Global Information Assurance Certification Paper

Synopsis of the Cybercrime Act 2001

Abstract

A rapid progression in computing technology over recent years has brought with it a large increase in computer-related crimes. In addition, terrorist groups are embracing this technology and using it to facilitate and coordinate terrorist acts. In reaction to these developments, Australian legislation has been introduced to criminalise various computer activities. Under the *Cybercrime Act 2001* [9] (hereafter referred to as the *"Act*") such activities now include hacking, virus propagation, denial of service attacks, and web site vandalism.
Although deemed necessary legislation, the *Act* has been strongly criticised by members of the Australian IT community, suggesting that certain legitimate IT activities have now been criminalised. This paper explores and explains the *Act* and it's potential impact on IT Professionals in Australia, highlighting areas of concern and possible amendments to the *Act*, providing a single point of reference on the *Act* for an Australian IT Professional.

1. Introduction

In the wake of the September 11, 2001 terrorist attacks in the United States, the *Cybercrime Bill 2001* [10] was rushed through the Australian Parliament with a host of other legislation, and is now in force as the *Cybercrime Act 2001*. It has significantly changed existing legislation relating to malicious cyber activity, and is the third piece of legislation to be passed since 1989 for cyber crime, providing a much-needed update to the most recent amendment of the *Criminal Code 1995* [13].
Provisions of the *Act* are consistent with the terms of the *Council of Europe Convention on Cybercrime* [5] on which the *Model Criminal Code* [15] was based, and extends, amongst other legislation, the *Crimes Act 1914* [12] and the *Customs Act 1901* [14].

While the *Act* reflects the types of criminal activity taking place in cyberspace, there are concerns about the breadth of the proposed new investigative powers [4]. Concern also exists over the excessively broad definitions adopted by the legislation, and the extent to which the *Act* has been left for interpretation by the courts [3]. More specifically, the *Act* has attracted criticism from the IT security industry due to the high potential for offences to be committed in the course of (legitimate) every day investigations carried out to determine the level of security or otherwise of a client's system [8].

This paper provides a single point of reference for those that may be affected by the *Act*. It is specifically written for Australian IT Security Professionals, however information presented here may be of interest to other IT Professionals, law enforcement bodies, legal entities, businesses and home computer users. This

paper not only presents the *Act* in the context of related legislation, it makes salient the changes, what those amendments mean, and any contentious issues with the *Act*. A short case study ties together some aspects of the *Act* to assist the non-legalistic reader understand the implications of the *Act*. A number of recommendations are also presented, detailing changes that may improve the *Act*, and advice is provided to IT Security Professionals.

2. The Cybercrime Act 2001

2.1 Influences on the Act

The *Cybercrime Bill 2001* was first tabled by the Attorney-General of Australia in June 2001. This *Bill* was primarily based on the *Council of Europe Draft Convention on Cyber-Crime 2000*, and implements section 4.2 of the *Model Criminal Code* which was released in January 2001. In October 2001, amidst much controversy, the *Cybercrime Act 2001* was passed and it became enforceable in April 2002. The *Act* amended existing federal legislation, including the *Crimes Act 1914,* the *Criminal Code Act 1995*, and the *Customs Act 1901*.

In 1989, the *Crimes Act 1914* was amended to take into account computer-related offences. Further steps were not taken to address the lack of legislation surrounding computer-related crime until the *Criminal Code Act 1995* was updated. Again, technology moved faster than the legislators could have imagined, and a new requirement for legislation was identified. It took a series of events, including the September 11 attacks in the US, large scale Denial of Service attacks, and a spate of rapidly proliferating malicious viruses, before the *Cybercrime Bill 2001* was rushed through the Australian Parliament.
It was this reactive and overzealous approach to the *Act* that seems to have resulted in the degree of controversy surrounding the *Act*, with debate continuing to this day.

According to a report in 2002 by Deloitte Touche Tohmatsu [1], recorded computer crime in Australia had doubled since 1999 and at that point exceeded US levels. This was despite increased investment in security and strong adoption of security technologies. Such an increase in computer crime seemed justification for amendments to the *Crimes Act 1914* and other relevant legislation. The fact that more attacks on Australian organisations originated from outside rather than inside, with most of these crimes going unreported to law enforcement authorities, drove home the point that there needed to be provisions whereby such activities would be criminalised.

The *Cybercrime Act 2001* was seen as a measure to provide a significant deterrent to those wishing to commit a cyber crime, and at the same time encourage victims of computer crime to report an incident to authorities. Importantly, while the number of computer crimes committed rose from 1999 to

the end of 2002, the percentage of incidents reported more than doubled, with the biggest increase being reporting of incidents to law enforcement groups. The biggest challenge in persuading organisations to report a cyber crime appears to be that most organisations do not believe perpetrators will be caught. While the *Act* seems to be having a positive impact in this respect, there is still work to be done on education in regards to computer crime. Chalmers [2] suggests that in fact the *Act* is simply intended to fulfill a symbolic role in painting cyberspace as a more regulated and safer place to inhabit, meaning that the *Act* has already fulfilled its intended purpose.

Criticism of the *Act* has come from a number of groups, and was formally presented in an inquiry into the *Cybercrime Bill 2001*. This inquiry included representatives from sectors including the IT/computer, Internet, and crime sectors, arguably all those that should have been consulted earlier, with representatives from the Attorney-General's Department to provide further insight to the *Bill*. Issues with the *Act* will be discussed further in this paper.

2.2 Overview of the Act

The Cybercrime Act 2001 enacts seven new computer offences based on the *Model Criminal Code* Damage and Computer Offences Report 2001. Seen as a vital first step to achieving national consistency and remedying deficiencies in the existing laws, updated offences replace existing and obsolete ones under the *Crimes Act 1914* [7]. Explanatory text on these offences is primarily sourced from the Second Reading [7] and is presented below.

2.2.1 Division 477 – Serious Computer Offences

477.1 Unauthorised access, modification or impairment with intent to commit a serious offence

This targets those who access or modify computer data or impair electronic communications to or from a computer that they are not authorised to access, modify or impair and who do so with the intention of committing a serious offence, punishable by five or more years imprisonment.
This was designed to stop hackers using data obtained to commit a serious offence, such as accessing and using credit card details to obtain money.

477.2 Unauthorised modification of data to cause impairment

This makes it an offence for a person to cause unauthorised modification of data in a computer where the person is "reckless" as to whether that modification will impair data. This criminalises activities such as hacking a system to impair data or intending to spread a virus.

477.3 Unauthorised impairment of electronic communication

This was intended to cover Denial of Service attacks such that any unauthorised impairment of electronic communications to or from a computer now carries the maximum penalty of 10 years imprisonment. An example of an offence here would be to flood a website with requests, resulting in a denial of service.

2.2.2 Division 478 – Other computer offences

478.1 Unauthorised access to, or modification of, restricted data

This relates only to unauthorised access or modification of data that is protected by an access control system such as password protection. Someone that enters a system with access control without authorisation can be imprisoned for up to two years.

478.2 Unauthorised impairment of data held on a computer disk

This relates specifically to a Commonwealth computer disk, credit card or other device, and carries a maximum of two years imprisonment for someone that destroys one of these devices, for example, by magnetically scrambling a disk.

478.3 Possession or control of data with intent to commit a computer offence, and 478.4 Producing, supplying or obtaining data with intent to commit a computer offence

These cover the use and supply of programs (and or data) intended to commit a computer offence. A person can be imprisoned for up to three years if he/she possesses a computer security or diagnostics tool with the intent to commit a computer offence based on the data they obtain using such tools. It would not be an offence, however, to merely be found in possession of such a tool with no intent of committing a computer crime.

2.2.3 Investigative Powers

In addition to Divisions 477 & 478 of Schedule 1, Schedule 2 of the *Act* introduces changes to investigative powers that facilitate enforcement of these laws. The *Act* amends and extends both the *Crimes Act 1914* and the *Customs Act 1901* provisions relating to search, seizure and copying of electronically stored data.

Again, technological advances have superseded these changes, with problems presented by the vast amounts of data held on storage devices, and the protection of data offered by means such as encryption.

New powers in the *Act* allow the issuing of warrants to cover an entire premise for a particular set of data, and are not necessarily restricted to one physical device.

In order to facilitate searches, equipment can now be moved off premises or data copied for such purposes, and the Courts can give an order for a person with knowledge of a particular computer system to provide assistance during an investigation.

2.3 Explanation and Criticisms of the Act

While the *Cybercrime Act 2001* is seen largely as a step in the right direction in addressing the serious and difficult task of protecting against cyber crime and prosecuting cyber criminals, a number of areas of concern have been raised. Such areas identified during the inquiry [16] include:

- the breadth of the proposed offences – some considered that the offences were not sufficiently precise enough to ensure they would be applied only to truly criminal behaviour;
- the definitions – some of the definitions were thought to be overly broad;
- the investigative powers – raised serious civil liberty concerns and privacy issues; and
- other privacy issues – in protecting private material, decisions are based on internal rules and guidelines of the investigating authority.

Opinions on the effectiveness of the *Act* vary, with the potential impact of its enforcement felt by numerous sectors of the community.
The main criticisms of the *Act* are the imprecise definitions used and the invasive nature of the investigative powers permitted.
McCullagh and McEniery [8] state that activities such as penetration testing and ethical attacks without authority will technically offend the provisions despite the intention behind them. This is absolutely the case, and is in fact a key point to the *Act*, that it is necessary to have authority before performing such activities. One should always ensure they have the necessary authority, although the definition of "authority" is somewhat lacking, and unfortunately the *Act* doesn't go so far as to say who may grant authority to access a system.
In the same paper, McCullagh and McEniery issued a warning to IT security providers to be careful in the allocation of security tools to staff and consultants, implying the providers may also be liable in the event such tools are used maliciously. What they fail to recognise here is that the providers must also have **intent** to commit or aid in the committing of a crime.

As is to be expected, different perspectives have resulted in different criticisms of the *Act*. Electronic Frontiers Australia (EFA) [6], in their commentary on the *Cybercrime Bill 2001*, were most critical of the assistance order provisions in Schedule 2 of the *Act* stating that the provisions present controversial issues and major difficulties. This commentary was seemingly ignored by the legislators with suggested amendments not appearing in the *Act*. EFA posed the question that if confidential information were left lying around in a public place, would we charge the finder with a criminal offence, and further stated that the Bill does exactly that under the offence of unauthorised access (478.1).

Criticism of the *Act* by Chan et al. [3] focuses on the broad definitions adopted by the legislation. They cite the definitions of "restricted data" and "authorisation", the mental elements of the offences (intent, knowledge and recklessness), and the actions that constitute an offence (unauthorised access, modification and impairment) as the major pitfalls of Schedule 1 of the legislation:

- "Restricted Data" is data held in a computer where access is restricted by an access control system. It is not, as the name would suggest, data that has associated access control placed upon it. Access to such data must be authorised, regardless of the security applied to it. The question here is "who can provide authorisation to access such data?".
- "Authorisation" is a grey area. There is no explanation in the *Act* regarding who may grant authorisation. Is it, for example, a system administrator, the owner of a file, the creator of a file, or an organisation?
- Chan et al. question the use of the word "recklessness" in the context of viruses, asking if it is considered "reckless" to not have the latest virus definition and consequently spread a virus. The law certainly regards this as reckless, although a judge's interpretation may be different.
- "Intent" and "Knowledge" are essential and central to infringements to Schedule 1 amendments, however the meaning of unauthorised access, modification or impairment fails to recognise this. Furthermore, it is not necessary for a person to be aware that they are committing such a crime.

The Law enforcement provisions in Schedule 2 of the *Cybercrime Act 2001* have also come under criticism for potentially undermining confidence in the security and integrity of electronic transactions [8]. By far the most criticised aspect of Schedule 2 is the section to be inserted in section 3LA of the *Crimes Act 1914* that allows a magistrate to make an assistance order that requires a specified person to provide information and assistance to enable access to, copying or printing of data. The intention of this amendment was to provide a means by which police could decrypt data and obtain passwords, however it doesn't take into account the possibility of someone genuinely losing an encryption/decryption key or forgetting their password. As stated, failure to provide assistance in this instance could result in imprisonment for up to six months.

John Corker [4] explains that search warrants, issued under section 3L(1) of the *Crimes Act 1914* and the equivalent in the *Customs Act 1901*, may be used to access data accessible from the search premises. As most computers are connected to the Internet, this theoretically extends to every computer connected.
Furthermore, under section 3L(1A) of the *Crimes Act 1914* and equivalent in the *Customs Act 1901*, all data on a computer may be copied, even if only some of the data is suspected of containing evidential material. Given the storage capacity of computers, this could be a vast amount of irrelevant and personal information. Equipment may also be taken to another location for up to five days to assist in this process, which may be enough time to do considerable damage to a business.

The *Cybercrime Act 2001* can be difficult to understand as it introduces a number of new concepts and amends other existing legislation. For ease of understanding, this section presents a scenario illustrating what an IT Security

Professional may have to consider in light of this legislation. This is presented below, followed by a brief discussion.

2.3.1 Demonstration

To demonstrate some of the most important aspects of the *Cybercrime Act 2001*, and possible implications for the IT Security Professional, a grossly simplified hypothetical situation is presented and is followed by a discussion that demonstrates pertinent issues. This by no means covers all possible scenarios, nor does it attempt to explain every facet of the *Act*, but does provide a more tangible way in which the reader can understand the impact the *Act* can have on both legitimate and illegitimate computer users.

The scenario consists of an IT security contractor ("Contractor"), hired by a medium sized organisation ("Business 1"), where his role is to "improve security, update and upgrade existing systems and relocate to new premises". This job coincides with this group of the company expanding and moving into new office space. The branch in question is one of four similar sized offices located in Australia, although it is not the company's headquarters.

Presented in Table 2.1 below is the "tool box" of the Contractor for this task. These software tools are some of the more popular tools in use amongst IT Security Professionals.

IT Security Tool	Description of Function
Ethereal	packet analysis
RAT (router auditing tool)	provides automated way to determine the security of a Cisco router and provides details as to why it isn't secure
Nessus, nmap	vulnerability and port scanning
S-Tools, Invisible secrets	steganography tools
PGP	data encryption tool
NetStumbler	Windows utility for 802.11b wireless network auditing
L0phtCrack	tests strength of passwords

Table 2.1 IT Security Tools

This task consists of the following work units:

1. Relocate existing network:
    a. Backup existing configurations and data before transport. This data needs to be encrypted in the event it is lost or stolen.
    b. Transport equipment to new premises and re-install.

2. Perform upgrades to network and provide additional infrastructure:
    a. Install new cabling, servers, PCs, routers, printers, and other devices as necessary.

3. Add wireless network:
    a. All managers' equipment must be upgraded for the inclusion of a wireless network.
    b. Test network with NetStumbler to determine wireless security and if spillage has occurred. Sign-off is provided by the Managing Director.

4. Apply patches and configure systems for security:
    a. The existing system required patching and was poorly configured from a security perspective – this must be remedied. This is done in cyclic fashion with step 5 below.

5. Audit system:
    a. The systems must be examined to determine weaknesses. Tools used include Ethereal, RAT, Nmap, and Nessus.

6. Audit passwords and other user details:
    a. Citing poor existing user security practices, and with the addition of a new security policy, Business 1 wants to ensure that users are adhering to procedures. L0phtCrack is used to check password strength.

2.3.2 Discussion

Unfortunately for Business 1, an associated company ("Business 2") is being investigated for suspected criminal activity. Business 1 is also now under investigation for dealings with this company.
Under the *Act*, an assistance order has been made on the Contractor, and failure to comply could result in criminal charges.

The first thing the investigators ask for is the data that has been exchanged between the two companies including any records of transactions and e-mails. While the Contractor is able to provide some of this data (already copied for relocation), he needs to provide the encryption key, as the data was encrypted using one private key. Unfortunately the Contractor cannot find the key he used to encrypt the data, and is warned that failure to provide assistance could result in up to six months imprisonment.
The investigators decide that rather than charging the Contractor, they will need to make a copy of all the data directly from all devices, however they don't have the necessary equipment with them, so they decide to take the data (servers, backup tapes and drives, some PCs) back to their lab for 5 days where they can copy that data. Business 1 must comply with this under the *Act* and will have to shut down operations for at least a working week.

A week has elapsed and the investigators hand back all equipment, meaning Business 1 can resume its relocation in conjunction with the investigation.

The Contractor finishes the first two steps, at which point he starts work on setting up the wireless network. After setup, he decides to use NetStumbler for network diagnostics, and promptly receives a visit from the investigators. The investigators, who had set up a small work area in Business 1's new office space, had their own wireless network, and were aware of someone sniffing their traffic. When confronted in regards to this, the Contractor did not deny that he had been sniffing, but was not aware that he was sniffing another network. He simply wanted to determine the boundaries of his own for security purposes, but was accessing restricted data without authorisation, even though he wasn't aware of doing so. The investigators warned him that they could charge him for an infringement of the *Act* (punishable by up to two years imprisonment under Section 478.1), but as they are aware that he is just doing his job, decide to waiver it this time. The Contractor has now breached the *Act* twice.

After upgrading and expanding the systems, applying all necessary patches to the system and changing the configuration to be more secure, the Contractor decides to perform some system audits to determine the security offered by the current systems. Using RAT on the new Cisco routers for configuration, and Nessus and Nmap for vulnerability and port scanning, the Contractor is now happy that he has the information required to further harden the systems. He then performs a check on the strength of all users' passwords, keeping a list of all passwords on his computer.
At this point, the investigators decide they have enough evidence to implicate Business 1 in the criminal activities of Business 2, so they inform Business 1's management. Being the good people that they are, Business 1's managers find a scapegoat to get them out of trouble – the Contractor! The investigators find this hard to believe, however they have to explore all avenues, and the existing magistrate's order already covers the Contractor's computer. Inspection of the computer reveals a number of "hacking" tools, including Ethereal, Nmap, Nessus, RAT, and L0phtCrack, together with not only the company's system information, but passwords for every user's account. Having a tool for steganography on his machine certainly didn't help. Unfortunately for the Contractor, he didn't gain written permission to be carrying out many of his tasks, and now has tools on his computer, together with information, that is considered illegal under the *Act*. It is now his word against the company, and he stands to face up to three years imprisonment if convicted under Section 478.3 of the *Act*.

3. Recommendations

3.1 IT Professionals

The following is a basic list of recommendations, particularly for IT Security Professionals, for operating under the *Cybercrime Act 2001*. Although common sense, they are listed here for completeness:

- Become familiar with all applicable legislation and how each applies to any activities to be carried out. This includes the *Cybercrime Act 2001* and it's *Explanatory Memorandum* and *Second Reading*, the *Crimes Act 1914*, the *Criminal Code 1995*, the *Model Criminal Code*, the *Telecommunications Act*, the *Customs Act 1901* [9,10,11,7,12,13,15,17,14].
- McCullagh and McEniery [8] advise to always seek written permission that legitimately authorises work to be carried out, and ensure that this carries with it the appropriate indemnities from all clients prior to conducting any security investigations in order to avoid criminal liability.
- If any legal concerns exist in regards to the conduct of work, seek legal advice before commencing.
- Ensure secure storage of encryption keys and passwords, details of contracts, and authorisation for work performed.
- Inform staff involved in an IT security-related task how this activity is to be performed and when it is going to occur. This should include a summary of the effects and implications this may have.

3.2 Changes to Legislation

While the *Act* is seen as a step in the right direction, and addresses many concerns that stakeholders had in regards to updating legislation for prosecution of those that commit computer crimes, some aspects of the *Act* are still cause for concern.

The inquiry into the *Cybercrime Bill 2001* produced seven recommendations made by the committee (which included industry representatives) that attempted to eliminate ambiguity and the possibility of subjective interpretation of the *Act*. These recommendations have been largely dismissed, making it difficult for further amendments to be approved.

To highlight aspects of the *Act* that are cause for concern, a list of recommendations is presented detailing possible improvements:

- Definitions should be narrower in scope [3], so as to confine offences to actual malicious activity. In particular, "unauthorised" should be further defined so that guidelines on identifying the appropriate authority for access, modification or impairment of data can be included in the provisions. Guidelines should state who can provide authorization and how the scope of this is determined. This may be achieved by a more detailed definition of "unauthorised".

- Both Sections 477.2 and 477.3 should require knowledge and intent, as opposed to recklessness (which also lacks a suitable definition) and knowledge.
- In respect to Paragraph 3LA, failure to provide assistance should not be an automatic offence, especially where encryption keys are concerned [3].
- Cause, knowledge, malicious intent and actual damage should be established as prerequisites in respect of all of the proposed new offence provisions [6].
- In conjunction with the Privacy Commissioner, regulations should be developed covering access to third party information that are subject to disallowance [16].
- Remote access should not be permitted and, in the event that it is, the warrant should be restricted to accessing data on a remote computer that is directly related to the computer being used for access at the warrant premises [4].
- A specialized IT savvy legal body should be established with jurisdiction to deal with the granting of warrants and other orders, rather than judges that lack the technical knowledge to understand the implications of granting such an order.
- Require a "license" to possess IT security tools, so that those registered would have considerably more flexibility to go about their task without the risk of inadvertently breaching the *Act*.

4. Conclusion

With a spate of crimes being committed in cyber space and with no real mechanism existing in Australia to criminalise such activities, the Australian Parliament passed the *Cybercrime Act 2001* which commenced in April 2002. This Act amended much of the existing legislation and provides a means by which to prosecute cyber criminals.
While the Act does make substantive and essential improvements to previously outdated legislation, stakeholders have criticised numerous aspects of it. IT industry groups believe the *Act* criminalises various actions intended to protect networks, echoing concerns raised by members of the security consultant community. Most criticisms stem from the broad definitions of various key terms and that a large amount of interpretation is required by courts.
Concern from legal bodies also exists in regards to the possible abuse of the *Act's* provisions by law enforcement agencies, citing the possibility of invasion of privacy and lessening of confidence in data security.

While there has been a formal inquiry into the *Act*, there seems little chance that amendments will be made in the near future. Advice for those affected by the *Act* consists of understanding all legal obligations and legislation, always seeking authority before performing any activities, and to keep thorough records of all activities. If in any doubt, one should seek legal advice.

5. References

[1] 2002 Australian Computer Crime and Security Survey. Technical Report, AusCert, Deloitte Touche Tohmatsu, NSW State Police, May 2002. www.security.iia.net.au/downloads/ crime%20and%20security%20survey.pdf

[2] Chalmers, Robert. Regulating the Net in Australia: Firing Blanks or Silver Bullets? Murdoch University Electronic Journal of Law, Volume 9, Number 3 (September 2002). www.murdoch.edu.au/elaw/issues/v9n3/chalmers93.html

[3] Chan *et al.* The Threat of the Cybercrime Act 2001 to Australian IT professionals. Proceedings of the First Australian Undergraduate Student's Computing Conference, 2003. www.cs.mu.oz.au/~bir/auscc03/papers/chan-auscc03.pdf

[4] Corker, John. Submission on Cybercrime Bill 2001. Letter to the Secretary, Senate Legal and Constitutional Committee, Parliament House Canberra. www.oznetlaw.net.au/pdffiles/Cybercrime_submission.pdf

[5] Council of Europe, Convention on Cyber-crime – Explanatory Memorandum. http://conventions.coe.int/Treaty/EN/projects/Final/CyberRapex.htm

[6] Electronic Frontiers Australia. Commentary on the Cybercrime Bill 2001. http://www.efa.org.au/Publish/cybercrime_bill.html.

[7] House of Representatives Official Hansard, Wednesday 27 June 2001, Thirty-Ninth Parliament, First Session – Ninth Period. Cybercrime Bill 2001 Second Reading, Mr Williams (Tangney – Attorney General).

[8] McCullagh, Adrian and McEniery, Martin. Cybercrime Act: some unforseen consequences. FindLaw Australia. http://www.findlaw.com.au/articles/printArticle.asp?id=6442

[9] Parliament of the Commonwealth of Australia. Cybercrime Act 2001, No. 161, 2001.

[10] Parliament of the Commonwealth of Australia. Cybercrime Bill 2001.

[11] Parliament of the Commonwealth of Australia. Cybercrime Bill 2001, Explanatory Memorandum, 2001.

[12] Parliament of the Commonwealth of Australia, Crimes Act 1914.

[13] Parliament of the Commonwealth of Australia. Criminal Code 1995.

[14] Parliament of the Commonwealth of Australia. Customs Act 1901.

[15] Parliament of the Commonwealth of Australia. Model Criminal Code, 2001.

[16] Parliament of the Commonwealth of Australia, Senate Legal and Constitutional Legislation Committee. Consideration of legislation referred to the Committee, Inquiry into the Provisions of the Cybercrime Bill 2001, August 2001.

[17] Parliament of the Commonwealth of Australia. Telecommunications Act 1997.