

Electronic Data Interchange and Computer Crime

by Indira Mahalingam Carr and Katherine Williams

This paper is based on 'Bytes into Computer Law' in Computers and Law Carr, I M and Williams, K S (1994) Oxford: Intellect Books.

Introduction

The last decade has seen the introduction of computers at all levels of human transactions. Introduction of any new technology inevitably raises a number of questions ranging from the social and the ethical to the legal. Computer technology is no exception. A major use envisaged for computers is in communications where data can be transferred electronically between businesses nationally and internationally - a use that is becoming commonplace. The use of electronic data interchange (EDI) raises important questions which relate to the degree to which it can be protected against unauthorised access, interference and use and the extent to which the law deters such activities. In this paper we consider the British laws on computer misuse and the suggestions put forward by the Council of Europe on computer related crime.

Electronic Data Interchange (EDI) and Computer Crime

The term 'computer crime' is used to cover a multitude of sins. In most instances, it simply refers to the fact that a computer has been used in the committal of an offence which could well have been carried out through other means. Just as murder can be committed by using a gun or a knife so too fraud can be committed using a computer or paper. In such instances, the existing criminal laws are probably adequate for dealing with computer commissioned crimes. However, there is a

species of computer centred activity that has the potential of causing a great deal of harm, mostly economic, to the legitimate user but which does not fall within the sphere of criminal law unless the meanings of existing criminal offences are strained to the fullest extent. And even where this is done it may prove inadequate.¹ It is this type of computer crime that poses a real threat to businesses, whether they are small scale or multinational, since they are increasingly relying on EDI rather than paper for carrying on their commercial activities. The worrying prospect which arises is that some individual (be it an employee or a complete stranger) will interfere with the information, either to their benefit (be it economic or psychological) or to the financial detriment of the legitimate user. And, as many of those in charge of businesses neither operate computers, nor understand their operation, there is a certain amount of myth and hysteria about the likelihood of falling victim to such activities. The fear was certainly far less when paper was used since its weaknesses were clearly understood and accepted as unavoidable.

The further factor that increases the need for some kind of control is that computer crime does not obey national boundaries. An individual sitting at a computer terminal in State A may access and use a computer system located in State B, with the capacity to alter or obtain copies of data held in the accessed computer.² This ease of transborder computer activity has led international organisations to consider the problems related to computers and crime.

The level of the problem is difficult to ascertain since most reports tend to be sensationalised and lack the

information necessary for a clear legal discussion.³ Where there are official statistics, as with all other criminal activity, they are not representative of the full problem. In the area of computer crime the statistical problem is compounded because much of computer related crime is not separately recorded. This however may prove to be a blessing. Over-provision in this area is perhaps best avoided since it would discourage the use of traditional criminal laws wherever these are inadequate to deal with the activity. Otherwise, criminal law may become over-specialised and become less able to handle more general problems.

In Britain, as in many countries, traditional criminal laws seem unable to cope with certain kinds of computer related crime because of the intangible nature of information held on a computer. Much of criminal law protects tangible property and either cannot be used to cover computer crimes⁴ or their use strains the natural meaning of criminal law to its limits and extends the laws in unacceptable ways which might affect us in non-computer related offences.⁵ Particular problems are encountered in respect of taking information. For example, if a disc containing information is stolen, a prosecution for theft can lie and it may be legitimate to assess the worth of that item taking account of the information contained on it, but if the thing taken is only the information on the disc, then nothing has been stolen and the charge of theft will be unsuccessful.⁶

As far back as 1987, the Scottish Law Commission in its report recommended that one offence needed to be added to the criminal laws, namely, obtaining unauthorised ac-

cess to a program or data stored in a computer where this is done in order to inspect or otherwise acquire knowledge of the program or the data or to add to, erase or otherwise alter the program or the data with the intention:

- (a) of procuring an advantage for himself or another person; or
- (b) of damaging another person's interests.⁷

In 1989 the report of the Law Commission for England and Wales⁸ recommended that unauthorised access should be an offence whether performed for its own sake or with another motive in mind. This would have made hacking *per se* unlawful even if only done in order to experiment with the user's skills in overcoming any security devices. The Government did not then act on the report but did so subsequently. A private member's bill was used as the basis for the *Computer Misuse Act 1990*.⁹ The Act creates three offences:

- obtaining unauthorised access to a program or data held on a computer (s.1);
- doing the above with the intention to facilitate the commission of a further offence (s.2); and
- unauthorised modification of the contents of any computer (s.3).

And, under s.17(2) a person secures access to any program or data held in a computer if by causing a computer to perform any function he:

- alters or erases the program or data;
- copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;
- uses it; or

- has it output from the computer in which it is held (whether by having it displayed or in any other manner).

And use is interpreted under s.17(3) as:

- causes the program to be executed; or
- is itself a function of the program.

From the above it is clear that minimal access will be enough to commit a s.1 offence provided the other

"It seems particularly unfortunate that the net has been cast so wide when other areas of the law would have proved adequate to deal with some actions"

elements are also present. Simply turning the machine on would suffice since the program will be activated. Moreover the hacker need not succeed in gaining access. An offence will be committed merely by accessing a security device on the machine. The other elements that need to be established for a s.1 offence are:

- the access must be unauthorised (s.1(1)(b));
- the user must know at the time when he causes the computer to perform the function that the access is unauthorised (s.1(1)(c)).

The requirement of knowledge of unauthorised access on the part of the user would be easy to discharge where the user has to enter a password, or there is some other device indicating that the access is available only to authorised personnel. Unauthorised access will also arise in situations where access is permitted for certain purposes but not for others. It is not necessary to prove intent to access any particular program or data (s.2) so that the s.1 offence covers those who gain access purely for the intellectual exercise with no idea of what they might find there.

Section 1 clearly covers the general hacker but as it protects access to a program or data it may also criminalise the loading and use of unauthorised copy of a computer program. Although this is not the intended target of the Act it may prove useful for software protection.

One of the problems with s.1 is that many items of everyday use like compact disc players, cars and telephones, have small computers as part of their operation. S.1 would make an unauthorised use of these machines an offence. The actions which will fall under this section would, if carried out without a computer, be classed as theft or some other offence or may amount to civil wrongs such as trespass. It seems particularly unfortunate that the net has been cast so wide when other areas of the law would have proved adequate to deal with some actions. This problem could be dealt with by giving definitions of key terms such as 'computer', 'program' and 'data'. The Act however left these terms undefined to permit sufficient flexibility to accommodate the rapid development of technology.¹⁰ However, one consequence is to create a peculiar situation where the unauthorised use of a compact disc player may be classified as a s.1 offence because it contains a microchip.

Another problem with s.1 is that it is so widely cast that it also covers the hacker who accesses files solely for the psychological thrill and neither intends nor causes any damage.¹¹ The reason for the width of the offence seems to be that the person or institution whose records have been violated may fear damage, and expend large sums of money in checking all the records or perform some other time consuming and costly procedure. But, would it not have been better to leave these problems to be dealt with by insurance thereby increasing the pressure on the companies to install good security devices?¹² This provision unwittingly may encourage businesses to rely solely on the Act as a deterrent and to disregard sophisticated security devices for financial reasons. A further result, if s.1 offences can be monitored successfully, will be to clog up the already over burdened criminal justice system.

The above problems in relation to s.1 would not have arisen if there had been acceptance of the Scottish Law Commission's recommendation to make it an offence to obtain unauthorised access with intent to cause harm to the computer owner.

S.2 creates an ulterior intent offence and occurs where the individual who gains unauthorised access to a computer intends to commit or facilitate a further criminal offence for which the sentence is fixed by law or where a first offender aged over 21 would be sentenced to a five year term of imprisonment. And for the purposes of this section it is irrelevant whether it would be impossible to commit the further offence.

S.3 offence covers unauthorised modification of computer material and includes those who introduce a virus in another computer as well as anyone who alters or deletes information. It is the computer equivalent of criminal damage.¹³

The *Computer Misuse Act* recognises that computer crime transgresses international borders by allowing British courts jurisdiction where a 'significant link' with Britain can be established. A significant link is established for s.1 and s.3 offences where the user or targeted computer is located in Britain. Where the offence is a s.2 offence, jurisdiction is permitted if it is established that the further acts intended are an offence in the country in which they were intended to take place.

At the international level the Council of Europe¹⁴ has suggested that eight types of computer related activity comprising the minimum list

*"The Act however
left ... terms
undefined to
permit sufficient
flexibility to
accommodate the
rapid development
of technology"*

should be incorporated in the criminal laws of Member States. These are:

1. Computer related fraud;
2. Computer forgery;
3. Damage to computer data or programs;
4. Computer sabotage;
5. Unauthorised access;
6. Unauthorised interception of data transmission; and
7. Unauthorised reproduction of a protected computer program.¹⁵
8. Unauthorised reproduction of a topography.

The Council also suggested that four other activities comprising the optional list should be discouraged. They recommended that it might be advisable to criminalise these but left the method and extent of control up to individual states. These are:

1. Alteration of computer data or programs;
2. Unauthorised use of a computer; and
3. Unauthorised use of a protected computer program.

Some of these suggestions have already been incorporated in the *Computer Misuse Act* 1990. In fact, the Council's fifth suggestion is narrower than s.1 of the *Computer Misuse Act* as it requires security measures to be infringed before the offence can be committed. This narrower protection was recommended by the Council in order to discourage managerial negligence in setting up of suitable protection systems. As suggested earlier, this would appear to be an acceptable limit. As far as the other proposals are concerned British laws leaves those to be dealt with through general criminal laws. Thus there is no new offence of computer forgery (although where the forgery is unsuccessful section 2 provides a remedy).

Of particular interest is computer espionage in the optional list. Computer espionage would certainly cover eavesdropping - an activity where the electromagnetic signals around the visual display unit of a computer are picked from outside the building using a video recorder and television set. The eavesdropper has no control on the kind of information picked up on a screen and the activity therefore is passive. During the debate leading up to the *Computer Misuse Act* the question of making computer eavesdropping a criminal offence was considered but

it was felt that it did not pose a serious threat. However one must agree with the conclusions reached by the Council of Europe that eavesdropping could become a real threat since much commercial and governmental communication is now carried out electronically and it is highly likely that the patient eavesdropper will frequently come across sensitive material. It is time that the threat of computer eavesdropping was given more serious consideration in Britain.¹⁶

The most important area which is missed by the 1990 legislation, by the discussion leading to the 1990 legislation and by the Council of Europe is that of enforcement. It is highly desirable to have these crimes on the statute book but if the means are not available to detect the offences the criminal law remains unenforced and relatively worthless. There was a little debate concerning detection in the parliamentary stages of the 1990 Act. The Act imports powers of searching premises and seizure to the police under s.14 provided the circuit judge is satisfied by information on oath given by a constable that there are reasonable grounds for believing that a s.1 offence has been committed or is about to be committed in the premises. Most unauthorised access however occurs by means of a telephone line and there are no provisions in the Act to allow the police to obtain details concerning telephone lines. Monitoring of telephone lines is routinely carried out by telephone companies and the police may request such information; it is up to the company to decide whether to provide the material or not. Without the power to make such searches of telephone data held by telephone companies it will be almost impossible to establish the 'reasonable grounds' necessary to obtain a warrant under s.14. Indeed, to pass legislation of this sort without giving

the policy any means of detection may give companies and individuals a false sense of security. Against this, to provide special powers to include automatic searches of telephone data by the police would raise the question of whether there would be a serious breach of an individual's right to privacy guaranteed under Article 8 of the European Convention on Human Rights. There is thus a difficult choice to be made. On the one hand without the powers of detection the *Computer Misuse Act* is likely to be considered a useless piece of legislation largely relying upon

"The lack of satisfactory enforcement procedures and the gaps in the current legislation need to be addressed immediately"

chance rather than careful investigation for discovery. On the other, to offer true protection will necessarily involve intrusive detection methods raising serious considerations about the virtues of protecting the collective whole against the sanctity of the individual's right to privacy. As things stand, it seems unavoidable that one or the other has to give way.¹⁷

Conclusion

Though Britain has specific legislation relating to computer misuse since 1990, its success is difficult to gauge for a number of reasons. Firstly, it is not possible to ascertain how many cases come to court since

they are settled in the lower courts and therefore not included in the law reports. Secondly, many instances of computer misuse remain unreported since victims fear adverse publicity and economic harm that prosecutions may bring. Finally, the difficulties faced in obtaining evidence without the voluntary co-operation of telephone companies mean that many instances of computer misuse go unprosecuted.

The British legislation is not sufficiently wide to make computer eavesdropping illegal. It is an unfortunate omission since it is legitimate under the existing laws to take confidential information in some circumstances.¹⁸ It also does not deal with those who aid and abet any of the offences under the Act - for instance, where an individual provides another with a password for accessing a computer.

The lack of satisfactory enforcement procedures and the gaps in the current legislation need to be addressed immediately. Failure to do so could result in huge losses since commercial enterprises are rapidly accepting the use of EDI. ☛

Indira Mahalingam Carr is a member of the Faculty of Law, University of Exeter.

Katherine Williams is a member of the Faculty of Law, University College of Wales, Aberystwyth.

Footnotes

¹ See *R v Gold and Schifreen* [1988] AC 1063 where through using a password issued to engineers the hackers obtained entry into the Prestel system - a data base service of British Telecom. They were charged under s.1 of the Forgery and Counterfeiting Act 1981 which states:

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 do to or not to do some act to his own or any other person's prejudice.

'Instrument' under s.8(1) of the Act includes any disc, tape, soundtrack or other device on or in which information is recorded or stored by mechanical, electronic or other means.

The Court however came to the conclusion that the words 'recorded or stored' implied a degree of continuance and the password did not carry that degree of permanence since it was expunged once the computer had executed the checking task.

2. See the business news section of *The Independent on Sunday* 6 June 1993. Citibank and a firm of private detectives are being prosecuted for allegedly hacking into the computers of Barclay Bank and National Westminster Bank to obtain details about a customer's wealth before his company was placed in receivership. The prosecution is reported as being brought by Mr. Raymond Hill, a property developer.

3. See Wasik, Martin (1991) *Crime and the Computer* Oxford: Clarendon Press, for an account of the scale of the problem.

4. See *R v Gold and Schifree (supra)* in which legislation passed partially with modern technology in mind, failed to cover the mischief committed.

5. See *Her Majesty's Advocate v. Wilson* [1984] SLT 116 where the crime of malicious mischief, normally attached to physical damage to actual property, was extended to cover interference with productive operation of machinery to make a profit. And *Cox v Riley* (1986) *Cr App R* 54 in which the Criminal Damage Act 1971, used to protect property of a tangible nature (s.10), was extended to cover interference with a computer program by saying that the owner was required to expend time and money in restoring it to its original condition. See also *R v Whiteley* (1991) 93 *Cr App R* 25.

6. See *Oxford v Moss* (1978) 68 *Cr App R* 183 where a university student obtained the original of an examination paper which he returned after copying. The Court held that taking of confiden-

tial information was not theft. Of course, if he had kept the paper on which the examination questions were printed the course of events would have been different.

7. Scottish Law Commission No.106 *Report on Computer Crime* Cmnd. 174, 1987 London: HMSO, Part IV.

8. Law Commission Report No.186, *Computer Misuse*, 1989, Cm.818, London: HMSO.

9. This Act came into force on 1st August 1990.

10. The recent Singapore Computer Misuse Act 1993 provides an exhaustive definition of computer. S2(1) defines computer as 'an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility.' The definition seems fairly flexible to include future advances in technology and clear enough to exclude devices that have microchips that are non-programmable like a CD player.

11. The *Fifth Report of the Data Protection Registrar* warned of this outcome saying that it would criminalise juveniles whose hobby was to access without causing harm, at pp 30-31.

12. The Data Protection Act 1984 certainly seems to have cast the onus on the user to ensure adequate security measures are taken. The Eighth Principle requires that appropriate security measures are taken against unauthorised access to, or alteration, disclosure or destruction of, personal

data and against accidental loss or destruction of personal data.

13. So situations like those of *Cox v Riley (supra)* and *R v Gold & Schifreen (supra)* would now be covered by s.3.

14. The other international organisation that has done much work in this area is the Organisation for Economic Co-operation and Development.

15. Council of Europe Recommendation No. R 89(9) *Computer Related Crime*.

16. The Singapore legislation on computer misuse seems to cover eavesdropping. Under s.6(1)(b) of Computer Misuse Act 1993, any direct or indirect interception without authority of any function of a computer by means of an electromagnetic, acoustic, mechanical or other device will be caught by the Act.

17. It is interesting that under the Singapore Computer Misuse Act 1993, a police officer is entitled at any time to have access to and inspect and check the operation of any computer and any associated apparatus which he has reasonable cause to suspect is or has been used in connection with any offence under the Act (s.14). Moreover, under s.15 of the Act any police officer has the power to arrest a person reasonable suspected of committing an offence under the Act without a warrant.


18. See note 6 above.

IN OUR NEXT ISSUE...

Our next issue looks at

PRIVACY

Contributions from members of all Societies are welcomed. Although this is the central theme of the issue, contributions can be on any topic relating to computers and law and can take the form of an article, product review, book review, abstract or press release.

 Please send your contributions to the Editors no later than 24 March, 1995.