yahoo-2000-11-20-lapres.html>

30 Australian Broadcasting Authority, *Investigation Into the Content of On-line Services, Report to the Minister for Communications & the Arts*, (Sydney: ABA, 30 June 1996) p158.

31 A number of such labelling schemes are in development. For a critique of such systems see <http://www.efa.org.au/Issues/Censor/cens2.html#filter> accessed 26/6/2001.

32 Australian Broadcasting Authority, *Investigation Into the Content of On-line Services, Report to the Minister for Communications & the Arts*, (Sydney: ABA, 30 June 1996) pp156-158.

33 Karen Koomen "Freedom of Speech and the Internet in Australia" Speech delivered at the Communications Law Centre Conference on 'Free Speech in Australia' Sydney, 10/9/96 p16.

34 Senator Alston, speech entitled 'Regulatory Challenges in Cyberspace' delivered at *Interactive Kids '98*. Sydney May 18th 1998.

35 David Kerr, *Action Plan on Promoting Safer Use of the Internet, Preparatory Actions – Self Labelling and Filtering*, Internet Watch Foundation, April 2000.

36 Australian Broadcasting Authority, *Six Month Report on Co-Regulatory Scheme for Internet Content Regulation*, July to Dec 2000. April 2001

37 Ibid

38 Irene Graham "The Net Labelling Delusion: Saviour or Devil?" <http://rene.efa.org.au/liberty/label.html> accessed 21/6/2000; Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books 1999) esp pp177-182.

39 Irene Graham, "The Net Labelling Delusion - Saviour or Devil?" http://libertus.net/liberty/label.html

40 Jennifer Lee, "Punching Holes in Internet Walls" New York Times, 26/4/2001.

41 Singapore Broadcasting Association, SBA's Approach to the Internet, http://www.sba.gov.sg/work/sba/internet.nsf/ourapproach/1

42 The OSA itself states that it is intended

(k) to provide a means for addressing complaints about certain Internet content; and

(l) to restrict access to certain Internet content that is likely to cause offence to a reasonable adult; and

(m) to protect children from exposure to Internet content that is unsuitable for children. *Broadcasting Services Act* (1992) (Cth). s3(1)(k),(l), & (m).

43 Senator Alston, speech entitled 'Regulatory Challenges in Cyberspace' delivered at *Interactive Kids '98*. Sydney May 18th 1998.

Cybercrime: Proposed legislation clamps down on use of technology to commit serious offences

Irene Zeitler, Partner, Freehills

Irene Zeitler is a partner in the Intellectual Property Group at the Freeehills Melbourne office and a consultant to the associated patent attorney firm, Freehills Carter Smith Beadle. Irene has substantial expertise in the field of information technology, intellectual property and trade practices.

A Bill recently introduced by the Federal Government contains new updated computer offences.[1] These offences are based on the offences recommended in the January 2001 Model Criminal Code Damage and Computer Offences Report.[2] The Bill is also consistent with the terms of the draft Council of Europe Convention on Cybercrime.

The purpose of the new offences is to overcome perceived deficiencies in existing computer offences inserted into the *Crimes Act* in 1989. These deficiencies arise from advances in computer technology and electronic communications which have given rise to new means for committing Cybercrimes, such as hacking, denial of service attacks and virus propagation. The Bill repeals existing offences.

The Bill has been referred to the Senate Legal and Constitutional Legislation Committee which is due to report on the Bill on 28 August 2001.

In summary, the new offences include the following:

Offence of causing unauthorised access to data held in a computer or any unauthorised modification of data held in a computer or any unauthorised impairment of electronic communications to or from a computer

To commit this offence, a person must know that the access, modification or impairment is unauthorised. The person must furthermore intend to commit, or facilitate the commission of, a serious offence against a law of the Commonwealth by the access, modification or impairment.

A serious offence is an offence punishable by life imprisonment or a term of five years or more. The new offence carries a maximum penalty equal to the maximum penalty for the serious offence the person is intending to commit.

This covers offences against State and Territory laws where the unauthorised access, modification or impairment is caused by means of a telecommunications service.

The proposed offence is intended to cover the unauthorised use of computers to commit serious offences such as a fraud or stalking. An example of this is where a person uses the internet to hack into the computer system of a bank in order to access credit card details for the purpose of obtaining money.

Offence of causing any unauthorised modification of data held in a computer

This proposed offence is established where the person knows that the modification is unauthorised and is reckless as to whether the modification impairs or will impair access to that or any data held in any other computer or the reliability, security or operation, of any such data. The maximum penalty for this proposed offence is a 10 year prison term.

For the offence to apply, the data must be held on a Commonwealth computer or the modification must be caused by means of a telecommunications service.

This proposed offence is intended to catch hackers and persons who circulate disks containing computer viruses.

Offence of causing any unauthorised impairment of electronic communications to or from a computer

This proposed offence applies where the person knows that the impairment is unauthorised. The electronic communication must be via a telecommunications service or involve a Commonwealth computer. The maximum penalty for the proposed offence is 10 years.

The purpose of the proposed offence is to target "denial of service attacks". This occurs where, for example, a website is swamped with a large volume of unwanted messages which overload and impair the functioning of the computer system.

The proposed offence applies only to acts and not omissions. Accordingly, a strike by telecommunications maintenance workers, which causes impairment of electronic communications, will not result in the striking workers committing an offence. Nor will this provision apply to a refusal by an internet service provider to carry certain types of electronic communication traffic on its network provided the refusal is dealt with in the contractual terms between the internet service provider and the user.

Offence of intentionally causing unauthorised access to, or modification of, restricted data

This proposed offence applies where the person knows that the access or restriction is unauthorised. The restricted data must be held in a Commonwealth computer or access to the restricted data must be caused by a telecommunications process.

Restricted data is defined as any data in a computer to which access is restricted by an access control system.

The penalty for this proposed offence is a maximum prison term of two years. The provision is intended to cover situations where, for example, an employee breaks a password on his or her employer's computer system to access the internet or access protected information.

Offence of intentionally causing any unauthorised impairment of the reliability, security or operation of data held on a computer disk, credit card or other device used to store data by electronic means

Under this proposed offence, the disk, credit card or other device must be owned or leased by a Commonwealth entity. The proposed offence attracts a penalty of up to two years.

Offence of possessing or controlling data with the intention that the data be used to commit or facilitate the commission of any of the foregoing offences

The maximum penalty for this offence is a three year prison term.

Offence of producing, supplying or obtaining data with the intention of committing or facilitating the commission of any of the foregoing offences

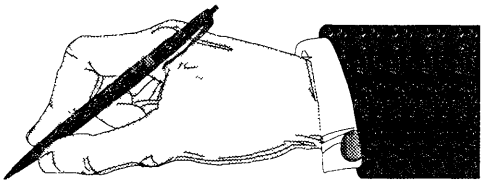
The maximum penalty for this proposed offence is also three years.

---

1 Cybercrime Bill 2001 (Cth), introduced and read a first time on 27/6/2001

2 *"Report - Model Criminal Code, Chapter 4 – Damage and Computer Offences"*, Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General, January 2001: http://www.cdpp.gov.au/publications/Model_Criminal_Code/index.htm (as accessed at August 2001)

Contribute to the Journal!



The Editors encourage submission of articles, casenotes, reviews and comments on topics relating to computers and law.

The following are some topics you may be interested in submitting a piece on: important IT cases, Internet, content regulation, jurisdictional issues, IT contracting issues, e-commerce, privacy and security issues, or feel free to write on your own topic of choice that is of current interest. (See page 51 for more details.)