Computer Crime: Implications of Recent English Decisions

by Gordon Hughes

The present state of Australia's computer crime laws has been the subject of a previous article by the author in this journal: (1991) No. 15 Computers & Law 15.

Notwithstanding reports of committal proceedings and impending prosecutions, there has been relatively little enforcement activity in Australia, resulting in continuing uncertainty as to the likely application of the various Commonwealth and State laws. For this reason, it may be instructive to consider the implications of recent decisions arising out of prosecutions in England under the *Computer Misuse Act 1990* and the *Criminal Damage Act 1971*.

The Legislation

The *Computer Misuse Act* received royal assent on 29th June, 1990 and came into effect on 29th August, 1990. The key provisions are as follows:

'1(1) A person is guilty of an offence if -

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the accessing he intends to secure is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

2(1) A person is guilty of an offence under this section if he commits an offence under section 1 above ('the unauthorised access offence') with intent -

(a) to commit an offence to which this section applies...

(2) This section applies to offences-

(a) for which the sentence is fixed by law...

(1) A person is guilty of an offence if-

(a) he does any act which causes modification of the contents of any computer; and

(b) at the time when he does the act he has the requisite intent and the requisite knowledge.

(2) For the purposes of subsection 1(b) above the 'requisite intent' is an intent to cause the modification of the contents of any computer and by so doing -

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data.

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 -

(a) alters or erases the program or data; ...[or]

(c) uses it; ...

(3) For the purposes of subsection (2)(c) above a person uses a program if the function he causes the computer to perform -

(a) causes the program to be executed; or

(b) is itself a function of the program...

(7) A modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer -

(a) any program or data held in the computer concerned is altered or erased; or

(b) any program or data is added to its contents;...'

The *Criminal Damage Act 1971* s.1(1) provides that the offence of criminal damage to property is committed where 'a person... without lawful excuse destroys or damages any property belonging to another intending to destroy or damage any such property'.

Prior to the enactment of the *Computer Misuse Act*, the *Criminal Damage Act* s.1(1) was regarded as the most appropriate means of achieving a successful prosecution against a person responsible for erasing or altering programs or data.

The *Computer Misuse Act* ss.1 and 2 are in broad terms equivalent to, for example, the Crimes Act 1900 (NSW) s.309(1) and (2). Section 3 is the broad equivalent of s.310 of the New South Wales legislation.

The situation is different in States such as Victoria which have not legislated specifically in relation to the erasure or alteration of programs or data. The only provision of relevance in Victoria is the *Summary Offences Act 1966* (Vic.) s.9A which provides that a person must not gain access to, or enter, a computer system or part of a computer system without lawful authority to do so.'

Beyond the above provision, any prosecution under Victorian law relating to the unauthorised alteration or deletion of a program or data (including the spreading of a virus) is still governed by the concepts applicable at common law to the offence of malicious damage to property: e.g. *Crimes Act 1958* (Vic.) s.197.

The Cases

In *R. v. Cropp* (unreptd, Snaresbrook Crown Court, 5 July 1991), Judge Agliondy ruled at first instance that the *Computer Misuse Act* s. 1 could only apply where one computer is used to gain access into another. The defendant was charged, inter alia, with unauthorised access to a computer on the basis that he had keyed in commands without authority. The defendant had obtained a 70% discount on goods being purchased from a supplier by accessing a computer used by the sales staff and by entering a false discount when the staff were distracted. The defendant had formerly been employed by the supplier, which was a business of wholesale locksmiths, and in his role as sales assistant was experienced in operating the computer concerned.

The charge was laid under the *Computer Misuse Act*, s.2(1), a pre-condition of which is the commission of an offence under s.1 but with intent to commit or facilitate a further serious offence. The question therefore arose whether the defendant had caused the computer to perform a function with intent to secure unauthorised access 'to any program or data held in any computer'.

It was held at first instance that the purpose of section 1 was to criminalise the common practice of 'hacking', that is, the gaining of unauthorised access to a program or data held in another computer. His Honour considered this could not occur when only one computer was involved. The term 'any computer' meant any computer other than the one to which direct access was obtained. His Honour considered that had parliament intended to include unauthorised access to the computer to which direct access was obtained, the words 'that or any other computer' would have been added.

"The effect of the decision was to remove from the scope of the legislation any persons who are likely to have direct, as opposed to remote, access to a computer system"

His Honour stated:

> 'It seems to me, doing the best that I can in elucidating the meaning of section 1(1)(a), that a second computer must be involved. It seems to me to be straining language to say that only one computer is necessary when one looks to see the actual wording of the subsection, 'causing a computer to perform any function with intent to secure access to any program or data held in any computer'.'

The effect of the decision was to remove from the scope of the legislation any persons who are likely to have direct, as opposed to remote, access to a computer system.

This remarkable judgment was overturned by the Court of Appeal on 16 June, 1992: *Attorney-General's Reference (No. 1 of 1991)*[1992] 3 W.L.R. 432. Lord Taylor C.J. and MacPherson and Turner JJ. applied a literal interpretation to s.1 and concluded that direct access to 'any computer' meant precisely that and there was nothing implicit in the legislation which could lead to the conclusion that more than one computer should be involved.

The Court of Appeal took full account of the intention of the legislation. It accepted the contention on behalf of the Attorney-General that to uphold the acquittal would mean 'there would be nothing in the Act to meet what is itself a mischief frequently encountered today, namely, industrial espionage or obtaining information as to security details or other confidential information which may be stored on a company's computer... [T]he kind of activity of going straight to the in-house computer and extracting confidential information from it could be committed with impunity so far as the three offences in this Act are concerned'

A recent successful prosecution under the *Computer Misuse Act* s.3 was *R. v. Goulden* (unreported, 1992, Southwark Crown Court). The defendant entered an office without authority and installed a security package on the main workstation and included a password known only

to himself. The office staff were subsequently unable to boot up the system and the defendant refused to divulge the password unless payment was made of disputed fees which he was claiming were owed to him. The defendant pleaded guilty and received a two year conditional discharge and a fine of £1,650. It was not disputed that his actions amounted to a 'modification of the contents' of the computer for the purposes of s.3.

There were two cases of significance under the *Criminal Damage Act* before it was superseded for the present purposes by the *Computer Misuse Act*. Although perhaps no longer of significance under English law, the judgments are directly relevant to those Australian jurisdictions which have not legislated in respect of erasing or altering programs or data. The issue arising in such cases is whether the defendant's activities have a sufficiently 'tangible' nexus.

The earlier case, which has been comprehensively discussed in recent years, was *Cox v. Riley* (1986) 83 Cr. App. R. 54. In that case, a conviction was recorded against a defendant who deliberately erased a computer program from the plastic circuit card of a computerised saw so as to render the saw inoperable. The issue was whether erasure of the program caused 'damage' to the printed circuit card. Stephen Brown L.J. of the Divisional Court concluded that it would be 'quite untenable to argue that what the defendant did on this occasion would not amount to causing damage to property'. His Honour rationalised his decision on the basis that the defendant's actions had 'made it necessary for time and labour and money to be expended in order to replace the relevant programs on the printed circuit card'.

A more recent decision was *R. v. Whiteley* (1991) 93 Cr. App. R. 25. From his home address, the defendant had gained unauthorised access to the Joint Academic Network ('JANET') system, a network of connected ICL mainframe computers at universities, polytechnics and science and engineering research council institutions. The defendant had knowledge of the computers concerned and he knew and was able to use the series of commands required for creating, deleting, writing to, opening and closing files. The court was told the defendant had deleted and added files, put on messages, made sets of his own users and operated them for his own purposes, changed the passwords of authorised users and ultimately successfully attained the status of 'SYSMAN', an acronym for Systems Manager, which in turn enabled him to act at will without identification or authority.

The defendant was charged with causing criminal damage pursuant to the *Criminal Damage Act* s.1(1). The defendant admitted the activities but argued they were not unlawful. He asserted that the computers and the disks could not be damaged by the sort of interference he perpetrated. They were designed to perform a particular function and, despite his actions, were still capable of performing that function. Neither the computers nor the disks suffered any physical damage. Any destruction or alteration of information on a disk, or the writing of information to a disk, only affected the information on the disk and did not damage or impair the value or usefulness of the disk itself. Relying in part upon *Cox v. Riley*, the Court of Appeal rejected this argument:

> 'It seems to us that that contention contains a basic fallacy. What the Act requires to be proved is that tangible property has been damaged, not necessarily that the damage itself should be tangible. There can be no doubt that the magnetic particles upon the metal disks were a part of the disks and if the appellant was proved to have intentionally and without lawful excuse altered the particles in such a way as to cause an impairment of the value or usefulness of the disk to the owner, there would be damage within the meaning of section 1. The fact that the alteration could only be perceived by operating the computer did not make the alterations any the less real, or the damage, if the alteration amounted to damage, any the less within the ambit of the Act.'

Conclusion

Perhaps little can be gleaned from the decisions under the *Computer Misuse Act* which is of relevance to Australian jurisdictions. The misguided pedantry of Judge Agliondy in *Cropp* was overturned by the Court of Appeal and in any event no Australian computer crime legislation is expressed in sufficiently similar language such as might encourage the mounting of a similar defence. *Whiteley* is important, however. It is probably of sufficiently pursuasive value to ensure that, in the event of a prosecution in Australia under criminal damage laws relating to the unauthorised erasure or alteration of programs or data, the increasingly limp defence that there has been no 'damage' is unlikely to be raised.

Gordon Hughes is a partner with Lander & Rogers, Melbourne. He is also President of the Victorian Society for Computers and the Law and President of the Law Institute of Victoria.