Computer Crime Laws Update

by Gordon Hughes

This article is a Summary of an address to Victorian Society for Computers and the Law in June, 1993.

Introduction

This paper outlines traditional deficiencies in the criminal law which led to the enactment of computer crime legislation in all Australian jurisdictions in the late 1980s and early 1990s. The paper goes on to outline that legislation. It also assesses the implications of reported cases in Australia.

Traditional deficiencies

Traditional deficiencies in the criminal law as applied to computer crime have been well documented.

The only area of traditional criminal law where courts appear to have succeeded in embracing modern technological phenomena involves the crime of 'malicious damage to property'. All States have laws to the effect that it is an offence to intentionally and without excuse destroy or damage property belonging to another. Based on Canadian (*Re Turner*) and English (*Cox v Riley, R v Whiteley*) decisions, it seems fairly certain that a hacker who, in addition to gaining unauthorised access to a computer system, deletes or alters data, may have committed an offence of 'malicious damage'.

In *Re Turner* (1984) 13 CCC (3d) 430, for example, the defendant gained access to a business competitor's computer tapes and encrypted the information in such a way that access to the data became impossible without knowledge of the new code. The tangible media had not been affected and the data was still accessible, but it was not accessible to the owner of the program. It was held that although the intangible data itself was not 'property' as recognised by the criminal law, the defendant's activities had had an adverse impact upon the rightful owner's use of the tapes themselves, and to this extent there had been a malicious damage to 'property'.

A similar decision was reached in *Cox v Riley* (1986) 83 Cr App R 54, in which the defendant deliberately erased the program from the plastic circuit card of his former employer's computerised saw so as to render it inoperable. Stephen Brown LJ of the Divisional Court concluded that it would be quite untenable to argue that what this defendant did on this occasion would not amount to causing damage to property' and he was particularly influenced by the fact 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'.

The most recent decision of relevance is *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. He 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.'

Summary of effect of traditional laws

It can be deduced from the discussion so far that traditional criminal laws are largely inadequate in regulating the activities of hackers who

gain unauthorised access to computer systems. Only if data is altered or deleted would an offence have been committed. As a result, all Australian jurisdictions found the need to enact legislation dealing with the situation.

Legislation

Attention will be focused in this paper principally upon the adequacy of Australian laws in addressing the problems of unauthorised access and computer viruses.

Victoria - In 1988, the *Summary Offences Act* 1966 was amended and the offence 'computer trespass' was introduced. Section 9A now states:

> 'A person must not gain access to, or enter, a computer system or part of a computer system without lawful authority to do so.'

This amendment directly addresses the deficiencies of traditional criminal laws in regulating unauthorised access. According to parliamentary debate, however, the traditional laws relating to malicious damage to property were considered sufficient to regulate the spreading of computer viruses.

New South Wales - In 1989, the *Crimes Act* 1900 was amended and the offence of 'unlawful access to data in computers' was introduced.

Sub-section 309(1) introduces an offence not dissimilar to the Victorian offence of 'computer trespass'. The legislation then proceeds, however, to some fine distinctions which the Victorian legislation does not contemplate.

Sub-section 309(2) provides a more severe penalty when the obtaining of access is accompanied by an attempt to defraud, to obtain financial advantage or to cause loss or injury.

Sub-section 309(3) imposes a similar penalty where, notwithstanding the absence of such intent, the unauthorised access relates to data classifiable within certain categories, such as confidential government information, personal information, trade secrets and records of financial institutions.

Sub-section 309(4) provides an additional penalty in circumstances where a person, having ascertained that the information obtained without authority relates wholly or in part to the matters referred to in sub-section 309(3), then continues to examine it.

"...traditional criminal laws are largely inadequate in regulating the activities of hackers who gain unauthorised access to computer systems"

On the question of computer viruses, s.310 introduces the offence of 'damaging data', encompassing circumstances where there has been an alteration or other objectively ascertainable interference with electronically stored data.

South Australia - In 1989, the *Summary Offences Act* 1953 was amended to introduce the offence of 'unlawful operation of a computer system'. Section 44 now criminalises unauthorised access to 'restricted access' computer systems.

Under sub-section 44(3), a 'restricted access' computer system is one in which -

> '(a) the use of a particular code of electronic impulses is necessary in order to obtain access to information stored in the system or operate the system in some other way; and
>
> (b) the person who is entitled to control the use of the computer system has withheld knowledge of the code, or the means of producing it, from all other persons, or has taken steps to restrict knowledge of the code, or the means of producing it, to a particular authorised person or class of authorised person.'

The problem of computer viruses has not been specifically addressed.

Western Australia - On 20 December 1990, the *Criminal Law Amendment Act* 1990 the Criminal Code was amended to introduce an offence entitled 'unlawful operation of a computer system' which is expressed in terms similar to the South Australian offence discussed above. The relevant section is s.440A, the only difference in wording being the inclusion of the words 'or set-off codes' after the expression 'particular code' in each sub-clause.

Tasmania - On 11 July 1990 the Criminal Code was amended with the introduction, inter alia, of Chapter XXVIIIA entitled 'Crimes Relating to Computers'. The amendments introduce the offence of 'unauthorised access to a computer' in s.257D:

> 'A person who, without lawful excuse, intentionally gains access to a computer, system of com-

puters or any part of a system of computers, is guilty of a crime."

There is also an offence of 'damaging computer data' (s.257C) which is similar to the *Crimes Act* 1900 (NSW) s.310 and an offence of 'insertion of false information of data' (s.257E):

> 'A person who dishonestly introduces into, or records or stores in, a computer or a system of computers, by any means, false or misleading information as data is guilty of a crime.'

Queensland - Unlike the other States, the Queensland government has, after detailed consideration of the problem of computer abuse, concluded legislation is unnecessary.

The Department of Justice published a Green Paper on Computer Crime in 1987. Particular attention was given to the offence of 'misappropriation of property' under the *Criminal Code* sub-section 408C(1):

> 'Any person who dishonestly applies to his own use or to the use of any person -
>
> (a) property belonging to another; or
>
> (b) property belonging to him which is in his possession or control (either solely or conjointly with any other person) subject to a trust, direction or condition on account of any other person, is guilty of the crime of misappropriation of property.'

The Green Paper expressed the view that this provision was sufficiently broad to embrace the use of computers for unauthorised purposes and the use of a terminal and modem to gain remote access to data banks.

In relation to computer viruses, the Green Paper considered Section 469 of the Code, dealing with unlawful destruction of property, should prove to be adequate.

A.C.T. - On 24 December 1990, the *Crimes Act* 1900 (N.S.W.) in its application to the A.C.T. was amended with the introduction of ss.152 to 154. Section 153 introduces the offence of 'unlawful access to data in computer', whilst s.154 makes it an offence, punishable by imprisonment, to destroy, erase, alter or insert data in a computer or to interfere or interrupt or obstruct the lawful use of a computer.

"Viewed from a national perspective, the resultant regulatory scheme for computer abuse in Australia is quite unsatisfactory"

Northern Territory - Legislation has not been enacted in the Northern Territory dealing specifically with the unauthorised accessing of a computer system. Nevertheless the *Criminal Code* was amended in 1984 to introduce s.276(1) which covers computer-related fraud and establishes the offence of making false data processing material. The mere altering or destroying or manipulating of data processing material with a fraudulent intent a crime. Furthermore, s.222 creates the offence of unlawfully extracting confidential information from a computer with intent to cause harm to another person or to obtain an advantage.

Commonwealth - The *Commonwealth Crimes Act* 1914, which regulates offences involving Commonwealth property or personnel, was amended in 1989 in accordance with the recommendations of an Interim Report on Computer Crime, prepared by the Attorney General's Department. The form of the legislation is consistent with the New South Wales amendments, which preceded the Commonwealth legislation but which were based on the same recommendations.

Sub-section 76B(1) makes it an offence to intentionally gain unauthorised access to data in a Commonwealth computer or Commonwealth data stored in any other computer. Sub-section 76B(2) makes it an offence to commit such acts where the public interest is jeopardised, including circumstances where the defendant ought reasonably to know that personal or commercially sensitive information is being exploited. Sub-section 76B(3) makes it an offence to proceed to examine data once it is known to have been obtained in contravention of the above sub-sections.

Addressing the problem of viruses, s.76C makes if an offence to intentionally destroy, alter or erase data stored in a Commonwealth computer or Commonwealth data stored in any other computer.

Pursuant to the Commonwealth power to regulate telecommunications, s.76E makes it an offence to use Commonwealth telecommunications in order to gain unauthorised access to data, or to maliciously destroy, alter or erase data (whether or not the data is owned by the Commonwealth or stored in a Commonwealth computer). The significance of this offence is that the legislation may on occasions embrace offences which do not involve Commonwealth data or Commonwealth

Out of date - see p26.

computers, thereby providing a backstop provision in circumstances where local State legislation proves to be inadequate.

Overview of Legislative Amendments - Viewed from a national perspective, the resultant regulatory scheme for computer abuse in Australia is quite unsatisfactory.

First, there is little semblance of unity between the various jurisdictions. Secondly, the introduction in most jurisdictions of the bland offence of 'unauthorised access' is a cause for concern. For example, the failure to distinguish between categories of information means the offences could have an extraordinarily wide interpretation. The South Australian legislation distinguishes between types of computer systems but not between types of information; the New South Wales and Commonwealth legislation introduce graduated penalties for serious infractions but still retain 'catch-all' provision at a lower level.

Enforcement

A number of prosecutions have been launched since the introduction of Australia's computer crime legislation.

Victoria

There have been three prosecutions of interest under the *Summary Offences Act* 1966 s.9A.

Belkin - In April 1990, the Prahran Magistrates' Court in Melbourne convicted Alexander Belkin of computer trespass and imposed a fine of $A750.00.

The court was told that Belkin was employed as a computer programmer with GNA Computing Pty Ltd. He was authorised only to use one specific computer and was prohibited from copying programs from other computers. He was discovered by an employee making a copy of a program which he was not authorised to access.

Belkin's counsel argued that the offence of 'computer trespass' should be viewed as something akin to ordinary trespass, for which it was necessary not just to prove an incident had occurred but that it was done with criminal intent. Otherwise the offence could extend to school children operating computers without permission.

According to newspaper reports, however, the magistrate ruled that the law applied 'not only to offences where there was criminal intent, such as computer hacking and theft, but also to regular uses, such as employees'. The magistrate added that whilst the present case had involved a computer program of 'great value', the application of the law would require considerable common sense. 'School children operating computers should not be in jeopardy.'

"The magistrate added... the application of the law would require considerable common sense"

Barylak - The ambit of the 'compute trespass' legislation was again tested by the Prahran Magistrates' Court in the prosecution of Deon Barylak in August 1990. The matter was subsequently the subject of a successful appeal by the defendant to the County Court on 7 February 1991.

The court was told that the defendant, a mature age post-graduate student at Swinburne Institute of Technology, was a qualified accountant who decided to take a year off work in 1989 to complete a diploma in business information technology. As an enrolled student, he had access to a computer laboratory which housed a network of Olivetti M24 twin drive personal computers. At the time he commenced, the network was experiencing intermittent abhorrent behaviour, with students complaining that data was being inexplicably wiped off disks. It seemed that in certain circumstances, a command to format a disk in A drive could in fact cause a disk in B drive to be formatted, with the effect that the data on the disk in B drive would be erased. It was subsequently discovered that this abhorrent behaviour was the result of a 'virus' which could be implanted by using an infected boot diskette. The virus would lodge in the random access memory of the computer concerned and would disappear when the affected computer was turned off.

The defendant was observed by a lecturer one day using four terminals in rapid succession, booting each one up and leaving it turned on. It was apparent he was using a boot diskette not issued by the college. One of the machines was checked and found to contain the 'virus'. When questioned, the defendant admitted he was using his own copy of a boot diskette, not a diskette issued by the college, but he denied knowledge of a virus. He was charged with computer trespass under the *Summary Offences Act* and attempted criminal damage to property under the *Crimes Act*.

In relation to the allegation that he had attempted to gain unauthorised access to a computer system in contravention of s.9A of the *Summary Offences Act*, it was argued that he lacked authority to use the college system in circumstances where he was not using a standard issue boot

diskette. The court accepted the defendant's explanation, however, that he did not lack lawful authority to access the system, being an enrolled student and being a person authorised to be on the premises. He was authorised to use the computer laboratory and the individual terminals on the network. The defendant had flouted the procedural requirement but the prosecution conceded that, if there was no evidence that the defendant had been attempting to spread a virus at the time, a charge of computer trespass could not be sustained as a breach of in-house rules would not deprive a person of lawful authority for the purposes of the section. It was subsequently established, on the facts, that the defendant had not been attempting to spread a virus as there was insufficient evidence that he was aware a virus was on the boot diskette he had copied from another student.

Murdoch - In *DPP v Murdoch* (unreported, Supreme Court of Victoria, 2 October 1992, Hayne J.), the Court dealt with an appeal by the DPP from a Magistrates' Court decision. The respondent was a computer operator who was employed by a bank in its network operations section. He held two accounts with the bank - a Visa credit card was linked to one account and a debit card was linked to the other. Evidence was given that the respondent, without permission, interrupted the connection of the bank's automatic teller machines to the host computer in order to overdraw the account applicable to his Visa credit card. On another occasion the respondent linked his debit card to the Visa credit card account in order to withdraw funds available in that account at a time when funds were not available in the debit card account. He was charged with obtaining property by deception contrary to the *Crimes Act*, s.81(1), computer trespass contrary to the *Summary Offences Act* 1966, s.9A and using a false document country to the *Crimes Act*, s.83A(2). The magistrate found all charges relating to obtaining property by deception provide together with two charges of computer trespass, whilst he found the respondent not guilty of other charges of computer trespass and not guilty of the charges of making and using a false document.

The computer trespass charge raised a pertinent question about what amounts to 'lawful authority'. Uncertainty has been heightened by *Barylak* as to culpability in a situation in which a person authorised to use a computer system disregarded an internal regulation or guideline regarding his or her us of the system - would such a person lack 'lawful authority'?

"The computer trespass charge raised a pertinent question about what amounts to 'lawful authority'"

In *Murdoch* the Court considered whether the respondent, through entering a command to take the central computer 'off host', infringed s.9A - he was authorised to use the system but he clearly lacked express or implied permission to enter this specific command for the purpose for which it was intended.

The magistrate formed a view that the section did not extend to 'internal' abuse of this nature and that the provision instead was intended to prevent entry into a computer system by 'outside persons or hackers'. In the Supreme Court Hayne J. rejected this distinction:

> 'Where, as is the case here, the question is whether the entry was with permission, it will be important to identify the entry and to determine whether that entry was within the scope of the permission that has been given. If the permission was not subject to some express or implied limitation which excluded the entry from its scope, then the entry will be with lawful justification but if the permission was subject to an actual, express or implied limitation which excluded the actual entry made, then the entry will be "without lawful authority to do so"'.

His Honour referred to the second reading speech by the Attorney-General in reaching his conclusion. He added that whilst in the case of entry by an eternal person it would be clear that authority was lacking, it would be necessary in the case of employees to inquire as to the limits of authority given to the employee in relation to using the system:

> 'If he has a general and unlimited permission to enter the system then no offence is provided. If however there are limits upon the permission given to him to enter that system it would be necessary to ask was the entry within the scope of that permission? If it was, then not offence was committed; if it was not, then he has entered the system without lawful authority to do so.'

Whilst this judgement certainly clarifies one aspect of the meaning of 'lawful authority', there are still some other issues which may arise. It remains unclear, for example, whether an employee with unlimited internal authority to use the system infringes s.9A by using the system for an unlawful purpose (such as spread-

ing a computer virus). It also remains uncertain whether an offence is committed in the case of a person who has unlimited authority to use the system but who disregards internal guidelines or procedures as to the manner in which the system may be used.

South Australia

Tester - In July 1990, a computer technician was convicted under South Australia's new 'restricted access' legislation.

The magistrates' court was told that Adelaide University discovered that 388 hours' use of its computer has not been authorised. Authorisation required knowledge of a number, but not a password. It was alleged a technician, Daryl Tester, had obtained a number and used a modem to download confidential information gathered from lectures, including research material, onto his home computer. He was also able to examine the computer's operating system.

The court was told that Tester has stored the informed for 'intellectual purposes' and has not wiped out any data or programs or made use of the information he had obtained.

The defendant was fined $1,500.00. The magistrate indicated that a more severe penalty would have been imposed 'had there been any intention to defraud or damage the Adelaide University computer'.

The case arguably highlights the inappropriateness of the 'restricted access' concept. It is difficult to see how, in this case, the defendant's activities were any more or less culpable by reason of the existence of an authorisation number.

Commonwealth

Jones - On 12 May 1993, Richard Martin Jones appeared before the County Court in Melbourne charged with obtaining unauthorised access to computer data under the *Crimes Act* 1914 (Cth). According to newspaper reports, the defendant has helped penetrate some of the world's highest security computer systems, including forcing 24 hour shutdown of external communications at the Virginia headquarters of NASA. In 1990 he has succeeded in establishing access to the University of Melbourne computer system and, through this, to a series of worldwide computer links, including universities in Finland and the United States and the United States' Naval Research Laboratories in Washington D.C. He had used stolen AUSTPAC and network user identification numbers to use hours of telephone time, with the charges levied against either the University of Melbourne or other OTC subscribers. He had been arrested after scientists at the University of Melbourne became aware of the use of their system and the connections were traced by Telecom. Authorised telephone intercepts had been placed on the defendant's home telephone. It was also alleged that the defendant was knowingly concerned with access to Australia' CSIRO and Lawrence Livermore Laboratories in the US.

Following conviction, Jones was given a six month good behaviour bond and sentenced to 300 hours unpaid community service.

Gordon Hughes is a Partner with Hunt & Hunt, Solicitors, Melbourne, and President of the Victorian Society for Computers & the Law.

IDEAS FOR THE JOURNAL...

BOOKS & JOURNALS

We have increased the coverage of recent books and journals to help keep our readers up-to-date with guides to information in this burgeoning field. If you know of books or journals which we have not covered we would be delighted to hear from you.

IDEAS

Alternatively, if you have ideas for columns or regular features which you think the readers will find useful, please give us a call. We are also open to suggestions as to themes for upcoming issues of the Journal. If you think there are worthwhile topics which we have yet to cover, let us know.

WE RELY UPON YOUR COMMENTS TO PROVIDE A BETTER JOURNAL FOR ALL READERS!