# THE THREAT OF THE CYBERCRIME ACT 2001 TO AUSTRALIAN IT PROFESSIONALS

Nelson Chan[1], Simon Coronel[1], & Yik Chiat Ong [2]

[1] Department of Computer Science and Software Engineering,
The University of Melbourne
[2] Faculty of Law, The University of Melbourne

ABSTRACT: Well known flaws in popular software and the resulting large scale outbreaks of computer viruses and worms have raised public awareness and concern over the vulnerability of computer systems. Recent terrorist activity in and against the United States of America have also increased the profile of malicious cyberspace activities. With such a risk to the Australian public, and because of a perception by legislators that there is a lack of suitable laws to deal with cyber-incidents, the Cybercrime Act 2001 was created. Unfortunately, due to the lack of adequate consultation and the broad definitions adopted by the Cybercrime Act 2001, many members of the IT community are now at risk of prosecution for doing legitimate work. In order to demonstrate the threat that the Act presents, this paper critically examines the details of the changes the Act makes to exising legislation. The historical context of the Act, influences in its development, and its similarities to existing problematic legislation are examined. The wider threat that the Act presents to the Australian IT community is discussed. Suggestions about how to improve the Act are also provided.

## INTRODUCTION

In April 2002, the Cybercrime Act 2001 came into effect in Australia. This was the third time that a Federal Government has passed cybercrime legislation; previous legislation being passed in 1989 and 1995. Each attempt was aimed at reducing the gap between legislation and malicious online activity.

However, the Cybercrime Act 2001 is the subject of much controversy as critics argue that it is too broad in jurisdiction, extends police powers too far, and threatens to facilitate the unjust conviction of many Information Technology (IT) professionals [5]. Much of the criticism is based on the excessively broad definitions adopted by the legislation, and the extent to which the Act has been left for interpretation by the courts.

This paper examines the Cybercrime Act 2001 and investigates the implications that it holds for all those who work in the IT industry. We will argue that the Cybercrime Act exposes IT professionals to an unreasonable degree of vulnerability to prosecution. In order to do this we will examine the Cybercrime Act 2001; the offences introduced and the investigative powers granted. We will also look at the influences to the Act's development; the aims of its authors and whether those aims were met.

Other equivalent legislation will be used as a basis for analysing the Act. Consideration will be given to the Model Criminal Code, the Council of Europe (CoE) Convention on Cybercrime, the Senate Legal and Constitutional Committee Hearings and Inquiry (with the accompanying submissions) into the Cybercrime Bill, and expert opinions from the IT and wider community. Suggestions about how to improve the Act will also be provided.

## HISTORICAL CONTEXT OF THE CYBERCRIME ACT

This most recent iteration of Australia's cybercrime laws is not the first time that questionable computer and Internet legislation has been passed by a government. The IT industry has been characterised by rapid advances in technology, enabling society to commmunicate and interact to a degree previously unheard of. However, new possibilities in computer and communications technology also mean new possibilities in crimes. It is a frequently observed phenomenon that the rate of technological advancement tends to be faster than the advancement of corresponding legislation. Nonetheless, governments

have made various concerted attempts over the past few decades to address the ever-growing issue of cybercrime[1].

The first reported incidences of what is now known as cybercrime appeared in the late 70s, with various relatively minor incidents of hacking[2] and phreaking[3]. However, as the size, accessibility and popularity of the Internet grew, so did the incidences of cybercrime in both number and significance.

The first item of Federal legislation regarding cybercrime in Australia was the Amendments to the Crimes Act, 1989 [17]. Further amendments were made to the Criminal Code Act in 1995, which were intended to address new crimes made more pervasive by advances in computer technology, such as hacking, denial of service attacks and virus propagation [14]. These legislations were passed with relatively little controversy and were developed as measures to combat the growing pervasiveness of cybercrime [17].

In the years since the amendments to the Crimes Act and Criminal Code Act, the Australian Government has observed that further advances in technology have necessitated further updates to the law [6]. These updates have finally arrived in the form of the Cybercrime Act 2001.

## THE CYBERCRIME ACT 2001

The developments heralded by the Cybercrime Act 2001 will threaten IT professionals with criminal convictions for previously legitimate activities. Although IT advocacy groups such as the Australian Computer Society (ACS), 2600 Australia, Electronic Frontiers Australia (EFA) and many others praise the motives of the Act, they are all concerned with the implications that the Act have for Australian IT professionals. Their evidence given to the Senate Inquiry Committee expresses the misgivings they hold regarding both the breadth of the new offences and the scope of the new powers [7, 8].

### New offences under the Cybercrime Act

The Cybercrime Act 2001 introduces the following new offences to the Criminal Code Act 1995.

The serious offences are under Division 477, being:

1. Section 477.1 Unauthorised access, modification or impairment with intent to commit a serious offence.
2. Section 477.2 Unauthorised modification of data to cause impairment.
3. Section 477.3 Unauthorised impairment of electronic communication.

The other offences are under Division 478, being:

1. Section 478.1 Unauthorised access to, or modification of, restricted data.
2. Section 478.2 Unauthorised impairment of data in a computer disk etc.
3. Section 478.3 Possession or control of data with intent to commit a computer offence.
4. Section 478.4 Producing, supplying or obtaining data with intent to commit a computer offence.

### Critical examination of definitions

The leading criticism against the Cybercrime Act is that it criminalises far too much, far too easily, leading to severe consequences for IT professionals. This problem arises primarily from the overly

[1] For the purposes of this essay, cybercrime is defi ned as criminal or malicious online activity.

[2] "Hacking" is an unauthorised attempt, or actual, entry to a computer system. Note that the authors feel this term is inaccurate, but due to widespread media usage, will be used for the sake of simplicity

[3] "Phreaking" is the act of illegally bypassing the payment systems of telephones in order to make free calls.

broad definitions adopted by this legislation, specifically “the breadth of the terms ... defined [in the Cybercrime Act] has created an even broader scope of potential criminality” [16].

Among the most concerning aspects of the Act are the definitions of “restricted data”, “authorisation”; the mental elements of the offences, and the actions which constitute an offence: unauthorised access, modification and impairment.

“Restricted Data”

For a set of data to be defined as restricted, it merely needs to be held in a computer which uses an access control system. It is NOT a requirement that the data itself is protected by an access control system, only the computer. Under this definition, the requirement of “restricted data” can be too easily met since almost all computers are protected by at least a password[4]. Hence in order to be in breach of s 478.1, all an individual needs to do is view almost any data without authorisation, whether or not that data was secured [9]. This is further complicated by the lack of explanation of what constitutes having “authorisation”.

“Authorisation”

A key requirement for conviction under any of the Division 477 offences and half those of the Division 478 offences is that access, modification, or impairment is undertaken without “authorisation”. Yet, the Cybercrime Act merely states that the action undertaken must be unauthorised, without actually specifying what constitutes authorisation.

The Act in no way addresses situations where authorisation may be disputed, revoked or granted conditionally. If, for example, an IT professional is hired to perform some work, but if in the course of that work, the authorisation granted to that person is disputed or revoked, then there may exist grounds for prosecution under s 478.2 for “unauthorised access or modification to restricted data” [9]. The additional requirement of “restricted data” can be easily met, as explained above.

Furthermore, there exist no guidelines as to who are the proper authorities (or sole authority) for the granting of authorisation to access, modify or impair data; it could entail any of the following authorities: the owner of the data, the owner of the account, the owner of the system, or the administrator of the system.

Thus, in any of these situations where authorisation is not clearly and explicitly expressed without reservation, any IT professional will risk a criminal conviction and up to a maximum penalty of 2 years imprisonment [9].

The mental elements: intent, knowledge and recklessness

In order to establish the mental element of the offences, the summary (ss 478.1 and 478.2) and preparatory offences (ss 478.3 and 478.4) all require knowledge and intent [16]. However, the main offences of unauthorised modification of data (s 477.2) and impairment of electronic communication (s 477.3) only require recklessness and knowledge.

The inclusion of ”recklessness” is troubling, considering the acknowledged danger of viruses today. ”Recklessness” is defined in s 5.4 of the Criminal Code as being ”aware of a substantial risk” and ”it was unjustifiable to take that risk” [9]. As viruses will typically cause impairment without authorisation, the very lack of the latest and best anti-viral software may constitute being reckless as to causing impairment. *There is no requirement that impairment actually occurs* [9]. This situation is only one of many where recklessness may be claimed, especially if security best-practices are not followed (for example, the use of telnet, or any other program that utilises unencrypted communication may constitute recklessness).

[4] 100% of all respondents to the 2002 Australian Computer Crime and Security Survey [1] use passwords, a form of access control system.

Furthermore, knowledge or intention in relation to access, modification and impairment is irrelevant according to the definitions in s 476.2. This means that awareness that any access, modification or impairment has resulted is not an element of the offence; prosecution only needs to show that access, modification or impairment has been caused [16].

### "Data" prohibited by the Act

Further demonstration of the threat posed to IT professionals by the Cybercrime Act can be seen in ss 478.3 and 478.4. These sections apply further constraints to hereto legitimate but necessary activities of IT professionals. In combination, these sections prohibit and criminalise the possession, control, supply, production, or obtaining of data (i.e. programs or other computer tools) that can be used to commit or facilitate the commission of any offence under Division 477 [9].

What legislators fail to realise is that IT professionals and researchers routinely use programs that can be used to commit or facilitate the commission of Division 477 offences, simply because such programs also have legitimate purposes. Examples of such programs include nmap (a utility to determine the usage of each port of a system), netstumbler (program that measures signal strength of wireless networks), and even root passwords (the password of a systems administrator), all of which may be used to facilitate the commission of a serious offence.

## POWERS GRANTED BY THE CYBERCRIME ACT

The majority of Schedule 2 redefines certain terms of the Crimes Act 1914, in order to be consistent with Schedule 1 of the Act. However, when redefining these terms, legislators also took the opportunity to introduce new powers for law enforcement.

New powers granted to law enforcement include: [9]

1. The power to remove a "a thing" to another place for examination or processing in order to determine whether it may be seized under a warrant" if it is more practical, or there are reasonable grounds that the "thing" includes or is evidence. (Paragraph 3K)
2. The power to "operate electronic equipment at the warrant premises to access data (including data not held at the premises)" if the police in question believe that the data (may) contains evidentiary material. (Paragraph 3L1A)
3. The power to require a person "to provide any information or assistance that is reasonable and necessary to allow the officer to" make a copy of data from equipment that might contain evidential material.
4. The power to require a "person with knowledge of a computer or a computer system to assist access etc." (Paragraph 3LA)

Of particular concern are the powers granted by paragraph 3L1A and 3LA. As a principle of law, search warrants are granted by the courts for a specific purpose; to search for a particular item at a particular location. The power described in Paragraph 3L1A of the Act removes the constraint of location, and will allow police to search and seize any computer technology that may be connected over a telecommunication services. Although the Government could not have intended to do so, this paragraph allows for a situation where police are granted a search warrant which may then be applied to any computer anywhere due to the nature of global networking via the Internet.

Paragraph 3LA of the Cybercrime Act may require that a person with "knowledge of a computer or a computer system" to assist a police officer to access data, make a copy of the data or convert the data into documentary form. Assistance may take the form where the person is required to explain the working of a computer system, or the disclosure of passwords and encryption keys. "A person commits an offence if the person fails to comply with the order" [9]. Under the Act no distinction is made at all between the inability to provide assistance and an unwillingness to provide assistance. If a person was

to genuinely forget certain information, for example, their password, when served with a warrant to assist access, then they would be liable to 6 months imprisonment [9] without any recourse.

Additionally "knowledge of a computer or a computer system" is not specified clearly as to whether it is sufficient to possess knowledge of a particular computer system, or a general knowledge of IT. There is also no limitation as to what the police may require assistance for. This potentially includes the disclosure of passwords, encryption keys, or other confidential or sensitive information. Without discussing the consequences this may have on the common law privilege of self-incrimination, the revelation of an encryption key or password may disclose information far beyond the scope of the warrant. Due to the nature of public-key encryption, revelation of a private key will compromise the confidentiality of all communication conducted with that key as well as the authenticity of future communications [3].

These two powers described in the legislation effectively allow police to search any computer, and to "request" assistance from any person to conduct that search. The only safeguard that the Australian public has towards protecting information disclosed in the course of a police investigation (whether related to the investigation or not) is the investigating agency's internal guidelines [7].

## INFLUENCES IN THE DEVELOPMENT OF THE CYBERCRIME ACT

The foremost influence on the Cybercrime Act 2001 is the Model Criminal Code[5] (MCC). Chapter 4 of the MCC deals with computer crime and cybercrime exclusively, and each offence in the Cybercrime Act can be traced to a recommendation made by the MCC [15]. Draft 25 of the Council of Europe (CoE) Convention on Cybercrime [6] was also strongly influential in guiding the development of the Act, to the point where consistency of the Act with the CoE convention is highlighted in the Explanatory Memorandum for the Cybercrime Act [15].

Incidents over the recent past have done a great deal to increase awareness and concern for incidents both offline and on. The development of a Cybercrime Act has been strongly influenced by a trend of increasing online attacks over the past decade [13], recent high profile outbreaks of malicious code, and the international concern of terrorism.

The past decade has seen an increase in online attacks in the form of viruses, worms, cyber-vandalism, which has in turn led to growing concerns of national and personal vulnerability to cybercrime. This trend came be seen in examining the period from 1997 until 2001 which saw the emergence of a continuous procession of virus epidemics (including the Melissa, SirCam and Nimda viruses, and the "Code Red I", "Code Red II" and "I Love You" worm among others), which caused at least financial losses of over US$150,000,000 in the USA [13] and almost AUS$900,000 in Australia [1].

What may have also been an influence, but one that cannot be quantified, is the impetus that the September 11th terrorist incident may have had in passing an ill-considered Bill through Parliament that could be possibly used against cyber-terrorism[7]. Certainly terrorist events have been a factor in the rapid passage of bills through the United States of America Congress, which impinge heavily on civil liberties. This includes the controversial USA PATRIOT Act[8].

The National Crime Authority represents the view of Australian law enforcement in saying that it "particularly supports the proposed new powers that will enable effective searches of computers and other electronic equipment" [7]. Yet in the course of the first Senate hearing into the Cybercrime Act, the National Director for the NCA could not verify that consultations were held as to whether the Cybercrime Act 2001 met law enforcement requirements in investigating cybercrimes [7].

Senator Ludwig of the Senate Legal and Constitutional Committee also continually pointed out that

[5] The Model Criminal Code (MCC) of the Committee of Attorney-Generals is a jointly developed guideline to ensure uniform structure, purpose and contents in Australian Criminal Codes in all States and Territories.

[6] Draft 25 of CoE convention was used, because at the time of development the Cybercrime Act, the CoE convention had not been fi nalised.

[7] Cyber-terrorism is "Any act of terrorism that uses information systems or digital technology (computers or computer networks) as either an instrument or target [4].

[8] Similar anti-terrorism legislation was proposed in the Australian House of Representatives but has so far been rejected by the Senate.

although organisations such as the NCA regarded the new powers granted as highly desirable, they did not possess sufficient expertise or knowledge to effectively utilise the new powers [7]. However, this has been somewhat addressed by the establishment of the Australian Hi-Tech Crime Centre [9] (AHTCC) in July 2003 in part to provide capability to enforce the cybercrime provisions.

The Senate hearings and subsequent inquiry into the Cybercrime Act also found that "it was abundantly clear that the Government did not include the information technology industry in the development of this legislation" [6] and that at no time during the development of the Bill that any effort was made to "consult with, or inform, all relevant stakeholders as to the intended content and application of the Bill" nor was there "public consultation or debate about the need for extended law enforcement powers" [6].

## COMPARISONS TO EQUIVALENT LEGISLATION

The Cybercrime Act 2001 came into effect on 1 April 2002. At the time of writing, no cases relating to these offences had been brought before the courts. However, this is not the first time a questionable piece of IT legislation has been passed. Over the last decade, several governments in Australia and overseas have developed well-intentioned but flawed technology legislation, such as the American Digital Millennium Copyright Act 1998 [12] (DMCA), UK Regulation of Investigatory Powers Act 2000 [11] (RIP Act) and the Oregon Computer Crime Law [10]. By examining some of these, we aim to emphasise the threat the Cybercrime Act presents by demonstrating its similarities to other pieces of legislation that have already been proven to be disproportionately severe.

An example of controversial legislation is the American State of Oregon's Computer Crime Law [10]. The Oregon legislation contains provisions that allows it to be misused to the detriment of well-meaning IT professionals. Section 164.377 of that Act makes it an offence to knowingly and without authorisation use, access or attempt to access any computer, computer system, computer network, software, program or data. Although its enactment was to close any legal loopholes which may enable hackers to escape prosecution, it has also endangered IT professionals acting in good faith.

One of the most well-known incidents involving the above Law was the case of Randal Schwartz, an IT consultant who was working as an independent contractor for Intel Corporation [10]. During his employment with Intel, he successfully ran a dictionary check against some of Intel's password files [11] to find obvious passwords [12]. Although he was unauthorised to do this, he did so in the belief that he could highlight security problems with Intel so that he would be offered a favourable contract upon the expiry of his current contract. His actions were discovered before he reported his findings. Schwartz was subsequently charged with and convicted of three counts of computer crime under Oregon's Computer Crime Law [13]. Hence, without malice aforethought, Schwartz was prosecuted based on some miscontrued actions alone.

The Schwartz case presents an ominous example for the future of Australian IT professionals following the introduction of the Cybercrime Act 2001. The Cybercrime Act 2001 is similar in many respects to the Oregon legislation; they both criminalise the unauthorised access and modification of electronic data, the unauthorised impairment of a computer network and the use of computers to facilitate a crime. The distinction between both pieces of cybercrime legislation is that a person's intention to commit these offences is irrelevant under the Oregon Crime Law. Nonetheless, the requirement of intention is still too easily satisfied under the Australian legislation.

Another prominent example of controversial legislation is the American Digital Millennium Copyright Act 1998 (DMCA). To counter the growing black market in pirated digital music and software, the DMCA

[9] http://www.ahtcc.gov.au

[10] For a more complete discussion of this case, please see http://www.lightlink.com/spacenka/fors/

[11] passwords in a *NIX system are stored in encrypted format, and logging in involves the encryption of the login password which is then compared to the encrypted stored password

[12] This is a common and well-known test for security and for crackers. The fact that Schwartz succeeded should highlight the obvious lack of proper security or its enforcement at Intel at the time.

[13] One count of "unlawfully, knowingly and without authorization altering a computer and computer network consisting of Intel computers", one count of "unlawfully, and knowingly accessing and using a computer and computer network for the purpose of committing theft of the Intel SSD's password fi le", and one count of "unlawfully, and knowingly accessing and using a computer and computer system for the purpose of committing theft of the Intel SSD individual user's passwords".

makes it an offence to circumvent protection on copyright material. Although this has been welcomed by content providers, it has also allowed the DMCA to be used as a tool for the suppression of legitimate research and software development.

One of the most well-known incidents involving the DMCA revolves around Edward Felten, a Professor of Computer Science at Princeton University. Felten headed a team researching (as part of a public challenge issued by the Record Industry Association of America (RIAA)) the security of RIAA copy-protection technology. Felten's team discovered loopholes in the technology, and wished to present their findings to the public. However, the RIAA threatened Felten with prosecution under the DMCA in order to prevent him and his team from revealing the results of their legitimate research [12].

As demonstrated in Felten's case, while the DMCA is a well-meaning and in many ways necessary piece of legislation, it contains clauses that allow it to be misused to the detriment of innocent individuals. The Cybercrime Act 2001 is similar in this respect, and both the Schwartz and Felten cases serve as examples of the threats that such legislation can represent to IT professionals and researchers.

## CONSEQUENCES OF THE CYBERCRIME ACT

Now that this legislation has been passed, members of the community, especially those working in the IT industry, must take note of its implications. As demonstrated in the case of Randal Schwartz, legislation similar in many respects to the Cybercrime Act has seen an eminent and highly-respected IT professional arrested and convicted for an innocuous act. Australian IT professionals now also risk the same happening to them.

The enactment of the Australian legislation means that it is now possible that other well-intentioned actions by Australian IT professionals may be regarded as criminal activities. IT professionals must now take a great deal more care in the performance of their duties, and must be much more aware of how their actions may be construed, to avoid risk of prosecution for their well-intentioned actions.

The enactment of the Cybercrime Act, and other legislation such as the DMCA and the RIP, indicates the beginning of a disturbing trend amongst technology legislation passed worldwide; a trend of misinformed and ill- considered legislation that bodes ill for those who work in technological industries. As shown by Felten's case, legislation similar in many respects to the Cybercrime Act prevented the publication and presentation of scientific and academic research into computer science until assurances were given by the US Federal Government that DMCA charges would not be laid against scientific endeavours.

As no similar assurances have been granted by the Australian Federal Government, the Cybercrime Act then heralds an era of de facto censorship in research and development of computer science fields. IT professionals or researchers that try to develop or publish material that relates to security may be prosecuted under the Cybercrime Act. It is unlikely that online developments by society's criminal elements will be deterred completely by the new Act, yet academics and other researchers will be. Australia may then see a drastic shift of knowledge to underground hacker and criminal movements, leaving Australian commercial and public interests to suffer the consequences. Ironically, the legislation designed to protect the IT community may end up harming it in the long term.

## RECOMMENDATIONS

Despite its flaws, the Cybercrime Act should not be repealed. The Act itself is important in amending out-of-date legislation to address cybercrimes such as hacking, denial of service attacks and virus propagation. However, the Act should be revised to take account of IT professionals so that innocent acts performed for work purposes are not criminalised. The recommendations discussed here are intended to create certainty and safeguard the interests of IT professionals.

Firstly, the definitions should be narrower in scope, so that it confines the offences to actual malicious activity. In particular, "unauthorised" should be separately defined, so that guidelines on identifying the appropriate authority for access, modification or impairment of data can be included in the provisions. The guidelines should state who can provide the authorisation and how the scope of authorisation is determined. A more comprehensive definition of unauthorised should provide greater clarity to the

evidential issue of how conduct is ”unauthorised”.

Secondly, both ss 477.2 and 477.3 should require knowledge and intent as the mental elements of the offences, not recklessness and knowledge. As discussed above, recklessness is too low a mental threshold for an offence that carries a 10-year prison term. The absence of recklessness or intent in s 477.3 is an even more serious omission, considering that you only need to ”know” that impairment is unauthorised.

Thirdly, an exception should be inserted for data that is used for legitimate research and business purposes. This can act as a counter-measure to the potential for prosecution under ss 478.3 and 478.4 in respect to IT professionals and researchers, who use programs that could be used to commit or facilitate the commission of Division 477 offences. This would be consistent with Article 6 of the CoE Convention, which incorporates safety provisions into its equivalent offences.

Finally, with respect to Paragraph 3LA, it should not be an automatic offence in the event of failure to provide assistance, especially where encryption keys are concerned. The law should provide indications as to how those served with assistance orders requiring encryption keys could successfully demonstrate that they cannot comply with the notice [2]. This would thus distinguish between those who are unable to provide assistance and those who are unwilling.

## CONCLUSION

Given the trend of poorly considered legislation presented before, and even passed by, various parliaments, it is obvious that more public consultation is needed to produce not only well-intentioned, but also appropriate legislation. It is likely that if the Australian Government sought the views of the IT industry during the development of the Act, the threats posed by this legislation may have been significantly mitigated.

Acts with failings like this have been passed before, and will undoubtably continue to be passed unless the Government works with more public feedback when creating or modifying technologically sensitive legislation. Only then can confidence be had in the Government’s ability to regulate technology issues.

That the Cybercrime Act was developed with the best intentions is not disputed. The crimes that the offences were intended to cover had not been considered in previous legislation. Despite these good intentions, the Act suffers from many significant ambiguities and unexplained omissions; a tremendous number of the Act’s details have been left to the courts to decide. Many of these have the worrying potential to cause unwarranted or excessive conviction for relatively minor or, in the worst case, unintentional offences. The Act also invests police with extensive investigative powers that were not requested nor identified as necessary until after the development of the Bill, yet nonetheless the Act lacks measures to prevent the abuse of the new powers.

The Cybercrime Act was not given sufficient consideration before its presentation to Parliament; the lack of public consultation, recent events online and off, and a deficiency of IT understanding by legislators have led to an inadequate Act being passed. In its present form, the Cybercrime Act 2001 presents a distinct and significant threat to individual Australian IT professsionals, which results in serious implications for the entire IT industry and community.

REFERENCES

[1] 2002 australian computer crime and security survey. Technical report, AusCert, Deloitte Touche Tohamtsu, and NSW State Police, May 2002.

[2] Electronic Frontiers Australia. Submission to senate legal and constitutional committee inquiry into the provisions of the cybercrime bill. 23 July 2001.

[3] M. Benanter. The internet public key infrastructure. Technical Report 3, IBM, 2001.

[4] Peter Flemming and Michael Stohl. Myths and realities of cyberterrorism. In *Proceedings of the International Conference on Countering Terrorism through ENhanced International Cooperation*, September 2000.

[5] Brian Greig. Cybercrime bill: A clumsy step in the right direction. *The Age*, 25 November 2002.

[6] Senate Legal and Constitutional Committee. Inquiry into the provisions of the cybercrime bill. *Parliament of the Commonwealth of Australia*, August 2001.

[7] Senate Legal and Constitutional Committee. Reference: Cybercrime bill 2001. In *Official Committee Hansard*, 19 July 2001.

[8] Senate Legal and Constitutional Committee. Reference: Cybercrime bill 2001. In *Official Committee Hansard*, 27 August 2001.

[9] Parliament of Australia. Cybercrime act. *Commonwealth of Australia*, 2001.

[10] State of Oregon. Computer crime law. *Oregon Revised Statutes*, 1993.

[11] Parliament of the United Kingdom of Westminster. Regulation of investigatory powers act. *United Kingdom*, 2000.

[12] Vir Phoha. The dmca needs fixing. *Communications of the ACM*, 44(12):33–34, December 2001.

[13] Richard Power. 2002 fbi/csi computer crime and security survey. Technical Report 1, Computer Security Issues and Trends, Spring 2002.

[14] Minister for Customs & Justice Senator Chris Ellison. Explanatory memos to amendments to the criminal code act. *Commonwealth of Australia*, 1995.

[15] Minister for Customs & Justice Senator Chris Ellison. Explanatory memo to the cybercrime act. *Commonwealth of Australia*, 2001.

[16] Alex Steel. Vaguely going where no-one has gone, the expansive new computeraccess offences. *Criminal Law Journal*, 26:72–97, April 2002.

[17] David Thompson and Desmond Berwick. Minimum provisions for the investigation of computer based offences. *129*, 1, 1998.