we seek the views of consultees. These are:

(1) Should a new offence of obtaining unauthorised access to a computer be expressed as:
   (a) to communicate with a computer intentionally and without authorisation by means of a public telecommunication system; or
   (b) to communicate with a computer intentionally and without authorisation by means of a telecommunication system; or
   (c) to communicate with a computer intentionally and without authorisation by any form of telecommunication; or
   (d) to communicate with a computer intentionally and without authorisation?

(2) Is there another formulation of the new offence which would be more acceptable than any of those shown in (1) above?

(3) Is it appropriate to use the words "communicate with" in the new offence?

(4) If there is to be a new offence on the lines suggested, are there any circumstances in which official authorisation in favour of, for example, the police would be required? If so, should provision be made for that in a manner similar to

that used in the Interception of Communications Act 1985?

(5) Do you agree that, with the possible exception of "public telecommunication system", none of the terms to be used in the new offence require express definition?

Penalty

6.12 We would welcome views as to the level of maximum penalty which should be applied to this new offence. Clearly the degree of gravity attaching to particular examples of the offence may vary between teenage adventurism at one end of the scale and determined industrial espionage at the other. To cover this span we propose that: The offence should be triable either summarily or on indictment. In the former case the maximum penalty could be three months imprisonment or a fine up to level 5 on the standard scale.[7] In the latter case the maximum could be two years imprisonment or an unlimited fine.

Others forms of misuse

6.13 So far as the other forms of misuse described earlier in this Memorandum are concerned we have concluded in some cases that they are likely to be dealt with adequately by existing law. No reform is therefore required in such cases. In the case of the pure taking of information we have concluded that that should not be subject to the criminal law at all. There remain,

---

7 At present £2,000.

however, some forms of misuse which fall into a rather different category.

6.14 Eavesdropping on a computer, and the unauthorised borrowing of computer software, may present problems for the criminal law; but they are, in our opinion, but particular examples of a possible defect in the law which, if it exists, extends to much more than simply misuse of a computer. The unauthorised use of computer time or facilities is to an extent in the same position, but additionally we are not convinced that it is an activity which in any event justifies the attention of the criminal law.

6.15 For the present, and until the views of consultees are known, we are not disposed to examine in detail the shape of any possible law reform in respect of these matters. The time for that would be when and if there was a strong consensus among consultees that such activities should, by some means, be made criminal offences.

Other possible reforms

6.16 Thus far in this Memorandum we have been addressing ourselves to the various types of activity which may be thought to constitute computer misuse, and to the need for possible reform of our criminal law in respect of such activities. There are, however, several other possible areas of law reform which have been suggested to us, and we would welcome the views of consultees on these as well.

6.17 One suggestion which has been made to us is that there should be a legal duty placed on computer users to disclose incidents of computer misuse. It is not clear to us to whom it is thought that any such disclosure should be made. The justification for this suggestion appears to be that at present many victims of computer misuse are reluctant, possibly for commercial reasons, to let it be known publicly that they have sustained losses caused by computer misuse, and that this simply encourages other miscreants to try their hand in the hope, if they are found out at all, of being permitted the same anonymity.

6.18 We are not at present persuaded that there is a case for the imposition, in any form, of a duty of disclosure. The British Crime Survey,[8] conducted for the Home Office and the Scottish Office, has shown that non-reporting of many crimes is at a high level; and of course that Survey was concerned only with activities which actually are crimes according to existing law. As we have endeavoured to show in this Memorandum some forms of computer misuse may not be crimes under existing law, and it seems to us that that, as much as any considerations of commercial credibility, may be the reason why at present incidents of misuse are not reported.

6.19 Even if that is not so, we doubt whether it would be either sound in principle or indeed practicable

---

8 The British Crime Survey; first report, Home Office Research Study No.76, 1983; The British Crime Survey Scotland, A Scottish Office Social Research Study, 1984.

to impose any duty of disclosure. So far as principle is concerned, we are not aware of any other kind of criminal behaviour which gives rise to such a duty, and we can see no reason why computer misuse, even in so far as it may become criminal, should be singled out for a different approach. So far as practicability is concerned, several points occur to us. Would the duty extend to all computer users and, if not, how would one distinguish between the classes of user to whom the duty did or did not apply? Any distinction between, for example, public companies and other users would be arbitrary and artificial, and would exclude many major computer users such as government departments. Even if a satisfactory solution to that problem could be found, there would remain a question as to how the duty should be enforced. Would it be a criminal offence to fail to disclose an incident of computer crime?

6.20 The foregoing considerations lead us to the provisional conclusion that: There should be no duty to disclose incidents of computer crime.

6.21 Another suggestion which has been made to us is that statutory provision should be made for minimum security measures which should be observed by all, or by specified classes of, computer users. Such measures should involve not only the physical and electronic security of the computer itself but also matters like internal audit control and management strategy.

6.22 It is certainly true, as was said by the Audit Commission,[9] that:

> "The risks of fraud and abuse will be all the greater if internal controls and internal audit are inadequate. Poor supervision and ineffective audit will almost certainly encourage the opportunity for large scale and long-running losses. Where the organisation sustains such an environment and still encourages the widespread introduction of computing the risks will be considerable."

6.23 While readily accepting these comments, we are not persuaded that the answer lies in a statutory code of practice. In saying that we have in mind the virtually infinite number of uses to which computers are put today, and the virtually infinite degrees of security which these uses demand. If a statute were to attempt to prescribe minimum security measures it would, we think, either be quite inappropriate for many computer users or be so bland and imprecise as to offer no useful guidance at all. Accordingly, we propose that: A statutory code of practice for computer users should not be introduced.

6.24 It does seem to us, however, that the diverse nature of computer use, and the varying security requirements which that entails, could properly be made the concern of bodies like trade or professional associations. The membership of such bodies is likely to be such that any computer use may be more homogeneous in character, and therefore more suitable for the application of general guidelines. We have no doubt that many such bodies already offer advice to their members on matters of computer security but, in so far as they do

---

9 Computer Fraud Survey, p.2.

not, we would venture to suggest that this is something which may be worth considering.

PART VII - JURISDICTION

7.1 If effect were to be given to our proposal to create a new offence in respect of the activity known as hacking, and even in so far as other forms of computer misuse may be covered by existing law, it would in our view be desirable to give some consideration to the matter of jurisdiction. Because of the nature of computers, and the way in which contact can be made with them from long range, it is obvious that in many instances offences could be committed partly in one jurisdiction and partly in another. We examine this problem in this Part of this Memorandum.

7.2 In relation to computer-related crimes the problem of jurisdiction is one which could involve any country in the world since it is just as easy for a computer operator in Edinburgh to make contact with a computer in Hong Kong as it is for him to make contact with one in Glasgow. We think, however, that it may be helpful to begin by examining the problem in a British context. For that purpose we now turn to a brief survey of the jurisdictional rules in criminal matters in Scotland on the one hand, and England and Wales on the other.

Criminal jurisdiction in Scotland

7.3 As a general rule the jurisdiction of the Scottish courts in criminal matters depends upon the *locus delicti*: the nationality or domicile of the

accused or victim are irrelevant.[1] There are some exceptions to this general rule but they are mainly statutory.[2] Two statutory exceptions deserve particular mention. The first is to be found in the Criminal Procedure (Scotland) Act 1975. Sections 7 and 292 of that Act provide that every person who has in his possession in Scotland property which he has stolen in any other part of the United Kingdom may be dealt with, tried and punished in Scotland in the same way as if he had stolen it in Scotland, and that any person who receives in Scotland property stolen in any other part of the United Kingdom may be likewise dealt with in Scotland as if the property had been stolen there. The second is in the Post Office Act 1953. Section 70 of that Act provides that thefts or attempted thefts of mail in course of transmission as such between different jurisdictions in the British postal area, and any robbery, attempted robbery or assault with intent to rob committed in stealing or with intent to steal mail, may be tried in any jurisdiction in Scotland.

Criminal jurisdiction in England and Wales

7.4 As in Scotland, criminal jurisdiction in England and Wales depends as a general rule on the

---

1 Hume ii, 49 et seq; Renton and Brown, Criminal Procedure according to the Law of Scotland (5th ed.), 1-07.

2 e.g., Geneva Conventions Act 1957, s.1; Aviation Security Act 1982, ss.1, 2, 8; Taking of Hostages Act 1982, s.2. Common law exceptions exist in relation to the crimes of piracy and treason.

locus delicti.[3] This general rule is, however, qualified by statutory and other exceptions as it is in Scotland. Many of the statutory exceptions are the same as those applying in Scotland, while others are comparable.[4]

Offences partly in one jurisdiction and partly in another

(a) Scots law

7.5 The application of the general rule on criminal jurisdiction obviously presents no problems where the offence consists of a single act. The locus delicti can then be determined with precision. Determination of the locus delicti is not so easy, however, when the offence consists of acts and consequences each of which may occur in a different jurisdiction.

7.6 Where not all of the ingredients of a given offence have occurred in Scotland the approach under Scots law has been to hold that the Scottish courts have jurisdiction if the "main act" occurred there.[5] Thus it has been held that there was jurisdiction in Scotland where money was obtained by an Englishman by means of fraudulent advertisement in Scotland,[6] where a Scots

---

3 Archbold, Criminal Pleading, Evidence and Practice (41st ed.), 2-28; Board of Trade v. Owen [1957] A.C. 602.

4 The counterpart of ss.7 and 292 of the Criminal Procedure (Scotland) Act 1975 is to be found in the Theft Act 1968, s.24, and the counterpart of s.70 of the Post Office Act 1953 is to be found in the Theft Act 1968, s.14.

5 Hume, ii, 54;

6 H.M.A v. Allan (1872) 2 Couper 402.

bankrupt uplifted money in England to defraud his creditors,[7] and where an Englishman, by means of false representations contained in letters posted in England to traders in Scotland, obtained from these traders goods without any intention of paying for them.[8]

7.7 Upon one view the last of the above-mentioned cases appears to make it clear that, where the crime in question is fraud, the "main act" will be the actual result achieved by the fraud. In holding that the courts of Scotland had jurisdiction in that case the Lord Justice General (Inglis) said:[9]

> "It is here that [the dupe] is imposed on and induced to believe the false and fraudulent representations of the panel; it is here that he acts on the belief ... Edinburgh is the locus delicti in the present case, just as much as if the panel had sent either an accomplice or an innocent agent to carry out his fraudulent scheme to completion in Edinburgh."

7.8 Very recently, however, a wider view on jurisdiction appears to have been taken by the High Court. In Laird and Another v. H.M.A.[10] the appellants were charged with fraud. The indictment alleged that, at the registered office in Glasgow of a company of which they were directors, or elsewhere in Great Britain, they pretended to Conoco (UK) Limited that they could supply a certain quantity of steel, complying with a specific

---

7 H.M.A. v. McKay (1866) 5 Irv. 329.

8 H.M.A. v. Witherington (1881) 4 Couper 475.

9 at p.492.

10 1984 S.C.C.R. 469.

British Standard, at a price of just over £81,000. The indictment went on to allege that, in a yard on Humberside in England, they uttered false certificates relating to the quality of the steel and thereby induced a representative of the company to hand over there a cheque for the above amount, and that thereafter they caused defective steel to be shipped from England to Conoco's construction yard in the north of Scotland. The appellants challenged the jurisdiction of the court in Scotland to try them, relying in the main, it appears, on the view that, on the authority of Witherington, the "main act" in this case had occurred in England.

7.9 The appeal against conviction was rejected. While acknowledging that the opinions of the judges in Witherington would prima facie appear to give support to the appellants' submission, the Lord Justice Clerk (Wheatley) went on to comment favourably on observations in some earlier Scottish cases to the effect that, where a "continuous crime" is involved, there may be dual jurisdiction in each country concerned. He then expressed the view that:[11]

> "... where a crime is of such a nature that it has to originate with the forming of a fraudulent scheme, and that thereafter various steps have to be taken to bring that fraudulent plan to fruition, if some of these subsequent steps take place in one jurisdiction and some in another, then if the totality of the events in one country plays a material part in the operation and fulfilment of the fraudulent scheme as a whole there should be jurisdiction in that country."

---

11 at p.472.

Applying that test the Lord Justice Clerk (with whom the other judges concurred) founded on the facts that the original fraudulent scheme had been devised in Scotland, that it had been followed up by telephone and telex messages emanating from Glasgow, that the false certificates of quality had been forged in Glasgow, and that the steel was eventually delivered to an address in Scotland. The Lord Justice Clerk concluded that these circumstances played such a material part, not only in the formation of the fraudulent scheme but in its execution, that it was justifiable to hold that the Scottish court had jurisdiction.

7.10 Before leaving the rules of Scots law in relation to offences committed partly in one jurisdiction and partly in another, reference should be made to a quite separate rule relating to offences which themselves consist of some form of communication. In Lipsey v. Mackintosh[12] a man was charged with sending invitations to bet, the invitations having been sent by post from Glasgow to Dundee. It was held that the sheriff court at Dundee had jurisdiction to try the case, the Lord Justice General (Dunedin) observing:[13]

> "... where something is going on by the medium of the post, the offence is really committed, if I may use the expression, at both ends of transmission by the Post Office."

Although not the subject, so far as we are aware, of express authority, we understand that prosecutors adopt

---

12 (1913) 7 Adam 182.

13 at p.187.

the same view in relation to offences committed by use of the telephone, for example a breach of the peace consisting of an obscene or offensive message. In practice such cases will normally be prosecuted in the court of the district where the recipient resides, if only because that is where he or she is likely to have reported the matter to the police. But so far as we can see, there is no reason why such a case should not equally be tried in the court for the district where the offender made the call.

(b) English law

7.11 So far as we can tell English law in some instances deals with offences committed partly in one jurisdiction and partly in another in a manner similar to Scots law. In other instances it takes a rather different approach. In part, we think, this may be because of the different way in which some offences are expressed under English law.

7.12 A similar approach to that of Scots law is to be found in R. v. Baxter.[14] In that case the accused, who was at all material times in Northern Ireland, posted fraudulent claims to football pool firms in Liverpool. He was charged with attempting to obtain property by deception and it was held that the English court had jurisdiction to try the offence. In reaching that decision the Court of Appeal proceeded on two alternative grounds. The first was that, at any moment during the

---

14 (1971) 55 Cr. App. R. 214; and cf. D.P.P. v. Stonehouse [1977] 2 All E.R. 913.

time when the proximate act or acts constituting an attempt to commit crime commence and the time when they finally fail, the attempt is still in being; and was therefore still in being when the letters came to light in Liverpool. The alternative ground was that "he who despatches a missile or a missive arranges for its transport and delivery (essential parts of the attempt) and is thus committing part of the crime within the jurisdition by the means which he has arranged.[15]

7.13 This approach to the question of jurisdiction appears to be similar to that adopted by the High Court in the case of Witherington[16] and, bearing in mind that the case of Baxter involved an attempt rather than a completed crime, also appears to be consistent with the Scots case of H.M.A. v. Semple.[17] It has been suggested that the principle in Baxter will apply, on similar facts, where the crime is completed.[18]

7.14 English law appears to follow a rather different course from Scots law (at least as expressed in the recent case of Laird)[19] where the facts are the other way round, that is to say where a person in England is alleged to have obtained goods by deception in another country. In R. v. Harden[20] it was held that the English

---

15 per Sachs L.J. at p.219.

16 See para.7.7 above.

17 1935 J.C. 41.

18 J.C. Smith, The Law of Theft (5th ed.), para.190.

19 See para.7.8 above.

20 [1963] 1 Q.B. 8.

courts have no jurisdiction in such a case, and that decision was followed in the later case of R. v. Tirado.[21] The decision in Harden was questioned in Treacy v. D.P.P.[22] by Lord Diplock who suggested that it should in due course be reconsidered, but that suggestion does not appear to have been taken up.[23]

7.15 Consideration has also been given to the question of jurisdiction under English law in cases of conspiracy to defraud, that being a charge which is frequently used in England and Wales in the absence of a charge of fraud on its own. The approach in such cases, it seems to us, has been in harmony with that adopted in Harden. A conspiracy in England to carry out a crime abroad is not indictable in England,[24] but a conspiracy is indictable in England where conspirators in England agree to do an unlawful act in England with intent to defraud a person abroad.[25] In Board of Trade v. Owen it was suggested that a conspiracy in England to commit a crime abroad might be indictable in England where performance of the conspiracy would produce a public mischief in England or injure a person in England by causing him damage abroad. However, it has recently been held[26] that there is no

---

21 (1974) 59 Cr. App. R. 80.

22 [1971] A.C. 537, at 563.

23 cf., for example, R. v. Markus [1976] A.C. 35.

24 Board of Trade v. Owen [1957] A.C. 602.

25 R. v. Hornett, [1975] R.T.R. 256.

26 Attorney General's Reference (No.1 of 1982) [1983] 2 All E.R. 721.

jurisdiction in England on the ground that a conspiracy to defraud abroad has caused economic loss and damage to the proprietary interests of a company within the jurisdiction or on the ground that a company has been injured here by being caused damage abroad. Finally it is to be noted that a conspiracy formed abroad to commit a crime in England will be indictable in England if acts in furtherance of the agreement are committed there.[27]

Jurisdiction in computer-related crimes

7.16 If the views expressed elsewhere in this Memorandum were to be accepted the result would be that some forms of computer misuse would be dealt with by existing crimes such as fraud or malicious mischief, while the activity of hacking would become a new statutory offence. Any of these crimes or offences could involve activities partly in one jurisdiction and partly in another; and although, as we have pointed out, these different jurisdictions could be at opposite ends of the earth, it seems reasonable to assume that in a not inconsiderable number of cases the jurisdictions in question will be, on the one hand, Scotland and, on the other, England and Wales. As we have shown, however, the existing rules in these countries for determining where a case is to be tried are not always entirely clear and consistent.

7.17 In these circumstances it is tempting to suggest that, where a computer in one country is used in connection with a crime or offence by a person in another

---

27 D.P.P. v. Doot and Others (1973) 57 Cr. App. R. 600.

country, provision should be made for the courts of either country to have jurisdiction. The difficulty about that suggestion is that, in respect of existing crimes such as fraud or malicious mischief, it would involve creating special rules for a specific form of these crimes while leaving other forms to be governed by possibly rather different rules. In our view this would not be a principled approach to law reform.

7.18 On the other hand our proposed new hacking offence would be in a different position since any special jurisdictional rules applied to it would stand alone and need not conflict with the rules applicable to other crimes or offences. Moreover, hacking is an offence which by its very nature is committed at long range, and is therefore likely to pay no heed to national borders.

7.19 We think that there is a good case for saying that jurisdiction to try the new offence should exist both in the place where the hacker is, and in the place where the computer which is the object of his attentions is situated. Accordingly we propose that: If effect were to be given to our proposal to create a new offence for the activity of hacking, it should also be provided that, where the offender carries out his activities in a different jurisdiction from that in which the computer that he is communicating with is situated, the courts in both places should have jurisdiction to try the offence.

PART VIII - SUMMARY OF QUESTIONS AND PROVISIONAL PROPOSALS

1. (1) Do you consider that we have correctly and adequately identified the main categories of computer misuse which are causing, or are likely to cause, concern?

(2) Do you agree with our assessment of the present law in Part III of this Memorandum? If not, on what points do you disagree?

(3) In particular -

(a) Do you agree that the making of a false pretence to a computer as opposed to a person should not present problems for our crime of fraud?

(b) Do you consider that our law of theft would penalise the temporary taking of computer discs or tapes?

(4) Do you agree that reform of the law is unnecessary in respect of:

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

(b) Taking of information;

(c) Malicious or reckless corruption or erasure of data or programs; and

(d) Denial of access to authorised users?

(5) Do you agree that the following, in so far as they may not be adequately dealt with under existing law, are part of a wider problem so that any reform of the law should not be specific to computers but should be of wider application:

(a) Eavesdropping on a computer; and

(b) Unauthorised borrowing of computer discs or tapes?

(6) Do you agree that there should be appropriate legislation to make it an offence to obtain unauthorised access to a computer?

(7) Do you consider that it should be an offence to make unauthorised use of computer time or facilities?

(Para.4.31)

2. (1) Should a new offence of obtaining unauthorised access to a computer be expressed as:

(a) to communicate with a computer intentionally and without authorisation by means of a public telecommunication system; or

(b) to communicate with a computer intentionally and without authorisation by means of a telecommunication system; or

(c) to communicate with a computer intentionally and without authorisation by any form of telecommunication; or

(d) to communicate with a computer intentionally and without authorisation?

(2) Is there another formulation of the new offence which would be more acceptable than any of those shown in (1) above?

(3) Is it appropriate to use the words "communicate with" in the new offence?

(4) If there is to be a new offence on the lines suggested, are there any circumstances in which official authorisation in favour of, for example, the police would be required? If so,

should provision be made for that in a manner similar to that used in the Interception of Communications Act 1985?

(5) Do you agree that, with the possible exception of "public telecommunication system", none of the terms to be used in the new offence require express definition?

(Para.6.11)

3. The offence should be triable either summarily or on indictment. In the former case the maximum penalty could be three months imprisonment or a fine up to level 5 on the standard scale. In the latter case the maximum could be two years imprisonment or an unlimited fine. **(Para.6.12)**

4. There should be no duty to disclose incidents of computer crime. **(Para.6.20)**

5. A statutory code of practice for computer users should not be introduced. **(Para.6.23)**

6. If effect were to be given to our proposal to create a new offence for the activity of hacking, it should also be provided that, where the offender carries out his activities in a different jurisdiction from that in which the computer that he is communicating with is situated, the courts in both places should have jurisdiction to try the offence. **(Para.7.19)**

APPENDIX A

COMPUTER CRIME LAWS IN OTHER JURISDICTIONS

1. In recent years many countries have attempted to tackle the problems which are perceived as arising from computer criminality, but for several reasons the approach to law reform has tended to differ from country to country. One reason is that some countries already have laws which are capable of applying to incidents of computer misuse, while others do not. Another reason is that some countries appear to entertain some doubt about the social or public need for new criminal laws to protect what are more likely to be private rather than public assets. Yet another reason is that some countries, including the United Kingdom, have not so far given any real consideration to the problem.

2. Taking account of these varying backgrounds and attitudes it is possible to identify three broad approaches to dealing with computer related crime. One is simply to proceed on the basis that such crime presents no special features requiring special new measures, with the result that any particular incidents can be adequately dealt with under existing law. A second approach involves recognising that existing laws may be inadequate for certain forms of computer misuse: these inadequacies are then catered for either by amending existing laws or by creating new offences. The third approach takes the view that the only proper course is to enact specific and comprehensive computer crime statutes.

3. One example falling within the first category is The Netherlands where, because of existing concepts of information, theft and fraud, computer-related crimes have been successfully prosecuted under existing criminal law. Another example in the same category is Belgium. Under Belgian law all public telephone and telegraphic communications are protected against tampering with messages, against the destruction of messages, and against unauthorised access to the contents of messages: all of this is apparently seen as including computer networks.

4. Several countries are to be found in the second category. They include Australia, Canada, Finland, France, West Germany and Sweden. It may be helpful to indicate how each of them has approached the subject.

Australia

5. In Australia any reform of the criminal law is complicated by the fact that in some States the law is codified whereas in others it rests largely upon the common law. In 1983 the National Companies and Securities Commission prepared a working paper on computer-related crime in which they selected the criminal law of New South Wales (based mainly on the common law) as a model for reform.

6. The Commission rejected the idea of a comprehensive computer crime statute and sought instead to limit its proposals to provisions which would simply make up perceived deficiencies in existing law. Amendments to

the New South Wales Crimes Act were proposed to deal with:

(1) Breaking and entering computer installations.

(2) Criminal damage to computers and computer-related property.

(3) Theft etc. of computers and computer-related property.

(4) Falsification of computer data and software and use of computer-related property for fraudulent purposes.

7. In relation to (3) above it was proposed that any new legislation should deal with (a) the adaptation and extension of larceny to the definition of computer-related property and also to accessing computers without consent, (b) obtaining etc. computer-related property by deception, and (c) dishonest misapplication or misappropriation of computer-related property by persons in positions of trust. To achieve all this it was proposed that the definition of "property" should be expanded to include computer-related property, including software, and that the crime of larceny should be redefined to include the temporary taking of another's property.

Canada

8. Following on the Report of the Canadian House of Commons Standing Committee on Justice and Legal Affairs' Subcommittee on Computer Crime, a new Bill to amend the Criminal Code was laid before Parliament in February 1984. A modified version of that Bill was subsequently passed as the Criminal Law Amendment Act 1985. Among

other things the Act introduces the concept of unauthorised use of a computer, and a new form of "mischief" to cover the unauthorised modification or destruction (without apparent right) of computerised data.

9. The Act contains a new section 301 in the Criminal Code, which provides:

> "Everyone who, fraudulently and without color [sic] of right,
>
> (a) obtains, directly or indirectly, any computer service,
>
> (b) by means of an electromagnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system, or
>
> (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 387 [mischief] in relation to data or a computer system
>
> is guilty of an indictable offence ..."

10. The new form of mischief is contained in an amendment to section 387. It is in the following terms:

> "Everyone commits mischief who wilfully
>
> (a) destroys or alters data;
>
> (b) renders data meaningless, useless or ineffective;
>
> (c) obstructs, interrupts or interferes with the lawful use of data; or

(d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto."

11. For the purposes of the new section 301 the Act contains definitions of terms such as "computer program" and "computer system".

Finland

12. The Ministry of Justice in Finland has appointed a Committee to revise the Penal Code so as to take account of computer technology. Fraud and property offences are to be redefined accordingly.

France

13. The Ministry of Justice in France has appointed a Commission to revise the Criminal Code. Its purpose is similar to that of the Finnish Committee mentioned above.

West Germany

14. In West Germany a Bill for the Suppression of Economic Crime was introduced in 1984. It seeks to amend the Criminal Code by creating new offences of computer fraud and falsification of stored data, and by expanding the concept of "deception".

15. A new Article 263(a) will be added to the Code in the following terms:

"Any person who with the intention of procuring an unlawful gain for himself or a third party causes loss to another person by influencing the result of data processing through improper programming, by interfering with the run of the program or by the

use of incorrect or incomplete data, shall be punishable ..."

16. A new Article 269 is to be added in the following terms:

> "Any person who, for purposes of deception in a legal transaction, alters without authority or uses in such altered form any electronic, magnetic or otherwise invisible or not directly readable stored data intended to be used in a legal transaction as evidence of legally relevant facts shall be punishable ..."

17. Finally, a new Article 270 will provide:

> "Wrongfully interfering with data processing in regard to a legal transaction shall constitute deception in a legal transaction."

Sweden

18. The Swedish Data Act 1973 already contains a provision[1] which states:

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

Notwithstanding the breadth of that provision the Committee on Crimes against Property is presently considering adjusting the definition of fraud to cover cases where it is committed by using a computer, and introducing a new offence of theft of computer time.

---

1 s.23.

United States

19. The third policy category mentioned in paragraph 2 above, namely that of introducing comprehensive computer crime laws, is to be found only in the United States. At a federal level several Bills have recently been introduced both in the Senate and in the House of Representatives. These include: the Counterfeit Access Device and Computer Fraud and Abuse Act, which would penalise unauthorised access to a computer system in certain circumstances; the Federal Computer Systems Protection Act, which would make it a federal crime to engage in computer-related fraud or theft, or to damage or destroy computer hardware, software or stored data; and the Medical Computer Crimes Act, which would make it a federal crime to use a telecommunication device to gain unauthorised access to medical records.

20. At least 23 of the States in the Union have already enacted specific computer crime laws. Although similar in some respects, these laws also have marked differences, particularly that only some make it possible to prosecute a hacker. Some of those that do not at present contain such a provision are considering appropriate amendments.

21. A typical example of a computer crime statute (and one which contains a provision against unauthorised accessing) is the statute introduced in Florida in 1978. It is of some interest to see its terms in full. They are:

"815.01 Short title

The provisions of this act shall be known and may be cited as the 'Florida Computer Crimes Act.'

815.02 Legislative Intent

The Legislature finds and declares that:

(1) Computer-related crime is a growing problem in government as well as in the private sector.

(2) Computer-related crime occurs at great cost to the public since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime.

(3) The opportunities for computer-related crimes in financial institutions, government programs, government records, and other business enterprises through the introduction of fraudulent records into a computer system, the unauthorized use of computer facilities, the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets are great.

(4) While various forms of computer crime might possibly be the subject of criminal charges based on other provisions of law, it is appropriate and desirable that a supplemental and additional statute be provided which proscribes various forms of computer abuse.

815.03 Definitions

As used in this chapter, unless the context clearly indicates otherwise:

(1) 'Intellectual property' means data, including programs.

(2) 'Computer' means an internally programmed, automatic device that performs data processing.

(4) 'Computer software' means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.

(5) 'Computer system' means a set of related, connected or unconnected, computer equipment, devices, or computer software.

(6) 'Computer network' means a set of related, remotely connected devices and communication facilities including more than one computer system with capability to transmit data among them through communication facilities.

(7) 'Computer system services' means providing a computer system or computer network to perform useful work.

(8) 'Property' means anything of value as defined in s.812.011 and includes, but is not limited to, financial instruments, information, including electronically produced data and computer software and programs in either machine-readable or human-readable form, and any other tangible or intangible item of value.

(9) 'Financial instrument' means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security.

(10) 'Access' means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.

815.04 Offenses against intellectual property

(1) Whoever willfully, knowingly, and without authorization modifies data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(2) Whoever willfully, knowingly, and without authorization destroys data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(3) Whoever willfully, knowingly, and without authorization discloses or takes data, programs, or supporting documentation which is a trade secret as defined in § 812.081 or is confidential as provided by law residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

815.05 Offenses against computer equipment or supplies

(1) Whoever willfully, knowingly, and without authorization modifies equipment or supplies used or intended to be used in a computer, computer system, or computer network commits an offense against computer equipment or supplies.

(2) Whoever willfully, knowingly, and without authorization destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization destroys, injures, or damages any computer, computer system, or computer network commits an offense against computer equipment or supplies.

815.06 Offenses against computer users

(1) Whoever willfully, knowingly, and without authorization accesses or causes to be accessed any computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another commits an offense against computer users.

815.07 This chapter not exclusive

The provisions of this chapter shall not be construed to preclude the applicability of any other provision of the criminal law of this state which presently applies or may in the future apply to any transaction which violates this chapter, unless such provision is inconsistent with the terms of this chapter."

22. As can be seen the Florida approach is to create wholly new categories of crime, namely offences against intellectual property, offences against computer equipment or supplies, and offences against computer users, though it seems likely that some of these offences, such as causing damage to computer equipment, will already be offences under general criminal damage provisions. That presumably accounts for the last paragraph in the provisions just quoted. An alternative approach which has found favour in some States is to frame offences in a way which more closely echoes traditional offences. Thus, for example, in Arizona one finds a provision which states:

> "A person commits computer fraud ... by accessing, altering, damaging or destroying without authorization any computer, computer system, computer network, or any part of such computer, systems or network, with the intent to devise or execute any scheme or artifice to defraud or deceive, or control property or services by means of false or fraudulent pretenses, representations or promises."

23. Despite containing many of the ingredients of traditional fraud, the foregoing offence still bears a new title, namely "computer fraud". Yet another approach (which may be more familiar to those accustomed to British legislative techniques) is simply to describe the

prohibited activities without giving any name to them. An example of that is to be found in the Californian Penal Code, section 502 of which provides:

> "Any person who intentionally accesses or causes to be accessed any computer system or computer network for the purpose of (1) devising or executing any scheme or artifice to defraud or extort or (2) obtaining money, property, or services with false or fraudulent intent, representations, or promises shall be guilty of a public offense."

APPENDIX B

List of individuals and organisations who offered information and advice prior to the preparation of this Consultative Memorandum

Associated Scottish Life Offices
Bank of Scotland
BIS Applied Systems Ltd
British Computer Society
Commercial Union Assurance
Committee of Scottish Clearing Bankers
Deloitte, Haskins and Sells, Chartered Accountants
R.T. Doswell
Eagle Star Group
W.A. Fenwick, California
FS Assurance Ltd
Brent Gammon, California
General Accident Fire and Life Assurance Corporation PLC
Guardian Royal Exchange Assurance
IBM United Kingdom Ltd
Institute of Chartered Accountants of Scotland
Mercantile Credit Company Ltd
Ekkehart Muller-Rappard, Council of Europe
Norwich Union Insurance Society Ltd
Emile Peeters, EEC Commission
J. Pringle
Royal Insurance (UK) Ltd
Professor B. de Schutter, Brussels
Scottish Amicable Life Assurance Society
Scottish Equitable Life Assurance Society
Scottish Widows' Fund and Life Assurance Society
Dr. Ulrich Sieber, Freiburg, W.Germany
Artur Solarz, Stockholm
Standard Life Assurance Company
Trustee Savings Bank Scotland