Combating Cybercrime

The Federal Government has introduced new legislation to combat the problems of cybercrime, Niranjan Arasaratnam and Maree Flynn explain.

On 27 June, the Government took aim at hackers and website vandals with the introduction of the *Cybercrime Bill 2001* (**Bill**). The Bill significantly bolsters the range of computer offences by adding a new Part 10.7 to the *Criminal Code Act 1995* (**Criminal Code**). The computer offences are modelled on the *January 2001 Model Criminal Code Damage and Computer Report* developed through Commonwealth, State and Territory cooperation. The Bill repeals the existing offences in Part VIA of the *Crimes Act 1914* (**Crimes Act**) which were enacted in 1989 and are considered irrelevant to today's technology.

The Bill also significantly enhances the investigation powers of law enforcement authorities for searching and seizing electronically stored data by amending the Crimes Act and *Customs Act 1901* (**Customs Act**). These amendments build upon the existing provisions which were enacted in 1994 and take into account the draft Council of Europe Convention on Cybercrime. There are also consequential changes to the *Australian Security Intelligence Organisation Act 1979* (**ASIO Act**), *Education Services for Overseas Students Act 2000* (**ESOS Act**) and the *Telecommunications (Interception) Act 1997* (**TI Act**).

There are estimates that cybercrime is costing companies worldwide approximately $3 trillion a year. The growth in the Internet population and electronic commerce over the last decade means cybercrime is a realistic and substantial threat to the security and reliability of computer data. The Federal Minister for Justice and Customs, Senator Christopher Ellison, has stated that the Bill aims to strengthen business, government and community confidence in using new technologies:

> *The large amount of data that can be stored on computer drives and disks and the complex security measures, such as encryption and passwords, which can be used to protect that information present particular problems for investigators. The legislation will enable police powers to copy computer data and examine computer equipment and disks off-site, enabling them to obtain assistance from computer owners.*

The new offences contained in the Bill also cover using a computer to commit serious offences such as stalking, fraud or sabotage. The maximum penalty contained in the Bill is up to 10 years imprisonment.

COMPUTER OFFENCES

There are 7 new computer offences. These offences have extraterritorial jurisdiction recognising that computer crime often occurs outside the country. It will not matter where the conduct constituting an offence takes place, because if Australia is affected then prosecution can take place here. This means that an Australian citizen travelling to a country where hacking is not an offence, who then uses a laptop computer to hack into a computer in a third country, will be liable.

The Bill provides for concurrent operation of Commonwealth, State and Territory laws to avoid any gaps in jurisdiction and allow computer crimes to be prosecuted where it is most convenient. For example, the State and Territory computer offences would cover computer crime activities by employees using an internal computer network. The Commonwealth cannot regulate this conduct because computer crime on such networks does not use the telecommunications system.

The new offences apply to computers, computer data, or communications to or from a computer. The Government has left the term "computer" undefined so that the proposed computer offences embrace technological change. This complies with the discussions raised in the *Model Criminal Code Report* on computer offences that a restrictive definition may unduly limit the application of the proposed offences.

Summary of 7 new offences

The following is prohibited:

- Unauthorised access or modification of computer data or impairment of electronic communications to, or from, a computer. There must be an intention to commit a serious offence which is punishable by 5 or more years imprisonment. The penalty applying is the equivalent for the serious offence. So a hacker accessing credit details in a bank computer and intending to use them to steal money, would face the same 10-year-penalty imposed for a fraud offence.

- Unauthorised modification of data in a computer by a person who is reckless about whether data will be impaired. A maximum penalty of 10 years imprisonment applies. This offence is wideranging and can cover unauthorised access to a computer system and impairing data, or using a disk containing a computer virus to sabotage a computer.

- Unauthorised impairment of electronic communications to, or from, a computer. A maximum penalty of 10 years imprisonment applies. This offence aims to prevent "denial of service attacks" caused when a computer server crashes after a website is swamped with excessive amounts of unwanted messages. The high penalty recognises that such damage can be comprehensive and expensive.

- Unauthorised access to, or modification of, restricted data held in a computer. This only applies to accessing or modifying data protected by a password or other

security feature. A maximum penalty of 2 years imprisonment applies. People illegally entering protected computer systems to access or alter personal or commercial information are targeted.

- Unauthorised impairment of the reliability, security or operation of any data held on a Commonwealth computer disk, credit card, or other device. A maximum penalty of 2 years imprisonment applies. Examples of impairing data are destroying computer disks or using magnets to affect credit cards.

- Possession and supply of data or programs intended to be used to commit a computer offence are covered by two new offences. A maximum penalty of 3 years imprisonment applies. Traders of programs for hacking and inserting computer viruses would be caught by this provision.

Consequential Changes

The repeal of the existing computer offences would also mean that:

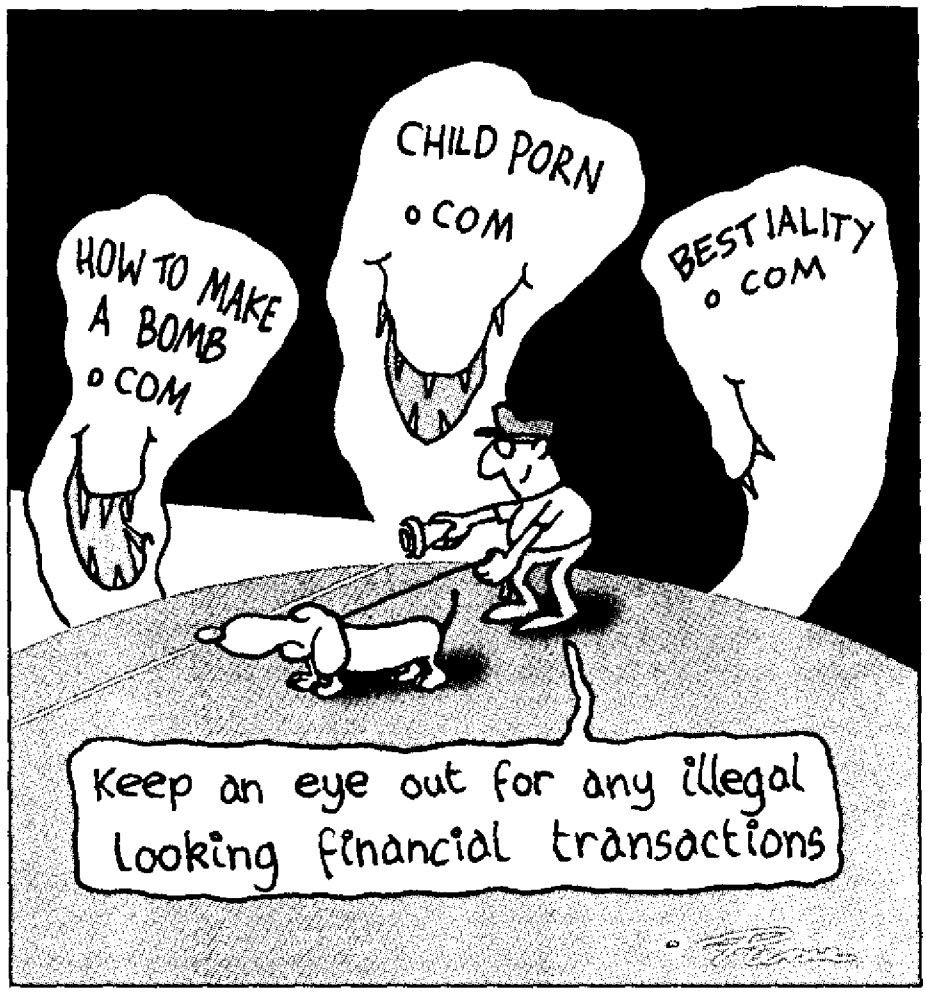
- Under the ASIO Act an ASIO officer accessing data stored in a computer under a computer access warrant will not commit an offence.

- Under the ESOS Act a person obtaining unauthorised access to information on a protected computer system receiving and storing information about students could be guilty of an offence.

- Under the TI Act a warrant can be obtained for the investigation of the proposed computer offences.

INVESTIGATION POWERS

The Bill also extends the criminal investigation powers in the Crimes Act and Customs Act for searching, seizing and copying electronically stored data. Law enforcement agencies are given further powers to detect and investigate crime involving computers. Under the existing law, investigators cannot receive assistance when accessing encrypted information from someone with knowledge of a relevant computer system.



This has left law enforcement agencies at a major disadvantage because large amounts of data are commonly stored on computer drives and disks which are protected.

Under the proposed amendments, a search warrant will allow law enforcement officers to search beyond computers located on search premises, to include material accessible from those computers but located elsewhere. This is particularly relevant because most businesses have networks to other computers and central storage computers.

Computer equipment and disks can also be examined offsite when this is significantly more practicable. This change acknowledges that large amounts of time are often required to circumvent today's complex security measures.

Officers will also be able to copy all data held on a computer hard drive or data storage device where some of the data is evidential material or if there are reasonable grounds to suspect this.

Finally, a magistrate may order a person with knowledge of a computer system to provide information or assistance so that an officer can access, copy or print data. Only necessary and reasonable assistance is required. Using such "insider knowledge" could be a major breakthrough in attempts to access encrypted information. This power is also contained in the draft Council of Europe Convention of Cybercrime.

Niranjan Arasaratnam is a Partner and Maree Flynn is a Research Assistant at the Sydney Office of Allens Arthur Robinson.