Australian Government
Australian Institute of Criminology

AUSTRALIAN HIGH TECH CRIME CENTRE

HIGH TECH CRIME BRIEF

Hacking offences

2005

05

The nature of hacking

This paper describes how computer hacking crimes are defined in Australia. The term 'hacker' has multiple meanings and variously describes a person who explores programmable systems, who is obsessive about programming, who is able to program quickly, or is an expert in a particular program. More generally, it refers to an expert enthusiast, one who enjoys creatively overcoming limitations, or a malicious meddler seeking confidential information (Reymond 1996). Levy (1984) described three generations of hackers, beginning with the programming pioneers of the 1950s and 1960s, followed by those who developed the earliest PCs and then those programmers who developed computer games. Taylor (2000) added a fourth generation – those who illicitly access other people's computers. This is now the common meaning given to computer hacking (PJC 2004). However, because of these overlays of meaning, it is difficult to match the common understanding of what constitutes computer hacking with anti-hacking laws.

Perhaps in view of the ambiguity attached to the term hacking, it is not used in the substantive offence provisions (however, the heading of the Queensland provision does refer to computer hacking and misuse). Relevant offences do not rely on or define the term hacking. In each jurisdiction except Tasmania anti-hacking laws criminalise hacker behaviour by reference to the intention (or recklessness) of the hacker, or instances where restrictions on data access are breached by a hacker.

The Cybercrime Act model

In 2001, state and Commonwealth laws dealing with computer crime were described as diverse in policy and partial in their application (MCCOC 2001). Since then, greater uniformity has been achieved as New South Wales, Victoria, the Australian Capital Territory and South Australia have implemented laws in terms similar to the Commonwealth Criminal Code provisions inserted by the *Cybercrime Act 2001* (Cwlth). The Northern Territory law is also loosely based on this model.

Importantly, access in itself is not prohibited. and an intention to obtain a benefit or advantage is not sufficient to constitute an offence, except for section 276B in the Northern Territory. In this scheme there has been a deliberate choice to peg criminal liability at four levels based on the defendant's intent or the way access to data is secured on a computer. It should be noted that the standard of criminal responsibility for the creators of viruses and worms under the *Cybercrime Act* model is set quite high and that this in itself reflects the tension inherent in seeking to adequately deal with malicious applications while allowing for the lawful use of the internet. The four levels are:

Level 1

Accessing data or impairing an electronic communication if this is done with the intention to commit a serious offence (defined as an offence with a maximum penalty of at least five years). In the Northern Territory the intention required is to cause loss or damage or to gain a benefit or advantage.

Level 2

Impairing or modifying data, or impairing electronic communications, if done with the intent to cause (or with recklessness to) harm or inconvenience.

Level 3

Possession, control, production or supply of data with the intent to commit any of the above computer offences. Recklessness is not sufficient. This type of offence may be very difficult to prove in relation to the unexpected consequences of the release of a virus, such as occurred with the Melissa virus (Ling 2000).

Level 4

Accessing data that is subject to an access control restriction (Commonwealth, ACT, NSW, Victoria).

Other laws

The remaining three jurisdictions of Western Australia, Queensland and Tasmania have quite different laws to regulate hacking offences.

Western Australia

In Western Australia, section 440A of the *Criminal Code* was introduced in 1990 under the heading 'unlawful operation of a computer system'. The section refers to a person who 'without authorisation' accesses 'information stored in a restricted access system' or who 'operates' such a system 'in some other way'. A restricted access system is defined as a computer system or a part or application of a computer system that is accessible only through the use of a code that is withheld by the person in control of the computer system or made available on a restricted basis. This provision is particularly suited to the situation of someone hacking a computer from outside but leaves considerable difficulty in determining when initially authorised access becomes unauthorised either by exceeding initial permissions or by the subsequent use of data or information accessed.

Queensland

The Queensland law introduced in 1997 uses the heading 'computer hacking and misuse' but the offence is defined as the

use of a restricted computer without the consent of the computer's controller. A restricted computer is defined as one that requires a 'device, code or sequence of electronic impulses' to gain access. There is a penalty scale of two, five or 10 years maximum term of imprisonment depending on whether (1) an offender simply uses a computer, (2) causes detriment or damage, or gains or intends to gain a benefit, or (3) the detriment, damage or gain is valued at more than $5,000.

Tasmania

The Tasmanian law follows the recommendations of Gibbs (1988). MCCOC (2001) noted that Gibbs addressed the protection of data stored on Commonwealth computers. The Tasmanian law requires intention and a lack of 'lawful excuse', in relation to damaging (or destroying, erasing or altering) computer data or simply accessing a computer or system of computers without authority. This formulation gives rise to uncertainty whether a person has a 'lawful excuse', which is not further defined. MCCOC (2001) argued that this formulation over-criminalises behaviour because of the breadth of the concepts of 'lawful use', 'access' and what constitutes a 'computer'. It is suggested, for example, that for one student to borrow the calculator of another student without permission would constitute unlawful use.

General issues

Hacking incorporates two quite distinct concepts of acting 'without authorisation' and of acting 'illegally'.

'Access'

An initial problem is that of defining 'access'. As Kerr (2003) puts it, no one knows what it means to 'access' a computer.

'Unauthorised'

Determining whether a hack is authorised or not is not straightforward and may involve detailed consideration of whether a computer owner has any data access policy, whether and how that policy is communicated to others, how accessible a computer is, and how accessible are the files, directories and other information on that computer. There may be questions of contractual or moral rights, or of implied consent, or the limits of a consent once given. A dominant characteristic of modern computing is the interconnection of devices via local area networks (LANs) and global connectivity via the world wide web. Sorting out legitimate from illegitimate use of encryption, trademarks in metatags, bulk spam, anonymity and disguised identity has been seen as particularly problematic (MCCOC 2001). The use of 'cookies' is an example of how the internet is itself based on the free exchange of data between computers and where the vagueness of standards for internet behaviour can be exploited. A cookie is a piece of data inserted by one computer on another so that the first computer can 'recognise' that other computer on a subsequent occasion. However, cookies can also be used to track, monitor and report on other internet activity conducted on the second computer. A cookie with this capacity is sometimes referred to as spyware. Spyware is relatively common and someone surfing the net may not realise, in agreeing to the terms of a download, that they are agreeing to such a cookie being placed on their computer (Barrett 2002). In the US and Australia it has been proposed to require consent for the insertion of such software (BBC 2004).

Privacy

In the Northern Territory there is an offence of unlawfully obtaining confidential information. Otherwise, Australian anti-computer hacking laws are concerned with computer security rather than issues of privacy. Where unauthorised access to data that are subject to access control is prohibited, but the relaying of confidential information gained through authorised access is not.

'Computer'

The laws in Queensland, Tasmania and Western Australia specifically refer to systems or networks of computers within the definition of computer. While the other jurisdictions refer to a computer, under the *Cybercrime Act* model, 'computer' is not defined. The use of digital technology in everyday machines and appliances is ubiquitous and the ordinary meaning of computer must be applied. An individual computer may or may not be connected to other computers and an increasing array of devices are capable of being connected either physically or using wireless technology. Interconnected computers can be hacked internally or externally and the world wide web itself might be considered to be a single computer (MCCOC 2001). Computers that are not connected to other computers nevertheless can be 'hacked' by someone directly accessing that computer.

Conclusion

Given the interconnectivity of the internet and the jurisdictional complications that flow from different laws in relation to this type of offending, there is a clear need to continue the process of harmonising anti-hacking laws in Australia. The *Cybercrime Act* model has now been adopted in the majority of states and territories and should be considered for adoption in the remaining three states.

Contact
Australian Institute of Criminology
GPO Box 2944 Canberra ACT 2601
Phone: 02 6260 9200 Fax: 02 6260 9201
Web: www.aic.gov.au

Project no. 0074 ISSN 1832-3413

The Australian High Tech Crime Centre funded this research.

Further reading

Barrett R 2002. Free software is the lure, online surveillance is the reality. *Consumer web watch news.* http://www.consumerwebwatch.org/news/articles/spyware.htm

BBC 2004. US moves to rein in spyware. *BBC news* 18 June. http://news.bbc.co.uk/1/hi/technology/3818057.stm

Gibbs H 1988. *The review of Commonwealth criminal law: interim report on computer crime.* Canberra: Attorney-General's Department

Kerr O 2003. Cybercrime's scope: interpreting 'access' and 'authorisation' in computer misuse statutes. *New York University law review* 78(5): 1596

Levy S 1984. *Hackers: heroes of the computer revolution.* New York: Bantam Doubleday Bell

Ling P 2000. Is Australian criminal law up to the threat of computer viruses? *Journal of the society for computers and the law* 41. http://www.nswscl.org.au/journal/41/Crime.html

Model Criminal Code Officers Committee (MCCOC) 2001. Damage and computer offences. *MCCOC report*. Canberra: Attorney-General's Department

Parliamentary Joint Committee on the Australian Crime Commission (PJC) 2004. *Cybercrime.* Canberra: Parliament of the Commonwealth of Australia

Reymond E 1996. *The new hacker's dictionary* (third edition). Cambridge MA: MIT Press

Taylor P 2000. Hackers – cyberpunks or microserfs? In D Thomas & B Loader. *Cybercrime*: 36–55. London: Routledge