COMPUTER MISUSE

Reproduced below is an extract from a publicatoin by Messrs Norton Rose which summarises the recommendations of the English Law Commission.

Introduction

On 10 October 1989 the Report of the Law Commission on "Computer Misuse" was published. The Commission concluded that computer misuse was socially undesirable and could be very damaging. It recommended the creation of three new criminal offences to combat the problem.

This Report followed the publication in September 1988 by the Commission of a consultation paper, asking whether computer misuse could really do the harm some claimed, and, if so, whether computer misuse should be made a crimal offence.

Following is a summary of the Commission's final recommendations.

Computer Misuse: the Nature of the Problem

Computer misuse may take the form of simply gaining unauthorised access to a computer ("hacking") or it may take the form of damaging or altering a computer program. It may involve theft or deception ("computer crime"). Some claimed that hacking was an innocent activity, indulged in by those who enjoy the intellectual challenge of gaining entry to a system designed to prevent such access. There was, they said, no evidence that unauthorised entry caused any harm to any computer operator, despite scare stories in the press to the contrary. So far as computer crime was concerned, existing criminal law was quite sufficient; there were enough criminal offences already without adding to their number.

In order to test the strength of some of these assertions and because little evidence of actual misuse was presented in response to the Consultation paper (probably because disclosure would be damaging to those whose computer had been misused), the Commission held a series of confidential meetings with computer manufacturers and major computer users.

As a result of these meetings the Commission concluded that computer misuse was indeed a social menace which could do great harm. For example computer "viruses" can wipe out valuable data: altering the program of a computer–controlled robot had in one case led to serious personal injury: and the risk of unauthorised entry to systems led users to waste large amounts of time and money in devising safeguards and in checking to see if hackers avoided these safeguards. The confidence of computer users and would–be users was in danger of being undermined. Finally, hacking that started innocently could easily develop into computer crime and was better criminalised at source.

The New Offences

The Commission recommends to Parliament that three new criminal offences are introduced:

1. Unauthorised access to a computer system;

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

3. Unauthorised modification of computer material.

The Unauthorised Access Offences

This offence seeks to restrain the general mischief of unauthorised access to computers. It is intended to deter the more innocuous form of hacking, and so prosecution of offenders takes place only in the lower courts.

The essence of the basic hacking offence is obtaining or attempting to obtain *unauthorised* access to data held on computer. The Commission has made it clear that a person is only to be guilty of the offence if, by his action, he actually *intends* to gain access to a system and, at the same time, knows that he does not have authority to do so. A person who tampers with a computer and who by accident accesses the information stored there will, therefore, not commit the crime.

The Commission points out that the hacker, working from home, will be in no

doubt that he acts without authorisation. However, as a result of its researches the Commission has found that misuse is commonly perpetrated by employees or other "insiders" who have some degree of legitimate access to the system but exceed the bounds of their authority. The actions of insiders should not be criminalised unless they are actually aware that in tampering with the system they are exceeding their authority.

The burden of proving that access to a program or data was known to be unauthorised is to rest on the prosecution. It will, therefore, become important for employers to be able to show that they have clearly defined to employees the limits of their authority and that these instructions have been understood, and that they are updated if employees' job descriptions change. Production of such evidence will be greatly facilitated if careful records are maintained by employers."Access" is defined by the Commission as the causing of the computer to perform any function. Successful entry to a program is not a necessary ingredient of the offence. It is enough, for example, for a hacker to have presented the computer with an identification code and password and caused it to check the combination as a preliminary to giving access to its programs. Mere physical access to the computer (for example, coming into close proximity with it) does not constitute "access" as defined by the Commission nor does the obtaining, without recourse to a computer, of a hard copy of information printed out from it, since the offence is designed to penalise interference with the system itself.

Unauthorised use of a Computer System with Intent to Commit or Facilitate the Commission of a Serious Crime – The "Ulterior Intent Offence"

This offence is aimed at criminalising unauthorised access to a computer for the purpose, once access has been gained, of committing a second and more serious crime punishable by a maximum sentence of imprisonment of five years.

Although English law includes criminal sanctions for attempting to commit crimes, doubts have arisen whether the use of computers was more than merely preparatory to committing a crime: if so, it fell short of being the crime of attempt. The Commission intends that its proposal should overcome this difficulty.

Unauthorised Modification of Computer Material

The English courts have previously decided that erasing data from a plastic circuit card used to control an industrial saw give rise to the offence of criminal damage. Nevertheless doubts have been expressed whether the law is adequate to deal with those who seek to gain access to computers with a view to damaging material held on them. To prove criminal damage the prosecution must at present show that damage to tangible property has been caused; and where misuse has resulted in damage to data or programs this involves considerable artificiality.

The new offence is designed to cover the following typical situations:

- The intentional erasure of programs or data held in a computer's memory, without the authority of the owner.
- The placing in circulation of any disk or other storage medium "infected" with a virus, with the intention that that disk will cause some damage to a computer system (whether by the addition, deletion, modification or alteration of data).

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

Jurisdiction

Computer misuse knows no national boundaries: a hacker working from his home in London can, for example, as easily gain unauthorised access to a computer in Wall Street as he can to one in Lombard Street. Special jurisdictional rules are thus required and the Commission recommends that a court in England or Wales shall have jurisdiction over the new offences if *either* the offender *or* the computer concerned was, when the offence was committed, in England and Wales.

Conclusion

Legislation based upon the Commission's recommendations may be introduced into Parliament next session or soon thereafter. The new crimes will probably be regarded by some as dangerously wide, but are likely to be welcomed in principle by most computer users.

No one can pretend – certainly the Law Commission do not – that creating the new offences will stop computer misuse. The existence of the crime of theft does not mean that there is no stealing but this is no reason not to have a crime of theft. The Commission hopes that its recommended offences will at least reduce the amount of computer misuse.

Australian Computer Journal

Special Issue

INFORMATION TECHNOLOGY AND THE LAW

CALL FOR PAPERS

The November 1990 issue of the Journal will focus on the interaction between computers and communications, and the law. Topics which the Guest Editors consider to be of particular interest include:

(a) *the application of the law to information technology matters, for example*

- intellectual property law;
- the law of evidence;
- liabilities arising in relation to hardware and software, including contract, negligence and product liability law;
- 'computer crime';
- telecommunications law, both national and international;
- judicial understanding and treatment of information technology matters;
- the teaching of topics in computers and law;
- jurisprudential considerations arising from information technology;

(b) *applications of information technology in support of legal processes, for example*

- matter management systems;
- specialised Office Automation applications, such as document preparation and precedents systems;
- litigation support systems;