Is Australian Criminal Law up to the threat of computer viruses?

Patrick Ling, Graduate at Law

1 INTRODUCTION

As the use and dependency upon computers and the internet rapidly increases, the incidence of criminal activity has also risen. This poses a serious problem for criminal law enforcement since the current framework has largely evolved without adequate consideration of computer related crime.

Although computer crime refers to a whole range of different activities, one form which has received widespread media coverage in recent times is the computer virus.

The worldwide spread of the 'Melissa virus' and 'Love bug' raises the question as to whether a successful prosecution under our existing laws could be achieved against the creator and distributor of such a virus.

The following discusses the nature of computer viruses, examples of computer viruses, the prosecution of virus creators and distributors, the current legal regime in Australia and new computer related offences proposed under the Criminal Code.

2 WHAT IS A COMPUTER VIRUS?

A computer virus is a software program written with malicious intentions and designed to replicate itself by attaching to files or disks. Viruses usually contain two parts, a self-replicating code and a 'payload' which delivers side effects. The payload may vary from a relatively harmless prank such as a message or cartoon to one which alters or destroys files.

Viruses are primarily transmitted from one system to another in two ways, contaminated disks which are used in clean computers and via telephone lines. With the increased usage of the internet and email, the rate at which viruses can be spread to computers anywhere in the world poses a greater risk to computer users compared to virus transfer via infected floppy disks.

Viruses come in different forms including worms and trojan horses. Worms replicate themselves once infecting a computer and continue to do so until the operation of the computer is slowed to a standstill. Trojan horses such as Back Orifice give remote access of the infected system to users over the internet without the knowledge of the victim. Once the program is installed on the computer, all files and even passwords which are available to the authorised user are capable of access by the outsider.

3 VIRUSES: CREATORS, EFFECTS AND LIABILITY

Despite the wide proliferation of computer viruses, few have caused enough damage to warrant prosecution. The following is a brief discussion of various computer virus cases.

3.1 US v Morris

Robert Morris, was convicted under the *Computer Fraud and Abuse Act 1986 (US)* of releasing a worm onto the internet. The worm caused widespread damage to hundreds of computers at the Massachusetts Institute of Technology.

The Court found that Morris had the intention to spread the worm and obtain unauthorised access to other computers. Although Morris claimed a lack of intention to cause harm, the Court held that to be irrelevant since the intention related to access to computers rather than intention to cause damage. Morris was fined and sentenced to three years probation and community service.

[United States v Morris, 928 F.2d 504 (2d Cir. 1991) cert. Denied, 502 US 817 (1991)]

3.2 Melissa Virus

The Melissa virus infected computer networks in March 1999 via emails which contained an infected attachment. The subject of the message stated 'Here's the information you requested' and directed the reader to open the attached word document.

If the attachment was opened using Microsoft Outlook, the virus would send copies of the infected document to the first 50 email addresses in the user's address book. What made the virus more destructive was that these addresses often contained groups of users.

The virus was estimated as having spread to 50,000 computers in less than 10 minutes. Although the virus caused little damage to data and files, the costs were high as a result of lost productivity whilst overloaded networks were repaired.

David L Smith was arrested after a six day manhunt which was headed by the FBI. He was charged with various State and Federal offences including interruption of public communication, theft of computer services and wrongful access to computer systems.

Smith pleaded guilty to creating the virus and acknowledged that the cost of his actions exceeded $US80 million thus triggering tougher Federal sentences. Smith faces imprisonment of up to 40 years and a fine of US$480,000 although concurrent serving of state and federal terms may see the length of his imprisonment significantly reduced.

3.3 The Love Bug

The Love bug was similar to the Melissa virus but caused greater damage by attaching itself to every entry in the user's address book. Once opened, the attachment also destroyed selected files on the user's computer.

With over 45 million computers infected, estimates of the damage caused by the Love Bug have reached over $A25 billion (most of which was uninsured). Victims included home computer users as well as large corporations and government departments in Australia and worldwide.

Although reports vary greatly, computer experts estimate that about 80 per cent of businesses received the virus, however, many had received virus alerts in time to prevent the full effects of the virus.

A computing student was arrested in the Philippines and charged with breaching the *Access Device Regulations Act* for 'unauthorised access' and 'destructive activities' to computer systems. Although laws have now been enacted, at the time the virus wreaked havoc across the world, computer hacking and uploading computer viruses were not outlawed under Philippines law.

3.4 Australia

There have been few prosecutions for spreading a computer virus in Australia. One case of interest is *Lynn v Barylak*. The defendant was a post-graduate student at the Swinbourne Institute of Technology. Following problems with the computer network, a virus was found to have infected the computers in the laboratory. A policy was put into place in order to contain the possible spreading of the virus.

The defendant was observed to breach the policy after using a non-standard boot disk at four terminals in rapid succession. A virus was found on one of the terminals which the defendant had accessed and he was arrested by the police.

Barylak was charged with two offences under Victorian legislation. Computer trespass under the *Summary Offences Act* states 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'. Malicious damage under the *Crimes Act* occurs when a person 'intentionally and without lawful excuse destroys or damages any property belonging to another'. The property must be of a tangible nature.

The charge of computer trespass failed on the basis that the necessary intention had not been met and the charge of malicious damage also failed since there were other innocent explanations for the defendant's behaviour.

3.5 New viruses

Although the Melissa virus and Love bug caused major damage to computer systems worldwide, experts warn that some new viruses have the potential to cause even greater damage.

The explore.zip worm hit computer networks in June 2000, deliberately seeking and destroying Microsoft files and software development files. A major contributing factor to the rapid spread of both the Melissa virus and the Love bug was that the email containing the virus appeared to arrive from an acquaintance.

The explore.zip worm and its variants have the potential to cause even greater damage. Not only does the virus arrive from what appears to be a known sender but the virus is hidden in '.zip' files rather than '.exe' files which generally alerts the recipient to the risks involved in opening the attachment. Fortunately the rate at which the explore.zip worm spread was comparatively slow.

In addition, viruses are now capable of infecting mobile phones and with approximately 8.5 million users in Australia, the threat which viruses pose is of even greater concern.

4 CURRENT LEGAL REGIME

Although jurisdictions such as the United States and the United Kingdom have had comprehensive computer crime legislation for at least a decade, Australia has been slow to realise the dangers which computer crime poses.

Although most jurisdictions have some legislation dealing with 'hacking' in the form of offences relating to unauthorised access, there are few criminal offences which are directly applicable to the circulation of a computer virus.

4.1 Criminal or malicious damage to property

Reliance on criminal or malicious damage to property may be the only possible avenue where specific computer related offences are not available. Generally, the offence involves the intentional destruction or damage to property belonging to another without lawful excuse.

Computer viruses may not cause damage to property in the traditional way since altered data is arguably not property under criminal law. However, English cases have held that only tangible property need be damaged, not that the damage had to be tangible.

4.2 Specific computer related offences

Although Australia does not have uniform computer related offences, the creation and distribution of a virus could fall under several provisions of both Commonwealth and State legislation.

Commonwealth

Part VIA 'Offences Relating to Computers' was inserted into the *Crimes Act 1914* in 1989. The offences under Part VIA are limited to areas over which the Commonwealth has constitutional powers.

Sections 76D and 76E creates certain offences where facilities operated or provided by the Commonwealth or a carrier are used to commit certain offences. These relate to unauthorised access and damaging data in a Commonwealth or other computer. The latter offence includes interference, preventing access to and impairing the lawful use of data. Although untested in relation to computer viruses, these provisions are potentially applicable to the

deliberate spread of a computer virus via email or over the internet.

New South Wales

Section 310 of the *Crimes Act* 1900 states that:

A person who intentionally and without authority or lawful excuse:

(a) destroys, erases or alters data stored in or inserts data into a computer; or

(b) interferes with, or interrupts or obstructs the lawful use of a computer,

is liable to imprisonment for 10 years, or to a fine of 1,000 penalty units, or both.

This provision is one of the only provisions in Australian law which is directly applicable to a situation where someone deliberately introduces a virus into circulation. However, it has been criticised on the basis that it is too broad in that locking a door to a computer room may fall within the scope of the offence.

Other

The Victorian Parliament did not believe it was necessary to create a specific offence to deal with computer viruses in the belief that criminal damage was sufficient to deal with the situation. Queensland also decided that existing provisions of 'misappropriation of property' and 'unlawful destruction of property' were adequate to deal with computer related crimes.

Tasmania and the ACT has provisions similar to NSW, with Tasmania also having an additional offence of 'insertion of false information of data'.

South Australia and Western Australia both have offences of unlawful operation of a computer system whereas the Northern Territory does not have either unauthorised access or alteration of computer data offences but does have computer related fraud offences.

4.3 Inadequacies of current legislation

As can be seen from the above, each state and territory has a rather inconsistent treatment of computer related crimes. Although most jurisdictions now have offences relating to 'unauthorised access', the creation and spreading of a computer virus would only fall under a very limited number of specific provisions.

One of the difficulties in successfully prosecuting a virus creator is the requirement to prove an intent to cause damage. This may be problematic especially where the damage caused results from a programming error as opposed to the malicious intentions of the virus writer. The Model Criminal Code attempts to address the difficulties in prosecuting under the existing regime.

5 MODEL CRIMINAL CODE

As early as 1987, the Standing Committee of Attorneys General realised the need for uniform legislation between the states on computer crime, however disagreement as to its form has until now precluded reform of the area.

A committee containing representatives from each Australian jurisdiction has proposed new offences directed at dealing with computer crime as part of the model criminal code aimed at eventually standardising criminal legislation in all the states and territories. Although the Code is only at a discussion stage, the new offences provide some insight into the future direction of computer crime offences in Australia.

The committee worked on the notion that general offences should be applied where possible (such as in relation to computer fraud and forgery offences), however they concluded that the less tangible consequences of computer offences required specific treatment.

The proposed offences are predominantly based on the *Computer Misuse Act* 1990 (UK) (the UK Act). The Code proposes the following offences in relation to computers:

(a) unauthorised access, modification or impairment to commit a serious offence;

(b) unauthorised modification of data to cause impairment;

(c) unauthorised impairment of electronic communications; and

(d) a summary offence of unauthorised access to restricted data.

The second offence of 'unauthorised modification of data to cause impairment' will be the most appropriate for the prosecution of a computer viruses creator and distributor but the other offences may also apply in certain circumstances.

5.2 Definitions

The Committee decided against defining 'computer' on the basis that any definition would prove to be both under and over inclusive. Under inclusive in the sense that new devices are continually being developed and over inclusive in that computerised components are now contained in many appliances, vehicles and even toys.

The concept of data has also been defined broadly to include information in any form or any program (or part of a program). As such, the scope of the provisions will depend on what the courts determine to be data, programs and computers based on their ordinary meanings.

5.3 Unauthorised modification of data to cause impairment

The offence occurs where a person:

(a) causes any unauthorised modification of data held in a computer, and

(b) knows that the modification is unauthorised, and

(c) intends by the modification to impair access to, or to impair the reliability, security or operation of, any data held in a computer, or who is reckless as to any such impairment.

The maximum penalty which can be imposed is 10 years imprisonment (similar to criminal damage) and as such acknowledges that damage

whether tangible or intangible should be treated in a similar manner.

The proposed offence is significantly more comprehensive than existing offences when applied to computer viruses. Not only is recklessness sufficient for the offence, there is no need to show that actual impairment occurred.

The offence will also apply in situations where a person with limited authorisation impairs data or programs whilst conducting an unauthorised operation or where a hacker obtains unauthorised access to data or a program and causes a modification of the data or program.

5.4 Unauthorised impairment of electronic communication

A person who causes an unauthorised impairment of electronic communications to or from a computer with the intention to impair or who is reckless to such impairment is guilty of the offence. Although impairment is not defined, it is intended to include intangible as well as tangible harm.

This provision has been proposed to deal with 'denial of service attacks' which have recently become more prevalent. Computers are programmed to simultaneously lodge requests for information at a selected website causing it to jam for hours.

Despite the specific nature of the offence, it may also be applicable to the circulation of a virus. Fast spreading viruses such as Melissa and the Love bug, have caused the servers of Internet Service Providers to stall as a result of the excessive volume of email being generated.

A conviction under this section would be an alternative to the offence of 'unauthorised modification of data to cause impairment'.

5.5 Unauthorised access, modification or impairment with intention to commit a serious offence

This section makes it an offence to cause an unauthorised computer function with the knowledge that it is unauthorised and the intention of committing a serious offence.

An unauthorised computer function is any unauthorised access to data in a computer, any unauthorised modification of data held in any computer or any unauthorised impairment of electronic communications to or from any computer.

This is a preparatory offence aimed at catching those who have yet to carry out the offence but have the appropriate intention to commit the offence.

The offence may also apply to the deliberate circulation of trojan horses. Where the trojan horse has infected a computer, the remote operator may be able to obtain passwords stored on the computer to commit other offences. Although the virus may not in itself cause any impairment or modification of data, the section will be triggered by the resultant unauthorised access.

Unlike the offences discussed above, this offence does not require the proof of impairment of data or of electronic communications. All that is needed is unauthorised access in conjunction with an intent to commit an offence punishable by at least five years imprisonment. The maximum penalty for this offence is the same as the penalty for the offence which the offender intended to commit.

5.6 Comparison with the UK Computer Misuse Act

The most significant difference between the proposed Code and the UK Act is in relation to intention. The UK Act requires the proof of intention to cause damage whereas liability under its Australian counterpart will attach where it can be shown that the accused acted recklessly.

Many viruses are not created with the intention to cause damage but do so as a result of programming faults. Smith, the creator of the Melissa virus claims that he deliberately programmed the virus in a way so that damage was not caused. However, the rate at which the virus multiplied was not anticipated by Smith. On that basis, Smith could argue that he lacked the necessary intention to cause the damage which eventuated.

As such, the lower threshold of recklessness in circumstances similar to this appears to be necessary in order for the legislation to be effective.

6 CONCLUSION

The proposed offences directed at the creation and dissemination of computer viruses can hardly be seen as necessary to prevent imminent danger to our computer systems. However, the adoption of the criminal code will undoubtedly place Australia in a better position to deal with computers viruses and other computer related crime generally.

If the criminal code is implemented in Australia, it is not expected to result in a rapid increase in the number of prosecutions but act more as a deterrent to would be cyber criminals. The penalties for damage caused to computer data or programs are not minor and mirror offences which involve damage to physical property.

The very nature of cyber crime presents jurisdictional issues. Where a computer virus is created and distributed from outside Australian borders, our laws will have little if any impact on the perpetrator. As such, international cooperation is essential in order to adequately deal with computer crime.

Regardless of whether the proposed Code acts as a deterrent to virus creators, avoiding the costs associated with a virus infection will ultimately remain the responsibility of computer users. Vigilance and common sense has and will always remain the most effective protection against computer viruses.