When is a computer not a computer

*Scott Standen and Tanya Fryc, Arnold Bloch Leibler Lawyers**

Scott Standen has extensive commercial experience. His practice covers the spectrum of corporate and commercial matters and has particular focus on biotechnology and information technology. Tanya Fryc is a member of the Technology Group and has experience acting in both general commercial and litigation matters. She has significant knowledge of issues relating to the telecommunications industry and has a focus on biotechnology and information technology.

Introduction

The New South Wales Government has recently introduced the *Crimes Amendment (Computer Offences) Bill 2001* into parliament which proposes the introduction of additional computer crimes. In light of the introduction of this Bill and recent publicity regarding computer crimes, it is topical to consider the ambit of existing and proposed legislation dealing with computer crime in Australia. In particular, it is relevant to consider the question of whether such existing or proposed legislation prohibits offences involving handheld devices, or other data storage devices such as "smart cards".

Gartner Group's Dataquest[1] predicts that by 2004, the worldwide sales of handheld devices will quadruple to 32 million units, taking the market to US$7.2 billion. With businesses requiring mobility and customers demanding anywhere, anytime commerce, mobile technology has very quickly become a part of every day use and will continue to grow in importance.

The recent outbreak of computer viruses, such as the "Love Bug" and "Melissa" viruses has drawn significant public attention to the fact that computer networks are not infallible and that the infiltration of those computer networks is becoming an ever increasing phenomenon.

Although the technology associated with handheld devices is relatively new, "*...viruses aimed at handheld devices do pose a threat at this point, and ... that will only increase as the number of these items grows...*"[2] PalmPilot and other similar handheld devices have been available for some time. Last year, the "Liberty" and "Phage" viruses targeted and destroyed files and programs on PalmPilot devices. Owners of PalmPilot devices were offered software that they believed would convert their freeware program into a full featured, registered version. However, when those owners sought to download that software, they downloaded the "Liberty" virus and all data was erased from their PalmPilot device. The "Phage" virus followed the "Liberty" virus, and also erased files from PalmPilot devices.

According to X-Force, the internal R&D arm of Internet Security Systems,[3] internet enabled mobile telephones have been fairly untouched to date, with only a few viruses targeting digital phone networks surfacing in Spain and Germany.[4] However, that does not appear to have prevented security analysts being extremely concerned with the vulnerability of such devices.[5]

The issues described in the preceding paragraphs have heightened the community's need to determine a way to prevent computer crime generally. The task of preventing computer crime will, of course, continue to be primarily tackled on the technological front, through the development of anti-virus protection software. However, the legislature has also sought to provide a disincentive for such activities, through the enactment of legislation prohibiting computer crime.

This article focuses on the question of whether legislative changes have gone far enough to enable successful prosecutions of crimes involving handheld and other data storage devices such as "smart cards". In order to provide some answers to this question, this article will consider the present state of legislation relating to computer crime in Australia (at the Commonwealth level and in Victoria and New South Wales), together with the proposed New South Wales legislation, and then consider specifically, the extent to which such legislation deals with offences against handheld and other data storage devices such as "smart cards".

Current Legislation

The United Kingdom and United States of America have had legislation specifically directed at computer related crimes for more than 10 years. Australia has been slower in adopting specific legislation and has to date had divergent approaches throughout the various State, Territory and Federal jurisdictions.

(a) Commonwealth

In 1989, the Commonwealth inserted Part VIA into the *Crimes Act 1914 (Cth)*. Part VIA specifically deals with offences relating to computer crime and contains provisions that are applicable to a "Commonwealth Computer", being "...a computer system or a part of a computer system, owned, leased or operated by the Commonwealth..."[6], or, data stored on behalf of the Commonwealth.

Part IVA of the Act contains provisions prohibiting the following acts:

- intentional and unauthorised access of data in a Commonwealth Computer and data stored on behalf of the Commonwealth in other computers;[7]
- intentional and unauthorised damaging of data in a Commonwealth Computer and data stored on behalf of the Commonwealth in other computers;[8]
- intentional and unauthorised access of data in a computer by means of a facility provided by the Commonwealth or a carrier[9]; and
- intentional and unauthorised damaging of data in a computer by

means of a facility provided by the Commonwealth or a carrier.[10]

Sections 76D and 76E of the Act apply broadly to any person who, without authority, gains access to or damages data stored in a computer by means of a facility operated or provided by the Commonwealth or a carrier. "Carrier" and "facility" are given the meanings ascribed to those terms in the *Telecommunications Act 1997 (Cth)*, which in summary, are respectively defined as the holder of a carrier licence, and, any part of a telecommunications network or any equipment used or for use in a system that carries or is capable of carrying communications by means of guided and/or unguided electromagnetic energy. The effect of these provisions is to make all unauthorised remote access or damage caused remotely by a person to data stored in a computer an offence under the Act, as all such access is likely to be obtained by means of a facility provided by a carrier (for example, via telecommunication networks, including mobile telephone networks).

(b) New South Wales

The *Crimes Act 1900 (NSW)* was amended to insert an additional Part 6, which deals with offences relating to computers.

Section 309 of the Act makes it an offence for a person to, without authority, gain access to a program or data stored in a computer.

Section 310(a) of the Act makes it an offence to damage data in a computer. However, as the section also makes it an offence to insert data into a computer, it appears that damage does not necessarily have to be caused in order for an offence under the relevant provision to occur. Therefore, inserting any information into a computer without authority will constitute an offence under this section.

Section 310(b) of the Act states that it is an offence if someone *"..interferes with, or interrupts or obstructs the lawful use of a computer.."*.[11] According to the Model Criminal Code Report, this provision is too broad as it prohibits any interference or obstruction with the use of a computer.[12] Ultimately, this means that conduct, such as locking a door to a computer room, that would normally 'fall short of minimum levels of wrongdoing'[13] could theoretically be penalised under this section.

(c) Victoria

The Victorian legislature, unlike its New South Wales and Commonwealth counterparts, has simply amended already existing criminal damage provisions of the *Crimes Act 1958 (Vic)*[14] to deal with computer crime. Section 197 of the Act deals with 'destroying or damaging property'. It makes it an indictable offence to intentionally and without lawful excuse, or dishonestly with a view to gain for oneself or another, destroy or damage any property belonging to another. The approach taken by the Victorian legislature appears to be based on the English decisions of *Whitely*[15] and *Cox v Riley*[16], which considered that damage to data in a computer could constitute criminal damage for the purposes of the relevant English legislation. In those cases, the Courts held that the rearrangement of the magnetic particles on the disk caused damage to the computer disk or storage device and therefore constituted an offence.

In the authors' view however, these cases, by focusing on the physical device, rely on an artificial interpretation of events and fail to acknowledge that the data itself is valuable. In addition, this approach may well prove to be insufficiently flexible to deal with new technologies.

In addition to the above, Sections 81 and 82 of the Act provide that it is an offence for a person, by any deception, to dishonestly obtain property or a financial advantage. These offences potentially encompass computer crimes since "deception" is defined as including *"... an act or thing done or omitted to be done with the intention of causing a computer system, ... to make a response that the person doing or omitting to do the act or thing is not authorised to cause the computer system or machine to make."*

Finally, the *Summary Offences Act 1966 (Vic)* includes a provision making it an offence for a person to engage in computer trespass.[17] Section 9A of that Act 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." Again, neither the term "computer", or, "computer system" is defined in that Act, necessitating that recourse be had to the courts to determine what either or both of those terms mean for the purposes of that section.

Scope of legislation: does it extend to offer protection to offences against handheld devices?

It is clear from the discussion above that Federal and State Governments in Australia have created different offences to tackle the problem of computer crime. In addition, generally speaking, the current legislation is dependant upon making a determination as to what constitutes a "computer". All of the jurisdictions discussed above have left the determination of what constitutes a "computer" to the courts.

In the past, the Law Reform Commission of Tasmania[18] proposed a definition of "computers" for adoption in Tasmania (although this was not ultimately included in any legislation), which provided as follows:

> *"A computer is, an electronic device that performs logical, arithmetic, and memory functions by the manipulation of electronic or magnetic impulses and includes all input, output, processing, storage, computer software and communication facilities that are connected or related to a computer."*

The above definition was not ultimately accepted.

The United States legislature has included a definition of computer in Section 1030(e) of the *Computer Fraud and Abuse Act 1986 (US) 18USC* as:

> *"..an electronic, magnetic, optical electrochemical, or other high speed data processing device 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, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device."

Although this is quite a broad definition, and may be sufficient to cover handheld devices, such as PalmPilot devices, the definition limits the scope of what constitutes a "computer". Moreover, in light of rapid technological change, this definition may not be sufficiently flexible to encompass emerging technologies. Ultimately, it is questionable whether a "smart card" would be a "...data storage facility...directly related to or operating in conjunction with.....an electronic, magnetic, optical electrochemical or other high speed data processing device performing logical, arithmetic or storage functions..." (emphasis added).

The term "computer" is also left undefined in the United Kingdom *Computer Misuse Act (1990)* (the "**UK Act**"). It is, as Martin Wasik notes,[19] left to its ordinary meaning, and again, on a case by case basis, the courts must determine what is and what is not covered by that legislation.

The United Kingdom has had cases dealing with the above legislation, but nothing specifically related to the question of whether the definition of "computer" could extend beyond the realms of what is generally understood as a traditional computer, to devices such as PalmPilot type devices, mobile phones and "smart cards".

The Macquarie Dictionary defines a computer as "an apparatus for performing mathematical computations electronically according to a series of stored instructions called a program".

Arguably, the concept of a computer does not extend to storage devices such as "smart cards" and other access and data storage devices. This fact may prove to be a deficiency in the legislation, especially in light of the emergence of a trend towards the separation of data storage and functionality. Microsoft's Net Vision, in which software will be hosted remotely on an application service provider and data stored on the user's device, is one example of this trend. The adoption of "smart cards" which store data also reflects the separation between data storage and functionality.

This separation between data storage and functionality is an important one and in the authors' view, legislation ought to be directed at protecting the integrity and security of both aspects of the technology. Certainly, the functional characteristics of a computer are important, and any interference with the proper functioning of a computer is appropriately the subject of an offence. However, the integrity and security of data is also important and deserves legislative protection without artificially limiting that protection by reference to the device in which that data is stored.

NSW Amendment Bill

In a press release about the Model Criminal Code, the Minister for Justice and Customs, Senator Amanda Vanstone said, "*[w]ith the rapid move to widespread use of electronic communications in the Australian economy and the rise of the Internet to handle such things as shopping and banking, the security and reliability of these networks becomes extremely important to our economic well-being.*"[20]

The Model Criminal Code is based on the UK Act and contains specific legislation targeted at computer crimes.

The Model Criminal Code Report which recommended the introduction of the Model Criminal Code stated that "[t]here are few areas of current legislative concern in which the need for uniformity of approach in the formulation of criminal offences is more desirable or more pressing."[21]

The above reasoning would appear to be sensible since, for obvious reasons, computer crime frequently extends beyond State boundaries, and, the existing legislative variations mean that there is an inadequately co-ordinated approach to dealing with these issues within Australia.

Recognising the need for uniformity, New South Wales introduced into Parliament in early April of this year the *Crimes Amendment (Computer Offences) Bill* 2001. The offences spelt out in that Bill follow those in the Model Criminal Code. The object of the Bill is to "...enact modern computer offences under the Crimes Act 1900...".[22]

The Bill includes provisions prohibiting the:

- causing of any unauthorised computer function, including unauthorised access to, or modification of, data held in a computer, or, the unauthorised impairment of electronic communication to or from a computer, knowing that it is unauthorised and with the intention of committing a serious offence;[23]
- unauthorised modification of data held in a computer with the intent to cause impairment;[24]
- unauthorised impairment of electronic communication to or from a computer;[25]
- possession or control of data with an intent to commit a computer offence;[26] and
- production, supply or obtaining of data with an intent to commit a computer offence.[27]

Under the proposed Bill it is also an offence to "devise, propagate or publish"[28] a computer virus. The relevant intention of the offender is important in this instance, as the offender must have intended to commit a computer offence, that is, through the unauthorised access, modification, or impairment of electronic communications, or have intended to "devise, propagate or publish" a computer virus.

Section 308D of the Bill, according to the Minister's Second Reading Speech,[29] covers a broad range of offences. For instance, it makes it an offence for a person with limited authorisation to impair data or programs by performing an unauthorised act. In addition, the section also makes it an offence to obtain unauthorised access to, and cause damage to data, such as by circulating a virus which infects a computer. Section 308E of the Bill

may also be relied on in respect of conduct that has resulted in economic loss or disruption of business. Both of these sections impose liability for reckless as well as intentional behaviour, in addition to which, Section 308D of the Bill extends to prospective impairment.

The Bill also includes summary offences for unauthorised access to, or modification of, restricted data held in a computer,[30] and the unauthorised impairment of data held in a computer disk, credit card or other device used to store data by electronic means.[31] The insertion of Section 308I appears to be an attempt to ensure that damage done to devices such as "smart cards" can be prosecuted .

However, the application of Section 308I to a "computer disk, credit card or other device", rather than a "computer", potentially raises a presumption that the use of the term "computer" in other sections of the Bill does not extend to devices such as "smart cards".

Section 308I allows for prosecutorial discretion to proceed against relatively minor offences summarily. However, the introduction of the terminology "data held on a computer disk, credit card or other device used to store data by electronic means" may be problematic. Sections 308D and 308E are directed at conduct relating to "data held in a computer",[32] which is defined to include data held in any removable data storage device for the time being in the computer".[33] Therefore again, one is faced with the task of determining what is a "computer". For example, does a computer include a device that simply reads the data in the smart card?

The Model Criminal Code Report states that:

> "...'Smartcards', which might be described as a 'device[s] to store data by electronic means' are, in reality, minaturised computers. Both the indictable and summary offences are capable of applying to conduct which modifies data held on the smart card..."[34]

Despite the view expressed in the Model Criminal Report, it is not certain that a "smart card" is a computer, as it does not perform any logical or arithmetical calculations, being simply an information repository. Sections 308D and 308E of the Bill apply to "data held in any removable data storage device for the time being in the computer" (which is likely to include a "smart card"), but will only capture conduct which occurs while that device is in a computer. Section 308I of the Bill applies to any conduct that damages data in these devices, irrespective of the manner in which that conduct occurs.

Ultimately, the authors consider that it is open to debate as to whether the term "computer" will be read down as a result of the broader terminology contained in Section 308I of the Bill.

Where the criminal activity relates to a handheld device, it would appear that a successful prosecution will depend upon whether the handheld device, such as a mobile telephone or a PalmPilot device, or even a "smart card", is:

- a computer; or
- a data storage device and the offence occurs in relation to data on that device while it is in a computer.

Consistent with the current legislation discussed above, and the approach adopted by the UK Act, the Bill makes no attempt to define the term 'computer'. Instead, the Model Criminal Code Report[35] concludes that "...statutory definitions are likely to prove both under inclusive and over inclusive...".[36] In the authors' view, there is a lot of sense in this conclusion. Attempting to define a "computer" according to today's understanding of what is (or could) constitute a "computer" could result in such definition being under inclusive in that the definition of a "computer" may not include a device of tomorrow that performs all the functions of what is understood today as a computer. It could also be over inclusive as computerised components are now being used in every day appliances, and it may not be necessary, or appropriate, depending on the circumstances of the case, to characterise such devices as "computers".

The Committee set up to establish the Model Criminal Code ultimately concluded that "... the scope of the offences cannot be determined by restrictive definition of what is and what is not a 'computer'...".[37] Therefore, the definition of "computer" is left to the 'process of judicial interpretation'. However, the task of determining what constitutes a "computer" is problematic, relying very much on expert evidence as to the state of technology at the relevant time, and, the circumstances of the case at hand.

Should the definition of "computer" be left open?

The authors endorse the approach to leave the definition of "computer" to judicial interpretation. In this way, legislation is flexible and adaptable to changes in technology. If the legislation were to seek to provide a definition for 'computer' there is the very real possibility that in a few years it would be outdated. Technology changes constantly and it would be extremely difficult for the legislature to enact legislation today that will still be relevant for tomorrow's technology. As the ordinary meaning of "computer" changes, so too will the meaning of what constitutes computer crime for the purposes of the relevant legislation.

There is, however, a distinct gap in the current state of the legislation discussed in this article, which has generally linked computer offences to conduct against the "computers". It is quite clear however, even from the state of technology at this point in time, that devices such as "smart cards", for instance, whilst arguably not "computers" (although note the comments of the Model Criminal Code Report above, in this regard) for the purposes of the relevant legislation (since they are arguably merely information repositories), may nonetheless become the subject of unauthorised access . How will such offences be looked upon by the courts? Possibly, the fact that such technologies are not considered computers may mean that offences against such technologies will remain unpunished. Perhaps the only attempt to deal with such devices to date has been in the *Crimes Amendment*

(Computer Offences) Bill 2001 (NSW), which has included summary offences provisions in Section 308I of the Bill relating to offences against "smart cards" and the inclusion of "smart card" style devices in the definition of "data held in a computer".[38] However, this Bill is obviously not the present state of the law, having not been passed by the New South Wales parliament, and neither have there been any steps on the part of the other legislatures discussed in this article to adopt similar legislation to the New South Wales Bill.

Conclusion

The existing and proposed legislation in Australia reviewed in this article is generally directed at prohibiting certain conduct involving "computers". Appropriately, this term is left to its ordinary meaning, ensuring the legislation retains the scope to adapt to changing technology. In most instances, handheld devices such as mobile phones and PalmPilot style devices, are likely to be regarded as a computer and covered by the legislation. However, by revolving around a "computer" rather than addressing the integrity of the data, irrespective of the technological method of storage, the legislation arguably may not, in many cases, prohibit conduct directed at devices such as "smart cards".

As the emerging trend towards separation of data storage and processing continues, the legislation may provide inadequate protections. The authors contend that the legislation should be amended to make it clear that the data protection provisions of the legislation include devices such as "smart cards", or, to enable the relevant Minister to declare a device is included in the term "computer" for the purposes of the relevant legislation.

---

* The authors would like to acknowledge the research assistance of Dov Paluch, Articled Clerk and the guidance of Michael Dodge, Head of the Technology Group and Partner of Arnold Bloch Leibler Lawyers and Advisers.

1 As referred to at http://www4.gartner.com/Init.

2 Larry Rogers, Senior Member of the Technical Staff at the US Government's Computer Emergency Response Team (as referred to at http://www.cert.org).

3 As referred to at http://www.iss.net.

4 Ibid.

5 Ibid.

6 Section 76A, Part IVA, Crimes Act 1914 (Cth).

7 Ibid, Section 76B.

8 Ibid, Section 76C.

9 Ibid, Section 76D

10 Ibid, Section 76E.

11 As does Section 76C(b) of the Crimes Act 1914 (Cth).

12 Model Criminal Code Report, Report of the Committee, January 2001, Chapter 4 Damage and Computer Offences, at page 161.

13 Ibid.

14 Section 197, Crimes Act 1958 (Vic).

15 Whitley (1991) 93 Cr App R 25, at 28 per Lord Lane CJ.

16 Cox v Riley (1986) 83 CR App R 54.

17 Section 9A, Summary Offences Act 1966 (Vic).

18 Report on Computer Misuse, Law Reform Commission of Tasmania, Report No 47 of 1986.

19 M. Wasik, Crime and Computer (1991), Appendix 4, as referred to in the Model Criminal Code Report, op.cit, at page 123.

20 Senator Amanda Vanstone, Minister for Justice and Customs, New Computer and Bushfire Offences Feature in Model Criminal Code, Media Release, Saturday 12 February 2000 as referred to at http://law.gov.au/aghome/agnews/2001newsag/2000newsjus/19_00.htm.

21 Model Criminal Code Report, op.cit., at page 6.

22 Crimes Amendment (Computer Offences) Bill 2001, Explanatory Notes.

23I bid, Section 308C.

24 Ibid, Section 308D.

25 Ibid, Section 308E.

26 Ibid, Section 308F.

27 Ibid, Section 308G.

28 Model Criminal Code Report, op.cit., at page 184.

29 NSW, Mr Debus, Attorney General, Minister for the Environment, Minister for Emergency Services, and Minister Assisting the premier on the Arts, Second Reading Speech, Legislative Assembly, 4 April 2001.

30 Refer to Section 308H.

31 Refer to Section 308I.

32 This is a defined term under the Crimes Amendment (Computer Offences) Bill 2001.

33 Refer to the definition referred to in the previous footnote.

34 Model Criminal Code Report, op.cit., at page 199.

35 Op.cit.

36 Model Criminal Code Report, op.cit., at page 123.

37 Ibid, at page 129.

38 refer to footnote 32.

What's New

Submission of the Legislative Watch SubCommittee of The New South Wales Society for Computers & the Law in relation to the

Crimes Amendment (Computer Offences) Bill 2001(NSW)

For a full text copy of this submission please visit the society's website at: http://www.nswscl.org.au