THE CYBERNETIC SEA: AUSTRALIA'S APPROACH TO THE WAVE OF CYBERCRIME

DANE BRYCE WEBER *

In today's age of ubiquitous internet access, cybercrime can be incredibly severe. This paper highlights the severity of cybercrime and critically examines Australia's response and history of cybercrime legislation. Through a study of Europe's approach compared to Australia's, the paper makes recommendations for improving Australia's response. The paper also addresses the future of Australian cybercrime law and how it can best be implemented with reference to European approaches and privacy concerns.

I INTRODUCTION

The internet has grown significantly since its inception in late 1969 as an implementation of packet-switching theory.[1] In 1991, the World Wide Web and HTML web pages were introduced and provided an easy to use graphical interface for the internet (though prior to 1991, ARPANet was widely used and, before that, the ITU X.25 packet-switching system was used for private and commercial purposes).[2] When considering the internet, it is worth noting this distinction: the World Wide Web merely exists on the internet. The analogy of the esplanade is fitting: the World Wide Web is a store using the street that is the internet.[3] Apart from the World Wide Web, various services exist on the internet, such as multitudinous peer-to-peer (P2P) protocols and even simple email.[4]

The internet has gone from being an early networking research project to what it is today - a global environment for instantaneous communication. It has become ubiquitous in modern life, from high-level government institutions to our pockets. Facebook alone has nearly one billion members sharing their personal information worldwide.[5] With this unprecedented access to the globe, it has been possible to share information like never before.

---

* LLM (IP&Tech) (QUT), GDLP(QUT), LLB (Hons) (USQ), Solicitor - Pioneer Legal Services

1 For a brief history of the internet see Barry Leiner et al, *Brief History of the Internet*, Internet Society <http://www.internetsociety.org/internet/internet-51/history-internet/brief-history-internet>.

2 Dan Ryan, *History of Computer Graphics: DLR Associates Series* (AuthorHouse, 2011) 366.

3 *The Difference Between the Internet and World Wide Web* (11 March 2014) Webopedia <http://www.webopedia.com/DidYouKnow/Internet/Web_vs_Internet.asp>.

4 Ibid.

5 Facebook, Inc, *Facebook, Inc – Registration Statement* (23 April 2012) United States Securities and Exchange Commission <http://www.sec.gov/Archives/edgar/data/1326801/000119312512175673/d287954ds1a.htm>.

DOI 10.5204/qutlr.v14i2.541

With such ubiquitous access, the internet has facilitated crimes with unprecedented efficiency and has spawned entirely new crimes. For example, in 2007, the Estonian Government moved a Soviet-era World War Two memorial, sparking protests in the nation's capital, Tallinn, and in the Estonian embassy in Moscow. Soon after, Estonian government websites were hit by distributed denial of service attacks ('*DDoS*'). The attacks took the websites offline by flooding the web servers with enough requests to overwhelm the nation's electronic infrastructure. This is the first time an entire nation's digital infrastructure has been taken offline, and one of the first times a government has directly fought back to protect the nation's security.[6]

In relation to infrastructure, in 2010, the 'Stuxnet' virus was discovered. It largely targeted Iranian nuclear enrichment facilities by sabotaging important equipment. It is the first known computer virus specifically designed to attack and shut down real world infrastructure, although it was possibly not transmitted electronically via a network, but physically through infected hardware such as a USB stick.[7]

In addition to sabotage by and against states, in December 2010, the online 'hacktivist' collective Anonymous initiated DDoS attacks against Visa and MasterCard. The attacks were designed to disrupt financial services by bringing down their websites in protest in support of whistleblowing website Wikileaks.[8] Espionage has also been cybercrime – in October 2012, newspaper *The New York Times* ran an investigative article on Chinese Prime Minister Wen Jiabao. From October 2012 to January 2013, the newspaper was subject to relentless hacking attempts, allegedly from Chinese hackers, which culminated in every corporate password for every employee being stolen.[9]

Although these are extreme examples of cybercrime, they show the potency of networking in the modern world. This potency allows traditional crimes to be committed in an entirely new environment and facilitates traditional crimes, much like the way the postal service facilitates illegal trafficking of drugs or roads facilitate traffic offences. It is helpful to remember the esplanade allusion: cybercrime may target both the stores and the esplanade itself, and as with physical crime, all-out assaults on infrastructure would be cyber-warfare. Cybercrime law then often overlaps greatly with telecommunications law.

The Australian Crime Commission provides some examples of traditional crimes becoming cybercrime, such as money laundering through online payment systems such as PayPal, child sex offences through child pornography websites, theft through identity crime such as stealing online bank account details or details from

---

6 Joshua Davis, 'Hackers Take Down the Most Wired Country in Europe' (2007) 15(9) *Wired* <http://www.wired.com/politics/security/magazine/15-09/ff_estonia>.

7 Jonathan Fildes, 'Stuxnet Virus Targets and Spread Revealed', *BBC News* (online), 15 February 2011 <http://www.bbc.com/news/technology-12465688>.

8 Simon Lauder et al, 'WikiLeaks Cyber War Heats Up', *ABC News* (online), 9 December 2010 <http://www.abc.net.au/news/2010-12-09/wikileaks-cyber-war-heats-up/2369076>.

9 Dara Kerr, 'Chinese Hackers said to Wage Cyberwar on The New York Times', *CNET* (online), 30 January 2013 <http://news.cnet.com/8301-1009_3-57566805-83/chinese-hackers-said-to-wage-cyberwar-on-the-new-york-times/>.

other websites, stalking, harassment and bullying through online messaging, and malicious damage through DDoS attacks and viruses.[10]

Security software company Symantec Corporation estimates that, in 2010, cybercrime cost 4.5 million Australians $4.6 billion in direct losses and the costs incurred by investigating and resolving crime. This is higher than the combined costs of burglary and assault.[11] The global estimate for losses due to cybercrime in 2010 was up to US$388 billion, and cyber-attacks on Australian business appear to be becoming more targeted and coordinated.[12]

Cybercrime has become an important issue due to the extremity of loss from it, efficiency of committing it, wealth of personal information available, and easy access to the internet. The younger generations view the internet and the real world as seamlessly integrated, with an estimated 10 billion devices connected to the internet as of 2013.[13] The issue of cybercrime will only grow in importance in Australia as the National Broadband Network is built, increasing internet access for all people across the nation. It is essential that Australia develops an effective response to cybercrime. The Australian Government has recognised cybersecurity as an integral component of Australia's national security strategy.[14] Recently, the Australian Government unveiled the Cyber Security Operations Centre[15] and released the Cyber Crime & Security Survey Report 2012[16] to better understand how cybercrime is affecting Australian business.

This paper aims to highlight the scope of cybercrime and address the effectiveness of Australia's legal response. European anti-cybercrime initiatives will be examined before contrasting Australian cybercrime law. The paper will show that Australia's response mostly follows that of Europe, and would be improved by further following European initiatives – though with reservations regarding

---

10 *Cyber Crime Fact Sheet* (April 2011) Australian Crime Commission <http://www.crimecommission.gov.au/publications/crime-profile-series-fact-sheet/cyber-crime>.

11 'Cybercrime Hits Aussies for $4.6B a Year – More Than Burglary, Assault Combined', *Sydney Morning Herald* (online), 8 September 2011 <http://www.smh.com.au/technology/security/cybercrime-hits-aussies-for-46b-a-year--more-than-burglary-assault-combined-20110908-1jyeo.html>.

12 Attorney-General's Department (Cth), 'Cyber Attacks on Australian Business More Targeted and Coordinated' (Media Release, 18 February 2013) <http://www.attorneygeneral.gov.au/Mediareleases/Pages/2013/First%20quarter/18February2013-CyberattacksonAustralianbusinessmoretargetedandcoordinated.aspx>.

13 *More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020* (9 May 2013) ABI Research <https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne>.

14 *Strong and Secure: A Strategy for Australia's National Security* (23 January 2013) Department of the Prime Minister and Cabinet <http://www.dpmc.gov.au/national_security/national-security-strategy.cfm>.

15 *CSOC – Cyber Security Operations Centre: ASD Australian Signals Directorate*, Department of Defence <http://www.asd.gov.au/infosec/csoc.htm>.

16 'Cyber Crime and Security Survey Report 2012' (Report, CERT Australia and Centre for Independent Study, 18 February 2013) <http://www.canberra.edu.au/cis/storage/Cyber%20Crime%20and%20Security%20Survey%20Report%202012.pdf>.

privacy. It will offer recommendations to address the few key areas of computer fraud, data retention and international cooperation.[17]

II WHAT IS CYBERCRIME?

Criminals have always taken advantage of new technology to commit crimes. Computers will always be vulnerable to people intent on exploiting the vulnerabilities: unless encryption keys are kept completely safe, even a computer in a locked vault cannot be guaranteed to be secure if it has networking capabilities. Although software, such as antiviruses and firewalls, can provide some protection against the vulnerabilities, education is also necessary to help people avoid situations which may compromise their online security. For this reason, the Commonwealth Department of Communications is implementing a comprehensive cyber-safety plan to educate Australians, young and old, on internet safety.[18]

Due to the pace computer technology improves, the law has to be frequently revised to address unforeseen developments. The Australian Crime Commission has identified three weaknesses that have led to the development of cybercrime: vulnerabilities in technology, inadequacy of legislation, and a lack of public awareness.[19]

Some of these weaknesses are addressed by CERT Australia[20] and AusCERT,[21] one of the world's oldest computer emergency response teams. They provide information and work with the Australian Security Intelligence Organisation ('*ASIO*'), Australian Federal Police and Australian Signals Directorate. If security software and the Australian Government's education policy are effective, the last bastion of deterrent and remedy against cybercrime is the law.

But what is cybercrime? Cybercrime can be classified into two categories: traditional crimes and new crimes exclusive to computers and the internet. Any traditional crime that uses communication over the internet can be considered cybercrime, such as using social networking sites, like Facebook, to harass or stalk, or committing fraud through scam emails. Traditional crime can also be committed in entirely new ways, such as fraud and money laundering through online banking and other payment services, like PayPal.

'Phishing' is another form of computer fraud.[22] Phishing involves sending emails claiming to be from, for example, a person's online banking or PayPal account, informing the user that something is 'wrong' with their account and they should rectify it. These seemingly genuine emails contain links to fake websites that steal

---

17 Given constraints, this paper will only address legal approaches. Non-legal approaches will only be touched upon and this paper will not delve into empirical research to determine the effect of laws on cybercrime.

18 *Online Safety and Security*, Department of Communications (Cth) <http://www.communications.gov.au/online_safety_and_security>.

19 Cyber Crime Fact Sheet, above n 10.

20 *CERT Australia*, Attorney-General's Department (Cth) <https://www.cert.gov.au/>.

21 *AusCERT* <https://www.auscert.org.au/>.

22 Jennifer Lynch, 'Identity Theft in Cyberspace: Crime Control Methods and their Effectiveness in Combating Phishing Attacks' (2005) 20 *Berkeley Technology Law Journal* 259.

personal details. Although existing laws can arguably extend, by analogy, to these new ways of committing traditional crimes, for true technological neutrality and applicability of the law, the existing laws require amendment to address the rapid change in technology and its usage.

There are also the new crimes that can be exclusively called cybercrime. Examples include DDoS attacks, computer viruses and data theft. Again, although these may be covered under law relating to analogous crimes, such as theft and property damage, legislation must address the new crimes specifically.

An important example of a traditional crime facilitated by the internet is identity theft. In the online world, it has exploded in comparison to what it once was. Although identity theft has been perpetrated for centuries,[23] the advent of social media, online shopping and online banking makes online privacy and identity theft a serious cybercrime threat in the online world.[24] It appears to be the fastest growing crime in the US.[25] Nowadays, identity theft can be easily committed and can wreak financial and personal ruin.

III THE EUROPEAN APPROACH

In considering whether Australian law effectively addresses cybercrime, it is desirable to compare it with another technologically sophisticated fora, such as Europe. The Council of Europe has drawn up the first international treaty specifically designed to address computer and internet crimes and to provide an international framework for cooperation between countries. This is the *Convention on Cybercrime.*[26] Although the Convention was drafted by the Council of Europe, non-member states have signed it. The Convention is already in force in the United States of America, Japan, the Dominican Republic and Australia.[27]

---

[23] Niloufer Selvadurai, Rizwanul Islam and Peter Gillies, 'Identity Theft: Aligning Law and Evolving Technologies' (2010) 34 *Criminal Law Journal* 33.

[24] 'Response to the Model Criminal Law Officers' Committee Discussion Paper - Chapter 3 – Identity Crime' (Response, Australian Federal Police, April 2007) <http://www.sclj.gov.au/agdbasev7wr/sclj/documents/pdf/mcloc_projects_identity_crime_submission_aust_federal_police.pdf>.

[25] Cassandra Cross, 'The Donald Mackay Churchill Fellowship to Study Methods for Preventing and Supporting Victims of Online Fraud' (Report, Winston Churchill Memorial Trust of Australia, 17 February 2012) 16.

[26] *Convention on Cybercrime*, opened for signature 23 November 2001, CETS No 185 (entered into force 1 July 2004). The Convention is supplemented by the *Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems*, opened for signature 28 January 2003, CETS No 189 (entered into force 1 March 2006). This Protocol criminalises dissemination of racist and xenophobic material and denial or approval of genocide or crimes against humanity over the internet. As this is not computer crime, the Protocol will not be discussed.

[27] *Convention on Cybercrime (Chart of Signatures, Ratifications and Entry into Force)* (18 June 2014) Council of Europe <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG>.

The principal Australian legislation on cybercrime - the *Cybercrime Act 2001* (Cth) ('*Cybercrime Act*') – is referrable to the Convention. The draft Convention was taken into account when the original *Cybercrime Act* was prepared and, as part of its accession to the Convention, Australia amended the *Cybercrime Act* to further consistency with the Convention (as discussed below). Accordingly, Australian law is readily comparable to the Convention.

A Law

The defining feature of the *Convention on Cybercrime* is that, as an international treaty, it aims to achieve harmonisation in the domestic law of each party and foster international cooperation.

The Convention (ch II s 1) requires all parties to it to enact legislation criminalising certain computer offences. These are illegal access and interception, data and system interference, misuse of devices, computer related forgery and fraud, offences related to child pornography, copyright infringement, and attempting, aiding or abetting. [28]

B Procedure

The Convention (ch II s 2) requires all parties to it to enact legislation adopting certain procedures. These relate to adequate protection for human rights, storage, disclosure and production of computer and internet traffic data, search and seizure of computer data, collecting internet traffic in real-time, and interception of content data.[29]

The Convention (ch III) specifically deals with international cooperation. It provides general principles for international cooperation and measures on extradition, mutual assistance, spontaneous information, mutual assistance without international agreement, confidentiality, storage, disclosure, mutual assistance and trans-border access for computer and internet traffic data, mutual assistance for real-time collection and interception of internet traffic data, and the provision of a 24/7 network.[30]

C Implementation

As data moves constantly through the internet near-instantaneously, information necessary to investigators can be difficult to track. Articles 16 and 17 of the Convention require enactment of laws for retention of computer and traffic data. The European Parliament and the Council of the European Union has provided some harmonised law on data retention for Europe – a 2006 directive on data retention (the '*Directive*').[31]

---

[28] *Convention on Cybercrime*, opened for signature 23 November 2001, CETS No 185 (entered into force 1 July 2004) arts 2-13.

[29] Ibid arts 14-21.

[30] Ibid arts 23-35.

[31] *Directive 2006/24/EC of 15 March 2006 on the Retention of Data Generated or Processed in Connection With the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC* [2006] OJ L 105/54.

Subject to human rights law, the Directive calls for all 'meta data'[32] relating to communications to be preserved for no less than six 6 months and no more than 24 months. This data is to be protected and secured from unlawful destruction, disclosure, storage, processing or accessing, and from accidental loss or alteration. The subject of meta data is controversial: what delineates meta data from content data? The Directive applies to details on senders and recipients - as an example, does a subject line in an email cross from being meta data to content data?[33]

The Directive has been the subject of great criticism. Numerous human rights groups have protested against it, including the Electronic Frontier Foundation[34] and European Digital Rights,[35] an organisation comprising 32 privacy and civil rights organisations. Member countries have also protested against the Directive. Sweden has argued that the Directive is unnecessary,[36] and has ultimately been ordered to pay penalties of €3 million for noncompliance.[37] Ireland has challenged the Directive and lost.[38] The Constitutional Courts of Germany,[39] Romania[40] and the Czech Republic[41] have annulled legislation transposing the Directive into their national laws. On 9 July 2013, the European Court of Justice held a hearing asking for proof of the necessity and efficiency of the Directive.[42]

IV THE AUSTRALIAN APPROACH – LAW

Much like the postal rule's application to email, the common law can apply existing law on offences to online offences by analogy. However, most cybercrime law in Australia is purely legislative. In Queensland, there are only two offences in the Criminal Code[43] that deal with the internet and computers: s 218A, using internet, etc to procure children under 16, and s 408E, computer hacking and misuse. As cybercrime is borderless, it is the Commonwealth that has enacted Australia's legislative regime to deal with it. The principle statute is

---

[32] Data *about* data, not actual content. Examples are the date of sending and receipt, details of the sender and recipient, etc.

[33] Renai LeMay, Turnbull has "Grave Misgivings" on Data Retention, Delimiter (9 October 2012) <http://delimiter.com.au/2012/10/09/turnbull-has-grave-misgivings-on-data-retention/>.

[34] Electronic Frontier Foundation (EFF) <https://www.eff.org/>.

[35] European Digital Rights (EDRi) <http://www.edri.org/>.

[36] Sweden Argues that Transposing Data Retention Directive Is Unnecessary (7 September 2011) EDRi <http://www.edri.org/edrigram/number9.17/sweden-contests-data-retention-unnecessary>.

[37] European Commission v Kingdom of Sweden (European Court of Justice, C-270/11, 30 May 2013).

[38] Ireland v European Parliament and Council of the European Union (C-301/06) [2009] ECR I-00593.

[39] European Commission, 'Data Retention: Commission Requests Germany and Romania Fully Transpose EU Rules' (Press Release, IP/11/1248, 27 October 2011) <http://europa.eu/newsroom/press-releases/databases/index_en.htm>.

[40] Ibid.

[41] Czech Constitutional Court Rejects Data Retention Legislation (6 April 2011) EDRi <http://www.edri.org/edrigram/number9.7/czech-data-retention-decision>.

[42] Monika Ermert, EU Data Retention Might Not be Proportional to Risks (9 July 2013) Internet Policy Review <http://policyreview.info/articles/news/eu-data-retention-might-not-be-proportional-risks/170>.

[43] Criminal Code Act 1899 (Qld) sch 1.

the *Cybercrime Act* as it has been amended from time to time (as discussed below).

A Original Commonwealth regime

Prior to the *Cybercrime Act*, the Commonwealth provisions on computer crime were in *Crimes Act 1914* (Cth) ('*Crimes Act*') (pt VIA). The *Crimes Act* provisions were based on the 1988 Gibbs Report[44] and were not substantially amended until the 2001 *Cybercrime Act*.[45] The *Cybercrime Act* amended six pieces of legislation, including the *Crimes Act* and Commonwealth Criminal Code ('the *Code*').[46]

The *Cybercrime Act* introduced computer offences. The offences were based on a report on computer offences released by the Model Criminal Code Officers Committee.[47] The report contained a model cybercrime bill, which was based on the United Kingdom's *Computer Misuse Act 1990* (UK). At the time of the UK legislation the Council of Europe had begun to draft the *Convention on Cybercrime*, so the UK legislation and Australian model cybercrime bill took the draft Convention into consideration.[48]

The *Cybercrime Act* took an 'interlocking regime' approach. That is, it added definitions relating to digital data to extend existing offences for traditional crimes to also apply when the crimes were committed over the internet. This followed the approach taken in the *Computer Misuse Act 1990* (UK).[49]

The *Cybercrime Act* provided a definition of 'data' for the purposes of the Code, *Crimes Act* and *Customs Act 1901* (Cth), to accommodate digital data, including its access. It also inserted s 476.1 into the Code, which provided definitions of 'electronic communication' and 'telecommunications services'. These were later amended by the *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No 2) 2004* (Cth). The amendment replaced 'telecommunications services' with 'carriage service' as defined in the *Telecommunications Act 1997* (Cth) as 'a service for carrying communications by means of guided and/or unguided electromagnetic energy'.

With these definitions, there was an interlocking regime to cover traditional crimes committed over the internet. Using a 'carriage service' included using the internet, and any offence which involved a carriage service would also include anything done on the internet.

B Recent developments

---

44 'Review of Commonwealth Criminal Law: Interim Report on Computer Crime' (Report, Attorney-General's Department (Cth), November 1988).

45 Information and Research Services (Cth), *Bills Digest*, No 48 of 2001–02, 10 September 2001.

46 *Criminal Code Act 1995* (Cth) sch.

47 'Report on Chapter 4 – Damage and Computer Offences and Amendment to Chapter 2: Jurisdiction' (Report, Model Criminal Code Officers Committee of the Standing Committee of Attorney's-General, January 2001).

48 Ibid 89.

49 Ibid.

On 22 August 2012, then Commonwealth Attorney-General, Nicola Roxon, announced that legislation was to be introduced to allow Australia to accede to and implement the *Convention on Cybercrime*.[50] The legislation to be introduced was the Cybercrime Legislation Amendment Bill 2011 (Cth).[51] This is now the *Cybercrime Legislation Amendment Act 2012* (Cth) ('*Cybercrime Amendment Act*'), and with Australia's accession to the *Convention on Cybercrime*, all provisions of the *Cybercrime Amendment Act* have come into force.[52]

The Cybercrime Amendment Act amends four pieces of legislation. The Telecommunications Act 1997 (Cth) ('Telecommunications Act'), Telecommunications (Interception and Access) Act 1979 (Cth) ('Interception Act'), Mutual Assistance in Criminal Matters Act 1987 (Cth) ('Mutual Assistance Act') and Criminal Code Act 1995 (Cth) are amended by schs 1 to 5 of the Cybercrime Amendment Act. The amendments relate to the preservation regime for stored communications, mutual assistance, computer offence amendment, telecommunications data confidentiality and other miscellaneous amendments.

C Current cybercrime offences

The *Cybercrime Amendment Act* introduced specific computer offences into the Code and amended other legislation to accommodate digital data.

The *Cybercrime Amendment Act* repealed *Crimes Act* pt VIA which previously dealt with computer offences, and replaced it with a new Code pt 10.7 entitled 'computer offences'. It also amended any legislation that referred to *Crimes Act* pt VIA to instead reference Code pt 10.7. Code pt 10.7 includes divs 476, 477 and 478: preliminary, serious computer offences and other computer offences. The offences under Code pt 10.7 include unauthorised access, modification or impairment with intent to commit a serious offence,[53] unauthorised modification of data to cause impairment,[54] unauthorised impairment of electronic communications,[55] unauthorised access to or modification of restricted data,[56] unauthorised impairment of data held on a computer disk or otherwise,[57] possession or control of data with intent to commit a computer offence,[58] and producing, supplying or obtaining data with intent to commit a computer offence.[59]

---

50 Attorney-General's Department (Cth), 'New Laws in the Fight Against Cyber Crime' (Media Release, 22 August 2012) <http://www.attorneygeneral.gov.au/Media-releases/Pages/2012/Third%20Quarter/22August2012-Newlawsinthefightagainstcybercrime.aspx>.

51 Law and Bills Digest Section (Cth), *Bills Digest*, No 31 of 2011, 18 August 2011.

52 Attorney-General's Department (Cth), 'Australia Signs on to International Cybercrime Treaty' (Media Release, 4 March 2013.

53 *Criminal Code Act 1995* (Cth) sch s 477.1.

54 Ibid s 477.2.

55 Ibid s 477.3.

56 Ibid s 478.1.

57 Ibid s 478.2.

58 Ibid s 478.3.

59 Ibid s 478.4.

The *Cybercrimes Amendment Act* similarly repealed *Crimes Act* pt VIIB, and replaced it (and all references to it) with a new Code pt 10.6. Code pt 10.6 (div 474) offences involve dishonesty with respect to carriage services, and interference with, and offences related to the use of, telecommunications. The offences under pt 10.6 relate to interception devices,[60] wrongful delivery of communications,[61] interfering with telecommunications device or account identifiers,[62] using a telecommunications network with intention to commit a serious offence,[63] threats[64] and hoax threats,[65] menacing, harassing or causing offence,[66] child pornography and child abuse material,[67] and procuring or grooming a child under 16 years of age.[68]

The *Cybercrime Amendment Act* also introduced ancillary offences. Although these do not create new computer offences, they protect the preservation and use of stored communications. These stored communications are subject to confidentiality. Under new ss 181A and 181B of the *Interception Act*, unauthorised use or disclosure of stored communications is an offence subject to two years' imprisonment. It is prudent to point out that 'stored communications' *only* relate to the communications that pass through the networks of carriage service providers, and it is only those communications which attract confidentiality. Any information collected by other entities, such as Facebook or Google, are not subject to confidentiality.

V THE AUSTRALIAN APPROACH – PROCEDURE

The Commonwealth cybercrime regime as originally introduced was an interlocking regime because, as described above, it added definitions to extend existing offences for traditional crimes to also apply when the crimes were committed over the internet. Another reason the *Cybercrime Act* was an interlocking regime was because of limits on Commonwealth constitutional power.

As Commonwealth legislation, the *Cybercrime Act* had to be constitutionally supported. For when a Commonwealth computer was not involved, the power relied upon was s 51(v) of the *Constitution* – 'postal, telegraphic, telephonic, and other like services'. The High Court in *Jones v Commonwealth*[69] had interpreted s 51(v) to include other forms of mass-communication, such as television and radio. The *Cybercrimes Act* relied on analogy to this High Court precedent to extend the s 51(v) head of power to the internet.[70] If the relevant activity was did not take place on a Commonwealth computer or a telecommunications network, then unless it was covered under another head of Commonwealth power, the

---

60 Ibid s 474.4.
61 Ibid s 474.5.
62 Ibid ss 474.7-474.12.
63 Ibid s 474.14.
64 Ibid s 474.15.
65 Ibid s 474.16.
66 Ibid s 474.17.
67 Ibid ss 474.19-474.24.
68 Ibid ss 474.26-474.29.s
69 1965) 112 CLR 206.
70 Information and Research Services (Cth), *Bills Digest*, No 13 of 2004–05, 2 August 2004.

Cybercrime Act did not apply.[71] Accordingly, the *Cybercrime Act* was devised to complement state law.

As an example of this interlocking regime, then Senator Chris Ellison explained that the Commonwealth regime would act against those taking photos and transmitting child pornography. If photos were taken with no transmission, the Commonwealth regime would not apply. However, state law would apply to the photos themselves.[72] This was recognised by the 'saving' provisions under Code ss 475.1(1) and 476.4(1). Under these sections, Commonwealth computer offences did not exclude or limit the operation of any other Commonwealth, state or territory law. This addressed any gaps in Commonwealth law by providing for the possibility of existing Commonwealth, state or territory criminal law to apply to cybercrime.[73] The only problem would arise if state or territory law did not cover the offences.

This possible gap in coverage has now been closed by the *Cybercrime Amendment Act*. As the *Cybercrime Amendment Act* implements an international treaty, the constitutionality of cybercrime offences will not need to rely on the offences being connected with a Commonwealth computer or entity or occurring over a carriage service. The head of power will shift from s 51(v) to the s 51(xxix) external affairs power.[74]

Consequently, *Cybercrime Amendment Act* sch 3 completely removes from Code divs 476, 477 and 478 any mention of offences being in connection with a Commonwealth computer or over a carriage service. The Commonwealth now has full jurisdiction over cybercrime offences committed in Australia without needing to support itself in reference to the telecommunications power. However, state legislation means offenders can be prosecuted in state courts under state law instead of relying on Federal courts.

This paper now discusses a number of detailed procedural points concerning the Commonwealth cybercrime regime.

A Evidentiary issues

Digital data, being as incorporeal and infinitely reproducible as it is, requires different procedures to obtain as evidence: it can be copied without actually removing it from a premises. The *Cybercrime Act* amended the *Crimes Act* by amending s 3L and inserting ss 3LA–3LB to address the nature of digital data. Sections 3L, 3LA and 3LB provide for obtaining a warrant to operate electronic equipment at a premises and to copy data or seize equipment, notice to occupiers of premises that this is happening, the destruction of data once unnecessary, and the requisition of expert assistance. These provisions have been judicially considered.

1 Copying data

---

71 Attorney-General's Department (Cth), above n 52.
72 Ibid; *The Age*, 28 July 2004, 4.
73 Such as the *Crimes Amendment (Computer Offences) Act 2001* (NSW).
74 C*ommonwealth v Tasmania* (1983) 158 CLR 1.

In *Kennedy v Baker*,[75] the copying of 'data' under *Crimes Act* s 3L(1A) was interpreted to allow copying of an entire computer hard drive. When considering the construction of s 3L(1A), Branson J considered the intention of the *Cybercrime Act* in amending the *Crimes Act*. 'Data' was taken to be a singular collective noun in this context, as details about the computer's operating system, meta data about files, and programs required to open files would be crucial. To not allow the copying of an entire hard drive would go against all good forensic techniques and only serve to *diminish* the powers of police to collect electronic evidence, contrary to the *Cybercrime Act*'s purposes.[76]

2 Seizure of data

In *Australian Securities and Investments Commission v Rich*,[77] 'seizure' of data was discussed. As the facts occurred before the *Cybercrime Act*'s amendments to the *Crimes Act*, the case references the now repealed ss 3L(2)(c) and 3F(5) of the *Crimes Act*. 'Seizure' was considered in three parts: seizure of electronic equipment, seizure of data when put in documentary form and seizure of data itself.

The first two definitions were considered to be settled, as these are physical objects that can literally be seized. Warrants authorised what would otherwise be considered trespass to goods.[78] However, seizure of data itself was a novel concept: to copy such data would be copyright infringement or breach of confidence, not trespass to goods. Given the *Crimes Act* authorised seizure of data, and in the absence of binding authority, the same rationale was applied: if warrants to seize property protect from trespass to goods, then warrants to seize data must protect from copyright infringement. As copyright infringement involves reproduction, seizure of data is effected when it is copied to a device (such as a CD) and is then removed, the copy taken into police custody.[79]

3 Synthesis of copying and seizure

Different Solutions Pty Ltd v Commissioner, Australian Federal Police (No 2)[80] brought the two previous cases together and solidified case law on data seizure. A distinction was drawn between 'copying' and 'imaging' a hard drive. Whereas 'copying' involves copying individual files and contents, 'imaging' a hard drive involves copying absolutely all data, in effect replicating an identical hard drive.

This amounts to forensic copying[81] which makes sorting through data practical. It is consistent with the decision in *Kennedy v Baker*[82] that 'data' is a singular

---

75 (2004) 135 FCR 520.
76 Ibid 535–54.
77 (2005) 188 FLR 416.
78 *Hart v Commissioner of Australian Federal Police* (2002) 124 FCR 384, 405 (French, Sackville and RD Nicholson JJ).
79 *ASIC v Rich* (2005) 188 FLR 416, 459–462 (Austin J).
80 (2008) 190 A Crim R 265.
81 Ibid 278 (Graham J).
82 (2004) 135 FCR 520.

collective noun.[83] Therefore, if evidentiary material can be found in a medium that contains other data, the medium itself could be seized - in this case, the imaged hard drive.

Despite these cases, however, the nature of technology may raise enough reasonable doubt to prevent prosecution of offences. Take for example if someone committed a crime on their home network with a 'burner' computer that was destroyed after the offence was committed. If their wireless network was unsecured, despite obtaining evidence that the offence was committed through that network, reasonable doubt could be raised as anyone could have accessed the wireless network. Short of a confession, it is incredibly hard evidentially to prosecute cybercrime, which explains the low number of cybercrime prosecutions in Australia.[84]

B Data retention

To properly implement the aims of the *Convention on Cybercrime*, the *Cybercrime Amendment Act* introduced in sch 1 a 'preservation regime for stored communications'. This amends the *Telecommunications Act* and *Interception Act*.

'Stored communications' refers to information *about* communications.[85] This can include subscriber information, telephone numbers and the date and time of a communication, among other information.[86] Unlike the European Directive, current Australian law does not provide for the retention of content data, such as phone conversations or email contents.

The main amendments made by the *Cybercrime Amendment Act* are to the *Interception Act*. The amendments reference the definitions in s 5 for 'enforcement agency', such as police forces, and 'organisation', meaning ASIO. *Interception Act* s 107G provides a succinct outline of preserving stored communications.

Interception Act s 107H provides for domestic preservation notices, requiring telecommunications carriers to preserve all stored communications for a period of time. The two notices that can be given are 'historic' and 'ongoing' domestic preservation notices. 'Historic' notices are in force for one day and 'ongoing' notices are in force for 30 days. The conditions for domestic preservation notices

---

[83] *Different Solutions Pty Ltd v Commissioner, Australian Federal Police (No 2)* (2008) 190 A Crim R 265, 286 (Graham J).

[84] Hannah Low, 'Hacking Masterminds are Hard to Prosecute', *Australian Financial Review* (online), 29 March 2012) <http://www.afr.com/p/business/marketing_media/hacking_masterminds_are_hard_to_qdGwyTeYwRLTiVY6EH27FK>.

[85] Nigel Brew, *Telecommunications Data Retention – An Overview* (24 October 2012) Parliamentary Library, Parliament of Australia <http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BN/2012-2013/DataRetention>.

[86] *Telecommunications (Interception and Access) Act 1979 Report for the Year Ending 30 June 2011* (2011) Attorney-General's Department (Cth) (2011), 10 <http://www.ag.gov.au/Publications/Pages/TelecommunicationsInterceptionandAccessAct1979AnnualReportfortheyearending30June2011.aspx>.

are contained in s 107J. Sub-sections (1)(b) and (1)(c) are crucial for an enforcement agency. If the agency is not investigating a serious contravention, and if there are no reasonable grounds to believe that stored communications might assist, the notice is mandatorily revoked under s 107L(2)(a). Similarly, for ASIO, if there are no reasonable grounds to believe that stored communications might assist in obtaining intelligence relating to security under s 107J(2)(b), the notice is mandatorily revoked under s 107L(2)(b). In either case, if no warrant is applied for, the notice will be revoked.

In light of the international context of the *Convention on Cybercrime*, there are also provisions in the *Interception Act* for foreign preservation notices. A foreign preservation notice can be given under s 107P(2) by the Australian Federal Police. A foreign preservation notice, like an historic domestic preservation notice, is in force for a single day.

C Mutual assistance

Interception Act s 107P(1) allows a foreign country to request the Australian Attorney-General arrange for access to stored communications relating to a criminal matter involving a serious foreign contravention. The foreign country can then request the Australian Federal Police to arrange for the foreign preservation for the stored communications. A request under s 107P(1) is made under *Mutual Assistance Act* s 15B (which was introduced by the *Cybercrime Amendment Act* sch 2).

Cybercrime Amendment Act sch 2 also introduced *Mutual Assistance Act* s 15D. It allows the Australian Attorney-General to assist foreign countries in their requests for telecommunications data in relation to a serious offence.

Cybercrime Amendment Act sch 2 further introduced *Interception Act* pt 4–1 div 4A, relating to foreign law enforcement and disclosure of information or documents. First, there is permitted 'primary disclosure'. *Interception Act* ss 180A and 180B provide that *Telecommunications Act* ss 276, 277 and 278 do not prevent disclosure to an authorised officer of the Australian Federal Police.[87] The authorised officer can then disclose to a foreign law enforcement agency, if satisfied it is reasonably necessary for the enforcement of the criminal law in their country.

Interception Act ss 180C and 180D provide for further 'secondary disclosure' to a foreign law enforcement agency, ASIO, an enforcement agency, the Australian Federal Police, or any other case if disclosure or use is appropriate in all the circumstances.

Interception Act s 180E provides conditions for disclosure to foreign countries. No information or document can be disclosed under ss 180A, 180B or 180C unless the information will only be used for the purposes for which the foreign country requested it, that any document containing the information will be

[87] Sections 276, 277 and 278 create offences for disclosure of certain information or documents, and are primary disclosure offences under *Telecommunications Act* pt 13 div 2. Likewise, *Interception Act* ss 180A and 180B are referred to as 'primary disclosure'.

destroyed when it is no longer required and, for disclosure under s 180B, on any other condition the Australian Attorney-General determines in writing.

Finally, *Interception Act* s 180F provides that privacy is to be considered before an authorised officer makes an authorisation under the above provisions. Any interference with privacy that may result must be justifiable. The officer must have regard to the likely relevance and usefulness of the information or documents and the reason why the disclosure or use concerned is proposed to be authorised.

Besides legislative provisions for mutual assistance, the Victorian case of *Director of Public Prosecutions v Sutcliffe*[88] has addressed the issue of jurisdiction and applicability of laws. In that case, the respondent had committed the offence of stalking under s 21A of the *Crimes Act 1958* (Vic). However, the victim of the stalking was located in Canada. Gillard J found that to limit the offence to all conduct taking place in Victoria would defeat the purpose of the legislation.[89] Therefore, s 21A was considered to have implicit extraterritorial operation. Although the victim in Canada could have complained to her local authorities, as the offender was amenable to Victorian jurisdiction, he was subsequently prosecuted in Victoria. It seems that Australian courts will be willing to prosecute people if their conduct offends Australian law, even if a victim may have a remedy in their own national courts.

VI AUSTRALIAN/EUROPEAN UNION COMPARISON

As noted above, because of the operation of the *Cybercrime Act* and *Cybercrime Amendment Act*, Australia's cybercrime regime is largely similar to the *Convention on Cybercrime*. In particular, the Code addresses Convention arts 2-7, 9 and 11 on substantive law,[90] the *Interception Act* and *Crimes Act* address arts 15, 17-19 and 21 on procedural law,[91] and the *Extradition Act 1988* (Cth), *Interception Act* and *Mutual Assistance Act* address arts 24, 28-31, 33 and 34 in relation to international cooperation.[92]

A Misuse of devices

Convention art 6 provides for the misuse of data *and devices*, yet s 478.4 of the Code only refers to *data*. This is just a consequence of the definition of 'data'. Although s 478.4 criminalises producing, supplying or obtaining data with an intention to commit an offence against div 477, sub-s (4)(b) provides for a *document* in which the data is stored to be included in the offence. Despite Australian law not using the word 'device', any device used to commit a

---

88 [2001] VSC 43.

89 Ibid [90]-[93].

90 *Criminal Code Act 1899* (Qld) sch 1 ss 474.4, 474.26-474.29, 477.1-477.3, 478.1-478.4.

91 *Telecommunications (Interception and Access) Act 1979* (Cth) ss 133, 180F, 181A, 181B, ch 3; *Crimes Act 1914* (Cth) ss 3L, 3LAA, 3LA, 3LB.

92 *Extradition Act 1988* (Cth); *Telecommunications (Interception and Access) Act 1979* (Cth) ss 107N-107S, 133, 180F, 181A, 181B, ch 3; *Mutual Assistance in Criminal Matters Act 1987* (Cth) ss 5EA, 15B, 15D, 142A.

computer crime must nonetheless contain data - otherwise, nothing would happen.[93]

B Copyright

Convention art 10 dealing with offences related to infringement of copyright and related rights is not specifically addressed by Australian cybercrime law. Article 10, however, also provides for parties to the Convention to fulfil their obligations under relevant copyright treaties. Australia has already done this under the *Copyright 1968* (Cth). Section 132AC criminalises commercial scale infringement, but does not make specific mention of infringement being done through computers. This is saved by 'articles' being defined in s 132AA as including any reproduction or copy of a work or other subject matter *in electronic form*.

C Computer fraud

Computer fraud is not merely about modifying data: it is also about deliberately and dishonestly defrauding people of their money, many of whom genuinely believe the requests are legitimate and willingly send money. These effects not only cost money, but often cost relationships and lives.[94] In most cases, such as scam emails and phishing, there is no data being modified at all.

Surprisingly, Convention art 8 dealing with computer related fraud is not specifically addressed by the *Cybercrime Act*. The only targeted offences of dishonesty and fraud in a digital context are under Code div 135 and s 474.2. However, div 135 is only in relation to Commonwealth entities and s 474.2 refers to dishonestly gaining from or causing loss to a *carriage service provider*.

Thus, computer fraud offences remain subject to the interlocking regime, and rely entirely on state and territory law. Unfortunately, the law is vastly inadequate in this regard. Although all states and territories have laws against simple unauthorised access to or modifying of data,[95] only the Northern Territory,[96] Queensland,[97] Tasmania[98] and Western Australia[99] specifically mention access or modification to gain a pecuniary benefit. Of those, Tasmania has the only true law specifically targeting computer related fraud. This is s 257B of its Criminal Code, 'computer-related fraud'.[100] Under sub-s (c), anyone who *otherwise* uses a computer with intend to defraud is guilty of a crime. This is the only Australian

---

93 Unless one considered using a sledgehammer to physically corrupt data, though that would be covered under offences to property.

94 For more information see Cross, above n 25.

95 *Criminal Code 2002* (ACT) pt 4.2; *Crimes Act 1900* (NSW) pt 6; *Criminal Code Act 2009* (NT) sch 1 pt VII div 10; *Criminal Code Act 1899* (Qld) sch 1 s 408E; *Criminal Law Consolidation Act 1935* (SA) pt 4A; *Criminal Code Act 1924* (Tas) sch 1 ch XXVIIIA; *Crimes Act 1958* (Vic) pt 1 div 3(6); *Criminal Code Act 1913* (WA) sch s 440A.

96 *Criminal Code Act 2009* (NT) sch 1 s 276B.

97 *Criminal Code Act 1899* (Qld) sch 1 s 408E.

98 *Criminal Code Act 1924* (Tas) sch 1 s 257B.

99 *Criminal Code Act 1913* (WA) sch s 440A(3).

100 *Criminal Code Act 1924* (Tas) sch 1.

law that directly targets computer related fraud in the many cases where victims believe the offenders are genuine.

This is a problem. Given the borderless nature of cybercrime, it is an oversight to not have a national approach to computer related fraud. The only saving Commonwealth grace is Code s 477.1, which makes it an offence to intend to commit a serious Commonwealth, state or territory offence by causing any unauthorised access, modification or impairment to data. 'Serious offence' is defined under Code s 473.1 to mean any offence punishable by imprisonment for five or more years or life. Although this covers non-Commonwealth law against fraud, it is limited to where access, modification or impairment to data is involved. It still does not cover the victims of online fraud.

As the basis of the new cybercrime offences are constitutionally supported under the external affairs power, there is no reason to not specifically address computer fraud in Commonwealth legislation. Computer fraud is otherwise only covered under normal laws against fraud or Code s 477.1 that still have an element of requiring access, modification or impairment to data, and do not cover the victims of online fraud.

D Procedure

The powers under *Crimes Act* ss 3L, 3LAA, 3LA and 3LB and the associated case law are consistent with the *Convention on Cybercrime* arts 14 and 15, requiring each party to adopt measures necessary to investigate and prosecute the relevant crimes. By the *Cybercrime Amendment Act*, Australia has also complied with most procedural provisions of the Convention.

E Storage and collection of computer and traffic data

The largest difference between Australian and European law is in the area of data retention. In Australia, there currently exists no provision for collection of content data. Information about communications can be collected by the issuing of a preservation notice under the *Interception Act*. However, these last either one day or up to 30 days. Whereas, under Convention art 16, collection or recording of traffic data is to be allowed for up to a maximum of *90* days.

Convention art 20 dealing with the real-time collection of traffic data is also only partly transposed. Once a preservation notice is in effect, this data is to be stored and preserved. This means that data can only be collected once a preservation notice is in force: there is no provision in Australian law for mandatory data retention, unlike the European Union's Directive calling for retention between six and 24 months.

F Mutual assistance

Although Australian law provides for mutual assistance, this assistance must be requested. Convention arts 26 and 32 require spontaneous information without prior request and access to stored computer data with consent without

authorisation. However, under *Interception Act* ss 180A to 180F, any foreign assistance must be authorised by an authorised officer of the Australian Federal Police or the Australian Attorney-General. In other words, the Australian provisions for mutual assistance will only have effect when specifically requested.

There is also no specific provision for a 24/7 network as required under Convention art 35. As any request for mutual assistance must pass through an authorised officer of the Australian Federal Police or the Australian Attorney-General, this limits the effectiveness of a purpose built 24/7 network. As it stands, such requests must necessarily pass through the Australian Federal Police or the Australian Attorney-General's Department without a dedicated 24/7 network.

VII CRITICISMS OF IMPLEMENTATION

Given the highly sensitive nature of intercepting communications, privacy concerns were at the forefront of criticisms levelled against the *Cybercrime Amendment Act* when it was introduced as a bill. For example, the specific implementation of mutual assistance was criticised by the Law Council of Australia for a lack of rigour in the proposed threshold tests, reporting obligations and privacy safeguards regarding access and disclosure.[101]

The main concern has been the issue of data retention. Concerns about Australia's *Cybercrime Amendment Act* have reflected the concerns about the European Union's Directive mandatory data collection and storage. Although it is indisputable that having access to communications data is invaluable in investigating and prosecuting cybercrime, it is the impact it will have on privacy and the security of data that it objected to.

Unlike the European Union's six to 24 months mandatory data collection and storage, data retention in Australia lasts for a maximum of 30 days. Under the Australian legislation, as explained by the Deputy Director of ASIO during the Joint Select Committee on Cyber-Safety Inquiry into Cybercrime, retention of data will only start when a preservation notice is ordered, data cannot be accessed until a warrant is obtained and the preservation can only begin when an intention to obtain a warrant has been formed.[102]

Australia's approach can be called a 'quick freeze' system, where data is retained only when there is a need to investigate. This system is argued by some in Germany to be the better option, as data can only be stored after a court order based on probable cause.[103] Unfortunately for Germany, this was considered to not transpose the Directive properly, and Germany is facing court action in the

---

[101] Law Council of Australia, Submission to Joint Select Committee on Cyber-Safety, *Inquiry into Cybercrime Legislation Amendment Bill 2011*, August 2011, 3.

[102] Evidence to Joint Select Committee on Cyber-Safety, Parliament of Australia, Canberra, 1 August 2011 (D Fricker).

[103] Jennifer Baker, *Germany Misses EU Data Retention Deadline, Could Face Court Action* (27 April 2012) PC World <http://www.pcworld.com/article/254614/germany_misses_eu_data_retention_deadline_could_face_court_action.html>.

European Court.[104] Australian police have argued for indefinite data retention.[105] Also, although Australia's approach only permit's retain of meta data, the Australian Securities and Investments Commission is looking to also retain *content* data.[106]

Despite Australia's currently less invasive approach to data retention, privacy is still a concern. Although s *Interception Act* 180F requires authorised officers to consider privacy, and art 15 of the Convention requires human rights to be taken into account, this has been argued to be an insufficient safeguard.[107] It was acknowledged by the Law Council of Australia that the privacy protections offered by s 180F are a 'move in the right direction' compared to those under the now repealed s 180F(5).[108] However, the Council still expressed concern that the authorised officer is to only have 'regard to' privacy concerns before making a decision. The Council instead offered the following formulation:

> Before making an authorisation, an authorised officer must be satisfied on reasonable grounds that the likely benefit to the investigation which would result from the disclosure substantially outweighs the extent to which the disclosure is likely to interfere with the privacy of any person or persons.[109]

The Law Council of Australia,[110] Electronic Frontiers Australia,[111] the Queensland Council for Civil Liberties,[112] the Commonwealth Ombudsman,[113] the Australian Privacy Foundation,[114] and the Cyberspace Law and Policy Centre[115] have all raised privacy and transparency concerns.

It will also be more costly.[116] This is no paltry concern. Of Google's US$37.9 billion revenue in 2011, 96% was from advertising.[117] Google's business model

---

[104] European Commission, 'Data Retention: Commission Takes Germany to Court Requesting that Fines be Imposed' (Press Release, IP/12/530, 31 May 2012) <http://europa.eu/newsroom/press-releases/databases/index_en.htm>.

[105] Renai LeMay, *Police Want "Indefinite" Data Retention* (27 September 2012) Delimiter <http://delimiter.com.au/2012/09/27/police-want-indefinite-data-retention/>.

[106] Renai LeMay, *Not Just Metadata: ASIC Wants Content Retained* (27 September 2012) Delimiter <http://delimiter.com.au/2012/09/27/not-just-metadata-asic-wants-content-retained/>.

[107] Bills Digest No 31, above n 51.

[108] Law Council of Australia, above n 101, 10.

[109] Ibid.

[110] Ibid.

[111] Electronic Frontiers Australia, Submission to Joint Select Committee on Cyber-Safety, *Inquiry into Cybercrime Legislation Amendment Bill 2011*, August 2011.

[112] Queensland Council for Civil Liberties, Submission to Joint Select Committee on Cyber-Safety, *Inquiry into Cybercrime Legislation Amendment Bill 2011*, August 2011.

[113] Commonwealth Ombudsman, Submission to Joint Select Committee on Cyber-Safety, *Inquiry into Cybercrime Legislation Amendment Bill 2011*, August 2011, 4.

[114] Australian Privacy Foundation, Submission to Joint Select Committee on Cyber-Safety, *Inquiry into Cybercrime Legislation Amendment Bill 2011*, August 2011.

[115] Cyberspace Law and Policy Centre, Submission to Joint Select Committee on Cyber-Safety, *Inquiry into Cybercrime Legislation Amendment Bill 2011*, August 2011, 3.

[116] Simon Cullen, 'Policing Privacy More Costly under Data Storage Plans' *ABC News* (online), 20 September 2012 <http://www.abc.net.au/news/2012-09-20/data-retention-changes-to-cost-more/4271898>.

[117] Meghan Kelly, *96 Percent of Google's Revenue is Advertising, Who Buys It?* (29 January 2012) VentureBeat <http://venturebeat.com/2012/01/29/google-advertising/>.

is built on collecting information, using it to profile internet users and targeting ads specifically tailored to the profile.[118] Through social media, web habits and a computer's IP address, a user's physical location, behaviour and personal information can be compiled.

The security of this data is incredibly important. Although safeguards are provided in the *Cybercrime Amendment Act*, they are merely a deterrent. There is no remedy against improper use of data. Digital data by its nature is infinitely reproducible, and once it is leaked it can never be returned,[119] as demonstrated by the theft and publication of thousands of AAPT customer records.[120] As Malcolm Turnbull has vividly portrayed, '[w]hatever privacy policies the Dutch Government may have had to protect against misuse of their database, the Nazi occupiers would have paid them no heed'.[121] This is exemplified by the existence of whistleblowing website Wikileaks, publishing leaked government information. Of particular Australian concern is the leak of the Australian Communications and Media Authority's secret internet censorship blacklist.[122]

There has already been a leak of secret government information: there is no guarantee that it cannot happen again. Indeed, the United States National Security Agency (NSA) has had former-contractor-turned-whistle-blower Edward Snowden leak documents which reveal the extent to which the NSA conducts surveillance on United States internet traffic and its effect on foreign traffic.[123]

The best prevention against data disclosure is proactively reducing one's 'digital footprint' from the outset, and this ironically thwarts the data retention scheme. Meta data and other communications can be concealed, such as by using 'proxy' servers to obscure location data or using Tor,[124] a network of virtual tunnels to protect users' anonymity. This hinders both the gathering of confidential stored communications and general activity by entities such as Facebook or Google.

VIII CONCLUSION

---

[118] Computer Weekly, *Google to Profile Web Use for Targeted Advertising* (12 March 2009) <http://www.computerweekly.com/news/2240088722/Google-to-profile-web-use-for-targeted-advertising>.

[119] Referred to as the 'Streisand Effect'. Barbara Streisand attempted to prevent photos of her house being spread online. People heard of information being suppressed on the internet and spread the photos globally.

[120] Andrew Colley and Chris Griffith, 'Anonymous Hackers Dump Stolen Data Belonging to Australian Telco AAPT', *The Australian* (online), 29 July 2012 <http://www.theaustralian.com.au/australian-it/telecommunications/anonymous-hackers-dump-stolen-data-belonging-to-australian-firm-aapt/story-fn4iyzsr-1226437681976>.

Malcolm Turnbull, 'Free At Last! Or Freedom Lost? Liberty in the Digital Age' (Speech delivered at the Alfred Deakin Lecture, University of Melbourne, 8 October 2012) <http://www.malcolmturnbull.com.au/media/speeches/free-at-last-or-freedom-lost-liberty-in-the-digital-age-2012-alfred-deakin-lecture/>.

[122] *Australian Government Secret ACMA Internet Censorship Blacklist* (18 March 2009) Wikileaks <http://wikileaks.org/wiki/Category:Australia>.

[123] 'NSA Surveillance Covers 75 Per Cent of US Internet Traffic', *ABC News* (online), 21 August 2013 <http://www.abc.net.au/news/2013-08-21/nsa-surveillance-covers-75-per-cent-of-us-internet-traffic/4902444>.

[124] Tor Project: Anonymity Online <https://www.torproject.org/>.

Australia is already running online safety education campaigns[125] and already has agencies dedicated to responding to cybercrime.[126] Australia's response to cybercrime can be legally improved in two key areas. The areas are mutual assistance and computer fraud. Although Australia is now party to the *Cybercrime Convention*, these areas can be improved by implementing legislation to better incorporate the Convention's aims.

In relation to mutual assistance, Australia is lacking a formal 24/7 network to facilitate international cooperation and is not forthcoming with volunteering information. Information disclosure must be authorised by an authorised officer of the Australian Federal Police or the Australian Attorney-General. As such, no information can be volunteered. Other countries must request information first. Given the importance of international cooperation - profoundly demonstrated during the Estonian cyberwar[127] - the lessons of the past should be heeded to facilitate efficient cooperation.

Secondly, Australia would be best served by enacting legislation specifically targeted at computer related fraud. As Australia has acceded to the *Convention on Cybercrime*, the Commonwealth has the power to deal with cybercrime under the external affairs power of the *Constitution*. Commonwealth legislation would be best placed to harmonise national law, and as a consequence, international cooperation would be made simpler.

To fully address computer related fraud under the Convention, Australia need only look in its own backyard - s 257B(c) of the Criminal Code in Tasmania.[128] As this applies to anyone intending to defraud who *otherwise uses a computer*, similar Commonwealth law would be able to *effectively* criminalise defrauding people online without having to require access, modification or impairment to data. Given the high economic and social costs associated with online fraud and phishing, Australia will benefit from having a targeted approach to these offences.

Data retention is one final issue that is a current hot topic. Australia currently has a 'quick-freeze' system in relation to meta data. This compares to the European Directive that imposes a mandatory system of retention of content data and retention of data for a period of time between six and 24 months. Although the Australian approach is less invasive, the privacy concerns are still phenomenal. This is because of how easily information from governments has been leaked and because, if data is leaked, there is potential for millions of Australians' personal information to be released worldwide and never able to be retrieved. The poignancy of this realisation only intensifies the need for the Australian Attorney-General's consultation to develop a stronger data retention plan. Yet, there has

---

[125] Online Safety and Security, above n 18; *Stay Smart Online*, Stay Smart Online <http://www.staysmartonline.gov.au/>. See also *Cybercrime – Protect Yourself Online*, Department of Justice (Vic) <http://www.justice.vic.gov.au/home/safer+communities/crime+prevention/cybercrime>.

[126] CERT Australia, above n 20.

[127] Erin Dian Debaucher, Lessons From Estonia: Preparing for a Major Cyberattacks (6 July 2011) Nextgov <http://www.nextgov.com/cybersecurity/2011/07/lessons-from-estonia-preparing-for-a-major-cyberattack/49352/>.

[128] Criminal Code Act 1924 (Tas) sch 1.

been 90 percent censorship of the plan in response to a freedom of information request.[129]

The world, especially Australia, is becoming increasingly interconnected through technology in every facet of our lives. As such, Australia must effectively address all legal avenues to combat cybercrime before the waves engulf Australian individuals, business and government.

[129] Ben Grubb, 'No Minister: 90% of Web Snoop Document Censored to Stop 'Premature Unnecessary Debate', Sydney Morning Herald (online), 23 July 2010 <http://www.smh.com.au/technology/technology-news/no-minister-90-of-web-snoop-document-censored-to-stop--premature-unnecessary-debate-20100722-10mxo.html>.