Conclusion

Computer programs contained in silicon chips are protected by the *Copyright Act.* The computer industry must be cautious when importing into Australia any computer equipment containing computer programs unless the ROM is, or forms part of an "integrated circuit" protected by the *Circuit Layouts Act.*

Computer Crime: The Liability of Hackers

• *G. Hughes*
Partner, Lander & Rogers, Melbourne

One of the negative features of the emergence of computers has been the inevitable development of "computer crime". Whilst there are many crimes which can be committed with the aid of computers, one of the most prevalent and potentially most concerning is the increased incidence of unauthorised access to computer systems. Because of deficiencies in traditional criminal laws, new legislation has been enacted or contemplated in all Australian jurisdictions, although the approaches adopted by the various States are far from consistent. This article examines the way in which the law has adapted to regulate the crime of unauthorised access.

Introduction

The advent of the computer age has given rise to many unique legal problems in a diversity of areas. These areas include intellectual property, taxation, privacy, contracts, insurance and crime. Within the area of crime alone, a number of further issues have arisen. Is it "forgery" to copy computerised information? Is it "deception" to extract funds from an ATM without authority? Is it a criminal offence to gain unauthorised access to someone else's databank? This article will concentrate on the last of these issues - the criminal liability of hackers who gain unauthorised access to computer systems.

The criminal law has experienced considerable difficulty in keeping up with the computer revolution. Persons can engage in conduct which was inconceivable a century ago and, as a result, many traditional laws are simply ill-equipped to deal with the situation. It follows that activities which might be regarded as socially objectionable will not be classifiable as criminal offences unless specific legislation is introduced to deal with them.

There are a number of examples of difficulties courts have experienced in attempting to bring unauthorised accessing of computer systems within the ambit of traditional criminal laws.

Theft

It might be thought that the unauthorised extraction of confidential information from a computer system should be regarded as "theft". There are two problems here, however. First, "theft" is a concept which can only be applied to "property", and it has been held that intangible information is not classifiable as "property" for the purposes of the criminal law (*Oxford v. Moss*).

Secondly, "theft" requires an intention to permanently deprive, and even if electronic information were classifiable as "property", it would be difficult to establish that a hacker intended to deprive the rightful owner of it: the rightful owner would still possess the information, even though it had been viewed and perhaps copied by the intruder.

Electricity Offences

Each of the States has a statute which creates an offence of "theft of electricity". These provisions were introduced because the unauthorised extraction or diversion of electricity would not, under traditional laws, amount to "theft" - "electricity" could not be regarded as "property". It has been argued that by

Reprinted from The Australian Computer Journal, Vol 22, No. 2, May 1990 with permission from the Australian Computer Society Inc.

gaining access to someone else's computer system without permission, a hacker is causing an unauthorised use of electricity in relation to that system and is therefore guilty of the offence. The argument has been rejected in a minor Hong Kong case (*R v. Sui Tak-Chee*) and, whether or not it is in fact sustainable, it is clearly not the purpose for which the offence was originally drafted.

Fraud

It is sometimes asserted that a person who gains unauthorised access to a computer system by usurping the access code of an authorised user should be adjudged guilty of "fraud" or "deception". There have been several cases in recent years in which the issue has been raised (*Kennison v. Daire, R. v. Evenett, R. v. Baxter*) and it has been asserted by the defence from time to time that it is illogical to talk of "deceiving" a machine. This defence has not been enthusiastically received, however, and it seems the court will find, by one route or another, that the machine is an extension of the rightful owner and that to defraud the machine is therefore to defraud the owner. The argument nevertheless has little application to intrusive hackers as the "fraud" and "deception" offences all relate to the misappropriation of "property", usually money. They contemplate for example, the extraction of funds from an ATM through the use of someone else's PIN number. Where mere intangible information is involved, a "fraud" or "deception" can probably not be committed.

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

Forgery

In one celebrated English case (*R. v. Gold*), two hackers were prosecuted under British forgery provisions. The defendants gained unauthorised access to British Telecom's Prestel information system by keying in the customer identification numbers and passwords of authorised users. They were charged with forgery on the basis that they had, in the words of the statute, made a "false instrument" when altering the segment by means of the electronic impulses keyed into the system. It is not necessary in this paper to closely analyse the bases upon which the prosecution's ingenuity was demolished by the Court of Appeal and again by the House of Lords. Suffice to say that the judges found a number of flaws in the prosecution's arguments and they emphasised that clearly the Act in question had never been intended to apply in this type of situation.

Malicious Damage

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*) 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*, 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*, 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.

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, most Australian jurisdictions have found the need to enact legislation dealing with the situation.

The enactment of "computer abuse" legislation has, however, not been without controversy, principally because there appears to be a significant element amongst the decision-makers who maintain that mere unauthorised access without other devious intent should not be made a criminal offence. Supporters of this philosophy argue that as it is not a criminal offence *per se* to look inside someone else's filing cabinet or to read a letter which is sitting on their desk, it is illogical to create a criminal offence applying to circumstances where the information is stored in electronic form.

The alternative philosophy is that information stored on computers is considerably more vulnerable than manually stored data and hence warrants specific legal regulation.

" ... there appears to be a significant element amongst the decision-makers who maintain that mere unauthorised access without other devious intent should not be made a criminal offence"

It was originally contemplated by the Standing Committee of Attorneys-General that each State would enact uniform laws in relation to computer abuse generally. These plans fell through, however, principally because a common philosophy could not be established in relation to the criminality of hackers in certain situations. As a result, each State has been left to determine its own requirements in relation to computer abuse legislation generally, and in relation to the question of unauthorised access specifically.

Some of these initiatives can now be reviewed.

Victoria

Victoria was the first State to introduce comprehensive computer abuse amendments. In 1988, the *Crimes Act* was amended in a number of respects, although these amendments had little to do with the issue of unauthorised access. More significant were the simultaneous amendments to the *Summary Offences Act*, into which the offence of "computer trespass" was introduced:

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

It was the government's original position that the unauthorised use of a computer system not involving criminal intent and harmful consequences should not be criminalised. This position was altered, ostensibly following "extensive consultation .... with the computer industry, banks, business organisations, legal experts, police and other interested groups". More significantly, however, the Opposition held the majority in the Upper House and had forcefully indicated it favoured the criminalisations of unauthorised access *per se* - the "computer trespass" amendment ensured the safe passage of the entire legislative package.

New South Wales

The New South Wales *Crimes Act* was amended in 1989 to embrace the general problem of computer abuse, and one of the new offences is "unlawful access to data in a computer". It is a *prima facie* offence to gain access to a program or data stored in a computer without lawful authority or excuse. A more sever penalty applies in circumstances where the obtaining of access is accompanied by an intent to defraud, to obtain financial advantage or to cause loss or injury. A similar penalty is imposed where, notwithstanding the absence of devious intent, the unauthorised access relates to data which is classifiable within certain sensitive categories (such as confidential government information or trade secrets). A further penalty applies where a person, having ascertained that data accessed without authority falls into one of these specified categories, then continues to examine it.

" ... the Commonwealth has been able to criminalise activities involving unauthorised access to private computers by means of Commonwealth communication facilities"

South Australia

During 1989, the *Summary Offences Act* was amended to include the offence of "unlawful operation of a computer system". The legislation criminalises unauthorised access to "restricted access" computer systems. These systems are ones which the use of a particular code is necessary in order to gain authorised access. The amendment is open to criticism on the basis that it makes an illogical distinction between sensitive data which may be fortuitously protected by a password or other access codes, and data which is not so protected. On the other hand the British Computer Society recently expressed support for the "restricted access computer system" concept when formulating its response to a Law Commission paper on Computer Abuse.

Western Australia

On 20th December, 1990 the Criminal Code was amended with the insertion of a new section 440A. This section introduces the offence of "unlawful operation of a computer system" and is expressed in the same terms as the corresponding South Australian amendment.

Queensland

In 1987, the Queensland Department of Justice published a Green Paper on Computer Crime in which, *inter alia*, certain provisions in the Queensland *Criminal Code* were analysed for their adequacy in dealing with a variety of forms of computer abuse. The Paper expressed the view that the *Code* already embraced, most likely, the activities of persons who used computers for unauthorised purposes or who used a terminal and modem to gain remote access to a databank. The Paper added that if such an interpretation were not correct, then unauthorised accessing of data *per se* should be criminalised as a matter of governmental policy. No legislation has subsequently been enacted, however.

The Territories

The Northern Territory *Criminal Code* contains the offence of "making false data processing material". This addresses the activities of any person who unlawfully alters, falsifies, erases or destroys any data. It also embraces the unlawful extraction of confidential information from a computer with intent to cause loss to a person or with intent to publish the same to a person not lawfully entitled to receive it. Unauthorised access *per se* is not, however, criminalised.

In the Australian Capital Territory, the *Crimes (Amendment) Act (No. 3) 1990,* which came into effect on 24th December, 1990, introduced the offence of "unlawful access to data in a computer", making it an offence to obtain access to data stored in a computer "intentionally and without lawful authority or excuse". The amendment further provides that it is an offence to destroy, erase, alter or insert data into a computer, or interfere with the lawful use of a computer. The amendments therefore mirror, to a limited extent, the corresponding provisions under the New South Wales *Crimes Act.*"

Tasmania

Amendments to the criminal law, which would embrace unauthorised access, have been mooted. At the time of writing, however, no legislation has materialised.

Commonwealth

In 1989, amendments were introduced to the Commonwealth *Crimes Act*, the form of which is largely mirrored in the New South Wales legislation discussed above. There are some aspects of the Commonwealth legislation, however, which are particularly significant as they have the capacity to embrace the activities of persons who might otherwise be subject only to State jurisdiction and not

Commonwealth criminal jurisdiction. Relying on the constitutional power to legislate with respect to postal, telegraphic, telephonic and other like services, the Commonwealth has been able to criminalise activities involving unauthorised access to private computers by means of Commonwealth communication facilities. Accordingly, the Commonwealth legislation could be effective in creating criminal liability in circumstances where States have not proscribed unauthorised access *per se* and where such access has been gained through the use of a telecommunication system.

Conclusion

Clearly there has been significant legislative activity in nearly all jurisdictions in recent times. Interestingly, a majority of jurisdictions appear prepared to accept that unauthorised access to a computer system, even when unaccompanied by any devious intent, should be criminalised. This seems to represent a philosophical shift away from the position adopted formally by some States two or three years ago. It is a reflection, presumably, of perceived community concern that electronically stored information is uniquely vulnerable to abuse and that persons responsible, therefore, should be the subject of criminal penalties. It will be interesting to observe, over the ensuing years, whether many prosecutions are launched, and if so, whether the legislation is demonstrated to have been adequately drafted.

" ... there has been significant legislative activity in nearly all jurisdictions in recent times"

Finally, it should be emphasised that this paper has only dealt with the question of criminality, not the equally complex issue of civil liability for damages. Can a person be sued for nuisance, misrepresentation or conversion as a result of gaining unauthorised access? Can a computer operator or database owner be sued for negligence if suitable preventative measures are not implemented? How effective is the federal *Privacy Act* in safeguarding data stored in Commonwealth owned computers? These issues are beyond the cope of this paper, but are clearly of direct relevance to all those affected by the storage of information on computers.

References

COX v. RILEY(1986): 83 Cr. App. R. 54.

Crimes (Amendment) Ordinance (No. 4) 1985 (A.C.T.), No. 44 of 1985

Crimes (Computers) Act 1988 (Vic.), No. 36 of 1988

Crimes (Computers and Forgery) Amendment Act 1989 (N.S.W.), No. 71 of 1989

Crimes Legislation Amendment Act 1989 (Cth), No. 108 of 1989

KENNISON v. DAIRE (1986) 60 A.L.J.R. 249

OXFORD v. MOSS (1978) 68 Cr. App. R. 183

Privacy Act 1988 (Cth), No. 119 of 1988

R. v. BAXTER (1988) 2 Qd. R. 537

R. v. EVENETT (1987) 2 Qd. R. 753

R. v. GOLD (1988) 2 W.L.R. 984

Re TURNER (1984) 13 C.C.C. (3rd) 430

Summary Offences Act Amendment Act ,1989 (S.A.), No. 50 of 1989

Biographical Note

Gordon Hughes LL.M, Ph.D is a partner at the Melbourne law firm of Lander & Rogers, practising exclusively in the area of computer law. He is the co-author of "Computer Contracts: Principles and Precedents" (Law Book Company, 1987) and Editor of "Essays on Computer Law" (Longman, 1990). He is also Chairman of the Law Office Management Section of the Law Institute of Victoria.