Computer Crime
&
Information Technology

HACKING

Lucas Wyte

11 IPT

November, 1995.

Information Processing and Technology - Social and Ethical Implications

Computer Crime and Information Technology
HACKING

The impact of the techno-revolution on society has been overwhelming. Considering that the first microprocessor was introduced to the world just over twenty years ago, we have witnessed a technological growth that has transformed the way we work, the way we act and the way we communicate. Yet despite these enormous changes in how we live each day, the legal system has been struggling to keep up. Laws that were developed in the Constitution of 1901 to accommodate last century's problems have been slow to be translated to the technological crimes of today and the rapidly approaching twenty-first century.

Crime is a term that refers to many types of misconduct forbidden by law. Computer crime involves the unauthorised and unlawful use of a computer. It has been found (Cudmore, 1994, p.8) that at present "the cost of computer crime in the United States [is] estimated to be at least $5000 million a year". Closer to home,

> "In 1980, the Caulfield Institute of Technology Computer Research Bureau (ACARB) surveyed 2000 Australian computer users and discovered 123 cases of computer abuse costing a total of $5.6 million." (Cudmore, 1994, p.8).

Between 1980 and 1991, 497 further incidents of computer crime were reported to ACARB, resulting in an estimated loss of $17 million. However, ACARB still believes that up to ninety percent of computer crime remains unreported - their cost unknown.

Computer crime tends not to be violent or public and therefore ~~has~~ been regarded by society as less serious than other crimes such as armed robbery or fraud. ✓ The act of hacking, a form of electronic break-and-enter, has even been glamorised by the media, to the extent that hackers aren't seen as criminals, rather as experts beating the system, eg. *Sneakers*, *War Games* and most recently *The Net*.

cite ref

The hacker most often comes from one of two extremes of the computer crime environment. According to Bloombecker (1990), the hacker may be simply addicted to the computer as a toy, joyriding through communications and computer systems, oblivious to the damage they may be causing. For example, Kevin Mitnick, a convicted hacker known to the authorities as the Condor, stated in a 1992 computer-security conference that "I never wanted to use technology as a tool for crime ... I was just an electronic joy rider having fun in cyberspace." (Goodell, 1995, p. 55). ✓

On the other hand, the hacker may take on the role of the 'cyberpunk', stalking 'cyberspace' with criminal intent and usually leaving the biggest tail of destruction. However, these hackers believe that their behaviour is not unlawful and that they are simply prompting organisations to improve their security systems. Zodiac, a hacker and virus writer for a notorious cyberpunk group named Rabid, explains that "I'm not a particularly malicious person, and I do not have a 'vendetta' towards the computer community ... I just enjoy programming viruses". To the developers of anti-virus software he feels that,

> "You should be paying us money and not trying to 'bust' us. We're keeping you in your dirty business ... because you, like the pigs, are too stupid to realise our higher intelligence/motives." (Clough, B. et. al., 1992, p.219-220).

Shit Kicker Jim is another cyberpunk, who broke in and destroyed essential files of the distribution company DHL. He believes that

> "I'm not normally as malicious as this but had to prove to DHL and everyone else in the Hong Kong business community that things like this can happen." (Plunkett, 1994, p.28).

Reported cases of hacking offences suggest that breaking into computer systems is not very difficult for the average hacker. Secret passwords that control the entry of users to large computer networks are either discovered by the hacker by trial and error, or more commonly disclosed by employees. Shit Kicker Jim berated DHL for having what he called "ridiculously obvious" passwords on their system (Plunkett, 1994, p.28) and another hacker, known as Triludan the Warrior, broke into a Prestel public-access computer system that was 'secure' - the ID code being a ten character string of letters and numbers, the password a four character string. For no obvious reason, Triludan entered '2222222222', and a message came back saying 'correct'. "He assumed that if the ID code was that simple, then the four character password must be equally obvious." (Clough, 1992, p.38). He tried '1234' and - 'Welcome to Prestel system management'! ""So this is hacking," he thought to himself'. (Clough, 1992, p.38). Is it really that easy? Plunkett (1994, p.28) has found that,

> "According to many authorities and computer security specialists, business and industry in Australia are not taking computer crime seriously enough, and accordingly, are doing far too little to prevent it".

The techno-revolution has obviously had a tremendous effect on society and its institutions. But how well equipped is our legal system to handle the new technology? Can the law cope with computer crime?

When we look at computer crime in today's world, it is important to distinguish between moral and legal issues, as an act that is considered morally wrong may not necessarily be illegal. Still, the catechism of the Catholic church has recently been rewritten to include many modern sins, such as computer hacking. Bishop David Konstant believes (Cudmore, 1994, p.25) that "this crime may seem new but it's just an old sin in new circumstances".

Is computer crime simply a more sophisticated way of committing traditional crimes? If it is, then the present criminal law will be adequate. However, if there are elements of computer crime that elude traditional law, then law makers and parliamentarians are faced with the challenge of creating new legislation to cover this abuse.

The problem for our law-makers, in regards to hackers and creating a new legislation to cover computer trespasses, is that it is essential to differentiate between the hacker who acts with malicious intent and the hacker who is prompted by simple curiosity. Failure to distinguish between both activities risks contradicting the fundamental principle on which our criminal

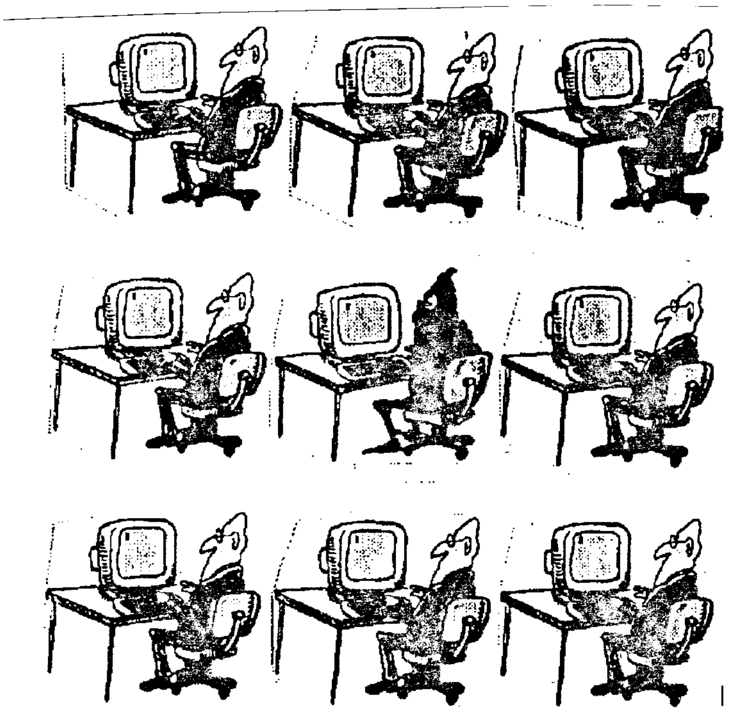
very important [illegible] to be highlighted.

law is based - that the defendant must not only commit an unlawful act (*actus reus*) but must also have a criminal intention (*mens rea*) (Cudmore, 1994, p.43).

Undoubtedly, computer technology will continue to challenge our legal system in the future. With so many people beginning to use computers in many parts of their everyday life, the potential for abuse and crime will increase. Kingsley (1992), playing the character Cosmo, in the motion picture *Sneakers*, questions our understanding of the role of information in today's society:

> "The world isn't run by weapons any more or energy or money; it's run by little ones and zeros, little bits of data. It's all just electrons ... There's a war out there ... A world war, and it's not about who's got the most bullets, it's about who controls the information! What we see and hear, how we work, what we think - it's all about the information."

In the future, more so than ever, information will mean power. It is essential therefore that our legal system produce a uniform legislation that is not only well defined, but that ensures that the "power" of the future is with the people of society, and not only concentrated in the hands of the few.



The Australian, 16 February 1992

BIBLIOGRAPHY

Bloombecker, B.	(1990). *Spectacular Computer Crimes.* Illinois: Dow Jones-Irwin.
Clough, B. et. al.	(1992). *Approaching Zero - Data Crime and the Computer Underworld.* London: Faber and Faber.
Cudmore, G.	(1994). *Computers and the Law.* Collingwood: VCTA Publishing.
Dwyer, T. et. al.	(1992). *IPT - Information Processing and Technology.* Melbourne: Pitman Publishing, 149-151.
Ellis, D.	(1994). "After You've Beat 'Em - Join 'Em". *Time Almanac 1990s* (CD-ROM). London: Softkey International / Time Inc. Magazine Co.
Elmer-DeWitt, P.	(1994). "Cyberpunk!". *Time Almanac 1990s* (CD-ROM). London: Softkey International / Time Inc. Magazine Co.
Elmer-DeWitt, P.	(1994). "Cyberpunks and the Constitution". *Time Almanac 1990s* (CD-ROM). London: Softkey International / Time Inc. Magazine Co.
Elmer-DeWitt, P.	(1994). "Ghost in the Machine". *Time Almanac 1990s* (CD-ROM). London: Softkey International / Time Inc. Magazine Co.
Elmer-DeWitt, P.	(1994). "Who Should Keep the Keys?". *Time Almanac 1990s* (CD-ROM). London: Softkey International / Time Inc. Magazine Co.
Goodell, J.	(1995). "Cyberthief". *Rolling Stone.* Issue 510, 52-57, 95.
Kinglsey, B.	(1992). *Sneakers* (video recording). Los Angeles: Universal Pictures.
Ohlin, L.E.	(1975). "Crime". In *The World Book Encyclopedia.* Chicago: Field Enterprises, vol. 4, 908e-909.
Peterzell, J.	(1994). "Spying and Sabotage by Computer". *Time Almanac 1990s* (CD-ROM). London: Softkey International / Time Inc. Magazine Co.
Stoll, C.	(1991). *The Cuckoo's Egg.* London: Pan Books.