University of South Australia

The Library
www.library.unisa.edu.au

Educating Professionals, Creating and Applying Knowledge, Engaging our Communities

NOTICE: This is the author's version of a work that was accepted for publication in *Computer law and security report*. Changes resulting from the publishing process, such as peer review, editing, corrections, structural formatting, and other quality control mechanisms may not be reflected in this document. Changes may have been made to this work since it was submitted for publication. A definitive version was subsequently published in *Computer law and security report*, vol. 29, no. 2, pp. 152-163, http://dx.doi.org/10.1016/j.clsr.2013.01.006

Cloud computing and its implications for cybercrime investigations in Australia

Christopher Hooper
Faculty of Law, Monash University, Victoria.

Ben Martini and Kim-Kwang Raymond Choo**
Information Assurance Research Group, Advanced Computing Research Centre, University of South Australia

The advent of cloud computing has led to a dispersal of user data across international borders. More than ever before, law enforcement investigations into cybercrime and online criminal activity require cooperation between agencies from multiple countries. This paper examines recent changes to the law in Australia in relation to the power of law enforcement agencies to effectively investigate cybercrime insofar as individuals and organisations make use of cloud infrastructure in connection with criminal activity. It concludes that effective law enforcement operations in this area require harmonious laws across jurisdictions and streamlines procedures for granting assistance between law enforcement agencies. In conjunction with these mechanical developments, this paper posits that law enforcement officers require a systematised understanding of cloud infrastructure and its operation in order to effectively make use of their powers.

Key Words
Cloud computing
Cybercrime
Digital forensics
Law enforcement investigations
Mutual legal assistance
Australian Law
Council of Europe Convention on Cybercrime
Jurisdictional issues

1. Introduction

On 22 August 2012 the Federal Government's *Cybercrime (Legislative Amendment) Bill 2011* passed the Senate after being referred to the Parliament Joint Committee on Cyber Safety in 2011. The Bill purports to allow Australia to accede to the Council of Europe Convention on Cybercrime and recognises the need for governments and law enforcement agencies ("LEAs") to continuously update and improve the investigatory and legal tools available to them in order to effectively police new and changing forms of criminal activity. [1]

One of these new frontiers is the advent of cloud computing, which allows users to utilise off-site (often in a foreign jurisdiction from an Australian law enforcement perspective) computing infrastructure as a platform for running networked applications, storing data and conducing other similar activities. Criminals who utilise information communications

** Corresponding author (Raymond.Choo@unisa.edu.au). This is the pre-print of the authors' version and citation should be "Hooper C, Martini B and Choo K-K R 2013. Cloud computing and its implications for cybercrime investigations in Australia. *Computer Law and Security Review* 29(2): 152–163".
[1] Explanatory Memorandum, Cybercrime (Legislative Amendment) Bill 2011 (Cth).1.

technologies ("ICT") have always operated on a transnational basis but through cloud computing, criminal investigations have taken on a new degree of internationalism. However, jurisdictional differences in substantive and criminal law may hinder police efforts to hold perpetrators to account for online criminal activity. This has implications both at a national and an international level in relation to the regulation of the internet and the ability to access data for investigative purposes.[2]

It is submitted that, to some extent, a number of these jurisdictional complications may be solved by greater international cooperation both in relation to mutual legal assistance and greater harmonisation of substantive and procedural laws in relation to cybercrime. This is a stated goal of the Council of Europe's *Convention on Cybercrime* ("the Convention").[3]

This paper seeks to interrogate the extent to which Australia's accession to the Convention will enable LEAs to better investigate criminal activity insofar as it occurs on, makes use of or targets cloud services. A key area of investigation will be whether the new laws under the *Cybercrime (Legislative Amendment) Bill 2011* are likely to give LEAs better access to the data requires for effective investigations into online criminal activity.

2. Cybercrime: The Scope and Effect of the Problem

ICT, such as personal computers, laptops, smart-phones and tablets, are fundamental to modern society and open the door to increased productivity, faster communication capabilities, and immeasurable convenience. However, it also changes the way criminals conduct their activities, and vulnerabilities in our ICT infrastructure are fertile grounds for criminal exploitation. Few today would challenge the assertion that the era of globalisation has been accompanied by an increase in the sophistication and volume of malicious cyber activities. Cyberspace can be used as an extension to facilitate and enhance traditional forms of crime as well as create new forms of crime. In this paper, the use of ICT as a tool for the commission of a crime or as the object of a crime[4] will be referred to as "cybercrime" for the purposes of linguistic simplicity. The term is referred to in the *Cybercrime Act 2001* (Cth) as well as the Council of Europe Convention on Cybercrime with different meanings.[5] Commonly, it is understood by reference to the types of conduct to which it applies; these include offences under Part 10.7 of the *Criminal Code Act 1995* (Cth) and conduct such as online fraud, cyber-bullying and using the internet to view or store child exploitation material or for the purposes of child grooming.

While the advent of ICT has allowed for the emergence of new types of criminal behaviour such as the use of malware (malicious software such as Trojan horses, viruses and worms), there is a growing consensus that existing laws in relation to areas such as theft, forgery and malicious damage to property are generally capable of suitable modification so as to adequately handle many of the situations envisaged by more specific laws directly targeting

[2] Victoria Baines, 'Online Child Sexual Abuse: the Law Enforcement Response' (Paper Presented at the World Congress III against Sexual Exploitation of Children and Adolescents, Rio de Janeiro, Brazil, 25–8 November 2008).10.

[3] *Convention on Cybercrime*, opened for signature 23 November 2011, ETS 185 (entered into force 1 July 2004) Preamble para 3.

[4] Tony Krone, *Concepts and Terms*: High-Tech Crime Brief. No. 1 (2005); Kim-Kwang Raymond Choo, Russell Smith and Rob McCusker, 'Future Directions in Technology-Enabled Crime: 2007-09' (Research and public policy series No 78, Australian Institute of Criminology, 2007).

[5] Ibid.

such behaviour.[6] Indeed, it is possible to argue that cybercrime is best thought of as 'the exploitation of a new technology to commit an old crime in new ways and…to engage in a limited variety of new types of criminal activity'.[7]

Nevertheless, there is no doubt that that use of malware for the facilitation of crimes such as internet banking and credit card fraud, identity theft and money laundering has increased markedly in recent years.[8] The same is true of the use of the internet by paedophiles in connection with online child exploitation activities such as online child grooming and dissemination of child abuse and exploitative material.[9]

A recent report by the Australian Crime Commission ("ACC") found that in the last five years, Australians have lost over AUD 113 million to serious organised crime investment fraud. That is, the use of deceptive mechanisms including cold calling, fake websites and false recovery services ("phishing") to convince individuals to part with their money or personal information on bogus investment opportunities.[10] Furthermore, in 2011, a report prepared by Norton-Symantec[11] showed that cybercrime cost the Australian economy just over USD 4.5 billion in 2010. USD 1.8 billion of this sum was directly or indirectly misappropriated while the remaining sum was accounted for by resultant increases in productivity costs associated with fixing the problems raised by cybercrime.[12] The same report identified a cost of USD 32 billion to the United States economy and USD 25 billion in direct losses to China.[13] It showed that 69% of surveyed adults who used online services have been victims of cybercrime.[14]

The vast majority of reports on patterns and trends in cybercrime disseminated (and in turn cited) are from the commercial sector and do not include details such as the research methodology or provide access to the raw data.[15] Guinchard[16] explained that the 'diversity of methods used to collect information on cyber incidents can produce widely different results ... [and] this facilitates extrapolations about the scale of the problem and the cost of cyber crimes'. For example, there have been assertions that cybercrime has '[s]urpassed Illegal Drug Trafficking as a Criminal Moneymaker.'[17] and a more recent report by Detica[18]

---

[6] Susan Brenner, 'Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law' (2001) 8(2) *Murdoch University Electronic Journal of Law* <http://www.murdoch.edu.au/elaw/issues/v8n2/brenner82.html>.

[7] Ibid.

[8] See. eg. *Home Users Computer Security Survey 2008,* Australian National Computer Emergency Response Team (AusCERT) <www.auscert.org.au>; Australian Payments Clearing Association. *Fraud Statistics 2011 Financial Year*; Australian Payments Clearing Association. *Fraud Statistics 2010 Financial Year*; Australian Payments Clearing Association. *Fraud Statistics 2009 Financial Year*.

[9] Kim-Kwang Raymond Choo. 'Responding to Online Child Sexual Grooming: An Industry Perspective' (Trends & Issues in Crime and Criminal Justice No. 379, Australian Institute of Criminology, 2009).

[10] Australian Crime Commission. *Serious and Organised Investment Fraud in Australia* (2012).

[11] Norton-Symnatec, *Cybercrime Report: The Human Impact.* (2011) <http://us.norton.com/cybercrimereport/promo?inid=us_hho_downloads_home_link_cybercrimereport>.

[12] ABC Radio National, 'Cybercrime cost Australia over $4.5 billion last year', *AM,* 8 September 2011 (Alison Caldwell) < http://www.abc.net.au/am/content/2011/s3312727.htm >.

[13] Norton-Symnatec*,* above n 11.

[14] Ibid.

[15] See. Patrick Gray, 'Exposing Norton's Cybercrime Scare Campaign', *The Age* (online) 21 September 2011 <http://www.theage.com.au/it-pro/security-it/exposing-nortons-cybercrime-scare-campaign-20110921-1kkip.html>.

[16] Audrey Guinchard, 'Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy' (2011) IV(2) *Journal of Strategic Security* 75, 78

[17] Symantec, 'Cyber Crime has Surpassed Illegal Drug Trafficking as a Criminal Moneymaker; 1 in 5 will become a Victim' (Press Release, No 10, September 2009) .

commissioned by the UK cabinet office estimated 'the cost of cyber crime to the UK to be £27bn per annum'. However, such figures have been criticised in both the media[19] and by academics[20] The currency of cybercrime as a term among members of the community means that it may be imprecisely applied to a wide range of criminal behaviour with the consequence that the scope of the problem is apt for overstatement; although this is not to suggest that the problem is not widespread.[21]

Despite the size and gravity of the problem however, individuals to a certain extent[22], and business in most cases, do not report many instances of cybercrime when they are affected. In 2009 on average only 8% of Australian businesses (surveyed in the Australian Business Assessment of Computer User Security) who had been the victim of cybercrime reported it to the police. In many cases this was because the crime was not considered serious enough.[23]

3. Cloud Technology: Advent and Definition

The opportunities for criminality outlined above have recently found new expression in the advent of "cloud computing", which provides "scalability" by allowing users to access infrastructure, software, data storage and applications on-demand, saving on the costs of acquiring these capabilities themselves.[24] This technology has been the subject of various definitional attempts prior to arriving at what is now the commonly accepted definition from the National Institute of Standards and Technology ("NIST") in the United States[25]:

> Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (eg. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud environments have certain features noted in the above NIST cloud computing definition which will be explained here briefly in order to better frame the discussion which follows. One of the key features of cloud computing is the capability to scale the available resources on an on-demand basis. In practice this generally means that a customer can purchase resources (e.g. processing, memory, storage, network bandwidth) online in an ad-hoc manner to provision services which may be, for example, an operating system and

---

[18] 'The Cost of Cyber Crime: A Detica report in partnership with the Office of Cyber Security and Information Assurance in the cabinet office' (Research Report, Detica Ltd, 2011) 2.
[19] Gray, above n 15.
[20] Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michael van Eeten, Michael Levi, Tyler Moore & Stefan Savage, 'Measuring the Cost of Cybercrime' (Paper presented at the 11th Workshop on Economics of Information Security (WEIS 2012), Berlin Brandenburg Academy of Sciences, Berlin, Germany, June 25–26 2012); Dinei Florencio & Cormac Herley, 'Sex, Lies and Cybercrime Surveys' (Paper presented at the Tenth Workshop on Economics of Information Security (WEIS 2011), George Mason University, USA, June 14–15 2011).
[21] See. Norton-Symantec, *Cybercrime Report: The Human Impact*. (2011) <http://us.norton.com/cybercrimereport/promo?inid=us_hho_downloads_home_link_cybercrimereport>.
[22] Norton-Symnatec, above n 11..
[23] Kelly Richards, 'The Australian Business Assessment of Computer User Security: A National Survey' (Research Report No 102, Australian Institute of Criminology, 2009) xii.
[24] Mark Vincent & Nick Hart, 'Law in the Cloud' (2011) 49(5) *Law Society Journal* 50, 51.
[25] Lee Barger, Tim Grace, Robert Patt-Corner & Jeff Voas. *Cloud Computing Synopsis and Recommendations: Recommendations of the National Institute of Standards and Technology*. (Special Publication No 800-146, National Institute of Standards and Technology: United States Department of Commerce, May 2011) 2-1; see also 'Cloud Computing Strategic Discussion Paper: Opportunities and Applicability for Use by the Australian Government' (Strategic Direction Paper, Version 1.0, Department of Finance and Deregulation, Australian Government, April 2011) 10.

services (such as a webserver) or instances in a software environment (such as mailbox instances). As demand increases (e.g. an increase in staff requiring the provision of mailboxes or a burst of customer demand on a webserver) the customer can provision an increase in resources in a close to real-time manner.

Another key component of cloud computing is its "multi-tenancy" capability[26] which is referred to as a "shared pool of resources" in the NIST definition. This refers to the ability of cloud services to support use of the same resources or applications by multiple users. In an IaaS model, server virtualisation allows several virtual machines to run their own operating system within a single physical machine/server, which helps to facilitate multi-tenancy.[27] It also facilities the cost effective provisioning of scalable resources for the use of cloud customers. Multi-tenancy generally occurs as part of both compute operations (active processing of computing requests using processing, memory and network resources) via virtual machines but also as part of storage operations where data will be stored on shared disks. Under certain circumstances individual files from individual customers may be distributed across multiple disks and storage systems across multiple jurisdictions if a cloud service provider has facilities in more than one country. This is a particularly important point for the preservation and collection of electronic evidence.

The servers located in the cloud will commonly be owned by a company or entity (the cloud service provider) that will enter into a contract (service level agreement) with the client. The service level agreement ("SLA") sets out the obligations of the parties and may allow for contingencies in the event of a digital forensic investigation. These matters include a definition of the applicable jurisdiction and laws that apply to the cloud service provider ("CSP") and the client. The SLA may also touch on data seizure procedures and how this would affect the integrity of the user's data, privacy and service delivery or continuity of the users' data.[28] Finally, the SLA can deal with issues such as intellectual property rights in relation to data stored on the cloud. Some agreements provide that the CSP obtains an interest in such material. This makes the area rather multi-disciplinary in nature[29] and raises issues in terms of data protection and the CSP's obligation to safeguard the intellectual property rights of its clients.[30]

In addition to these environmental characteristics, cloud technology is commonly understood as existing in a number of different deployment models ranging from open access *public clouds* and *community clouds*, to *private clouds* which service a specific organisation. There is also the potential for *hybrid clouds* which combine one or more of the above models.[31] In many cases the cloud deployment model changes the methodology for collection and preservation of electronic evidence. For example, the public cloud model may result in data of potential evidential value being stored outside of the physical jurisdiction of the LEA

[26] 'Security Guidance for Critical Areas of Focus in Cloud Computing' (Version 3.1, Cloud Security Alliance, 2011) 14.
[27] Kim-Kwang Raymond Choo, 'Cloud Computing: Challenges and Future Directions' (Trends & Issues in Crime and Criminal Justice No 400, Australian Institute of Criminology, 2010) 2.
[28] Denis Reilly, Chris Wren & Tom Berry. 'Cloud Computing: Pros and cons for computer forensic Investigation' (2011) 1(1) *International Journal Multimedia and Image Processing* 26, 27, 39, 40; Vincent above n 24, 52.
[29] Horacio Gutiérrez, 'Peering Through the Cloud: The Future of Intellectual Property and Computing' (2011) 20(4) *The Federal Circuit Bar Journal* 590, 590–1, 601,602–7.
[30] Stephanie Overby, 'Keeping Secrets in the Cloud: How to Protect Your Intellectual Property in the Cloud'. [2012] *CIO Magazine* <http://www.cio.com/article/699494/How_to_Protect_Your_Intellectual_Property_in_the_Cloud >.
[31] Cloud Security Alliance, above n 26, 25.

which complicates traditional methods of preservation and collection. The hybrid cloud model may result in some data being physically stored in a public cloud and with other data stored in a private cloud which may also complicate identification of electronic evidence.

A CSP may offer any one of a number of services to clients, allowing them to interact with the cloud environment in a variety of ways. These include the following widely-accepted descriptions:

- *Cloud Infrastructure as a Service (IaaS):* This provides clients with access to storage space, bandwidth and other fundamental computing services. It effectively expands the computing capability of the customer, allowing them to run their own software and applications using the cloud infrastructure;
- *Cloud Platform as a Service (PaaS):* Allows the customer to gain access to the computer platform or operating systems of the cloud instances (eg. Windows and Linux) and an underlying database so that they can create or acquire applications; and
- *Cloud Software as a Service (SaaS):* This allows clients of the cloud service provider to utilise software and applications running on the cloud infrastructure. The applications are accessed via remote computers and mobile devices using the appropriate cloud interface software. The consumer's device acts like a portal to the software and data stored in the cloud.

These deployment and service models will vary the type and amount of electronic evidence that can be collected on the client, server and network layers. Common across all the deployment and service models is the collection of log data; that is, information on how the primary/content data has been used or accessed is often collected as part of the standard operations of the cloud computing environment.

4. Consequences for Cybercrime and Digital Forensic Investigation

In much the same way as cybercrime may be understood as a new way of committing traditional crimes such as fraud and theft, cloud computing presents criminals with new tools with which to commit these offences.[32] Despite this, little work has been carried out in relation to the implications of cloud computing for LEAs and criminal investigation.[33] However, it has been suggested that many current law enforcement procedures have not been adapted to investigate attacks on cloud services[34].

Akin to cybercrime generally, cloud systems may be both the object and the subject of criminal activity.[35] Rogue elements may target cloud systems with the intention of capturing or corrupting data.[36] This can be achieved, for example, through the use of malware. Criminals may also use cloud computing systems to store illicit or illegal data (eg. child exploitation material) or, due to the quantity of processing power often available in a cloud computing environment, use the cloud as the base for a "brute force attacks" to crack

[32] Joseph Alhadeff, 'The Privacy and Security Implications of Cloud Computing' (Speech delivered at the United Nations Internet Governance Forum, Sharm El Sheikh, Egypt, 15–18 November.2009).
[33] Alan Sherman & Josiah Dykstra, 'Understanding Issues in Cloud Forensics: Two Hypothetical Case Studies' (Paper presented at. the Association of Digital Forensics, Security and Law Conference on Digital Forensics, Security and Law, Richmond, Virginia, United States, May 30–21 2012) 2–3.
[34] Choo, above n 27; Ben Martini and Kim-Kwang Raymond Choo, 'An integrated conceptual digital forensic framework for cloud computing', *Digital Investigation* 9(2) 71–80.
[35] Krone, above n 4, 1.
[36] Sherman & Dykstra, above n 33, 2.

passwords and encryption.[37] A recent report released by McAfee and Guardian Analytics[38] gave details of an online banking fraud scam which netted as much as £2billion. The scam operated by using phishing emails which infected the victim's computers with a Trojan capable of mimicking the website of the victim's bank. The Trojan would load a bogus copy of the bank's website and when users tried to transfer money between their accounts online, it would direct the transferred funds into the criminal's bank account. The unusual feature of this case was that the Trojan malware conducted transactions in the cloud environment rather than on the victim's computer.[39]

Digital forensic investigation is used to collect electronic evidence for investigations into both traditional criminal activity and cybercrime, such as the example just given. McKemmish[40] has described this field as 'the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable'. The four key elements of McKemmish's definition feature as points of discussion in analysis of digital forensic practices for technologies introduced today such as cloud computing. Identification refers to knowing the presence, type and format of electronic evidence, the identification of evidence is complicated by the introduction of cloud computing. Preservation relates to the requirement to ensure that evidence remains unmodified or modified as little as possible.

Cloud computing introduces a number of complications to conventional digital forensics processes. Many conventional tools have focused upon having physical access to the media that stores the data of potential interest. However, in a cloud computing environment it is often not possible or feasible to access the physical media which stores a customer's data. This is due to a number of features intrinsic to cloud computing. For example, in many instances cloud data will be stored overseas (and out of the jurisdiction) from the investigating agency. Even if the data is stored within jurisdiction, data distribution technologies may split a user's data across a number (potentially thousands) of storage devices within the cloud computing environment. LEAs would need to rely upon the cloud technology and the cloud service provider to gain access to the data that is stored by a customer and this can introduce issues with chain-of-custody best practices.

Before this data is exported for use by the LEA the data must be "preserved" (to ensure that the potential evidence is not modified) — a function which many cloud computing environments do not currently support. Consequently, this could result in accidental modification of data as it is exported from the cloud computing environment for LEA use or intentional destruction of data by the suspect.

Once the LEA has secured access to the cloud computing data, the format of the data is still not guaranteed and most of the prevalent digital forensic analysis tools have not yet been updated to decode the major cloud computing data export formats.[41] While many IaaS data exports will likely mimic the data format that is currently supported as virtual machines, SaaS

---

[37] Choo, above n 27, 3.
[38] *Dissecting Operation High Roller* (10 July 2012) McAfee and Guardian Analytics,. <http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf>.
[39] Elinor Mills, *Cybercrime Moves to the Cloud*.(30 June 2012) Digital Forensic Investigator News < Digital Forensic Investigator News >.
[40] Rodney McKemmish, 'What is Forensic Computing?' (Research Report No 118, Australian Institute of Criminology, 1999) 1.
[41] National Institute of Standards and Technology, 'Challenging Security Requirements for US Government Cloud Computing Adoption' (Draft Working Document, United States Department of Commerce, Gaithersburg, 2011) 21–4.

instances are more likely to use proprietary data formats and as such are unlikely to be supported by current tools.

5. Law Enforcement Responses

In response to the advent of cybercrime and digital evidence[42], LEAs have developed specialist investigatory bodies or divisions with skills and training in this type of crime.[43] The requirement that digital evidence be properly identified, collected, processed and analysed, both as a part of police investigations and in the context of court proceedings, has led to the development of "digital forensics". This specialised field of policing refers to 'the application of science' to the above process so as to ensure both the integrity of the information and the maintenance of a strict chain of custody for the data.[44]

Before this process can take place however, LEAs must first gain lawful access to data pertaining to a particular group or individual's activities. This enables the identification of an individual or collective thereof who appear to be engaging in illicit activity online. Access to existing data and interception of live data in Australia is governed by the State/Territory and Federal legislation. This controls the relationship between the Government/LEAs and the private sector, which provides internet, telecommunication and cloud services as it is the private sector's networks and infrastructure across which the suspect data passes and is ultimately stored.[45] Once this identification is made, LEAs may commence investigations into a group or individual using general or specific investigative powers (depending on the jurisdiction in question) and ultimately lay charges under the relevant legislation.

The law on data security and cybercrime in Australia is currently in a state of flux with the recent passage of the *Cybercrime (Legislative Amendment) Bill 2011* (Cth) ("the Bill") by the Australian Parliament and the current review being conducted of the national security legislation.[46] The passage of this Bill allows Australia to accede to the Convention on Cybercrime and brings Australia's law in relation to data retention, access and interception into line with a growing international network of LEA cooperation envisaged by the Convention.[47] While the scope of these changes should not be understated, it is important to note that in a number of respects, Australian law was compliant with many of the tenets of the Convention prior to the amendments mentioned above.[48]

5.1. Data Interception & Access Regime

LEAs undertaking cybercrime investigations routinely need access to two types of data: *content data* which is the substance of a communication or data packet (images, content of

[42] Digital devices are highly pervasive and any type of crime may produce digital evidence, not just those directly associated with cybercrime.
[43] For Example, the Australian Federal Police, High-Tech Crime Operations.
[44] Keyun Ruan, Joe Carthy, Tahar Kechadi & Mark Crosbie. 'Cloud Forensics: An Overview' in Gilbert Peterson & Sujeet Shenoi (eds). *Advances in Digital Forensics VII* (Springer, 2009) 36; Karen Kent, Suzanne Chevalier, Tim Grance & Hung Dang, *Guide to Integrating Forensic Techniques into Incident Response: Recommendations of the National Institute of Standards and Technology* (Special Publication 800-86, National Institute of Standards and Technology: United States Department of Commerce, 2006) C-1.
[45] Sharon Rodrick, 'Accessing Telecommunications Data for National Security and Law Enforcement Purposes' (2009) 37 *Federal Law Review* 375, 378.
[46] *Equipping Australia Against Emerging and Evolving Threats* (Discussion Paper, July 2012, Attorney-General's Department, Australian Government).
[47] Commonwealth, *Parliamentary Debates*, Senate, 22 August 2012, 6 (Matt Thistlewaite); Commonwealth, *Parliamentary Debates*, Senate, 22 August 2012, 7–8 (Joe Ludwig).
[48] Commonwealth, *Parliamentary Debates*, Senate, 22 August 2012, 7 (Joe Ludwig).

conversations, etc.) or *traffic data* containing information about the communication (point of origin, destination of communication, etc.). This section of the paper will focus on the legislative mechanisms currently in place which mediate the relationship between LEAs and the private companies who are in possession of this data from time-to-time and how LEAs gain access to this data.

For the purposes of this paper, the relevant legislation in this area is the *Telecommunications (Interception & Access) Act 1979* (Cth) ("TIA Act") and the *Telecommunications Act 1997* (Cth) ("Telco Act") as amended by the Bill.[49] These laws exist alongside legislation in force in the States/Territories and form part of a complex regulatory matrix governing the relationship between government and the private sector in relation to telecommunications data.

Much of the tension surrounding this issue revolves around the competing interests of LEAs on the one hand to be able to gain access to the data they need in order to effectively investigate and prosecute crime.[50] On the other hand, however, there has been vocal advocacy for individuals' right to privacy in relation to their online movements, with Rodrick[51] arguing that such concerns are more important than national security concerns. A third perspective is that of the service providers themselves, who have argued that an over-zealous approach to data retention would be costly and inefficient.[52] As the use of cloud computing becomes more prevalent, it is quite possible that a significant amount of evidence for crimes in Australia will leave Australian territory to a foreign cloud provider, and the only way to collect it may be via lawful intercept. The legislative regime also contemplates the provision of evidential material to foreign LEAs and this has given rise to concern that Australian LEAs may be implicated in investigations in foreign jurisdictions which lead to the imposition of the death penalty on an individual.[53] The government is of the opinion however that sufficient safeguards exist in this area.[54]

At present, it is common to break up the interception and access regime in Australia into three "interfaces".[55] The first relates to the ongoing relationship between the private sector and LEAs; it is governed by statute and contract law and relates to the obligations imposed on service providers to retain, store and monitor data and is largely administered through *service level agreements* between providers and the Government. The second deals with the ability of LEAs to access certain data without the need for a formal warrant. Finally, the third interface, concerns the data which LEAs can access pursuant to a search warrant.

The first interface requires the service provider to maintain the ability to intercept data flowing across their infrastructure or network to ensure that they can comply with requests by LEAs to access or intercept such data.[56] This is currently a focus of the inquiry into the national security legislation mentioned above, a key concern of which is 'tailored data

[49] This Bill was passed by the Senate on 22 August 2012.
[50] Commonwealth, *Parliamentary Debates*, Senate, 22 August 2012, 7 (Joe Ludwig).
[51] Rodrick, above n 45, 384–5.
[52] See. eg. Dylan Welch & Ben Grubb, 'Spy in the Machine', *The Age* (online) 21 July 2012 <http://www.theage.com.au/technology/technology-news/spy-in-the-machine-20120720-22fdi.html>.
[53] Joint Committee on Cyber Safety, Parliament of Australia, *Review of the Cybercrime Legislation Amendment Bill 2011* (2011) 46.
[54] Commonwealth, *Parliamentary Debates*, Senate, 22 August 2012, 8 (Joe Ludwig).
[55] LexisNexis, *Telecommunications Law and Policy in Australia* (at 20 August 2012) Ancillary Communications, 'Introduction' [610,100].
[56] Ibid, [611,200].

retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts' under the TIA Act.[57]

The second interface deals with LEAs' ability to access telecommunications data pursuant to service-providers' obligation to render 'reasonable assistance' to LEAs under s 313 of the Telco Act for the purposes of inter alia enforcing the criminal law.[58] For the purposes of this section the assistance required includes giving help by way of, for our purposes, giving effect to a stored communications warrant under the TIA Act[59] (see below), providing information about a communication that is lawfully accessed under such a warrant,[60] giving effect to authorisations under Division 3 or 4 of Part 4-1 of the TIA Act,[61] and (under the newly amended provisions) complying with a domestic or foreign preservation notice in force under Part 3–1A of the TIA Act (see below).[62]

Importantly, one means of access under this interface allows LEAs to acquire "telecommunications data" without the need for a warrant where it is volunteered by an employee of the service provider[63] or where disclosure is authorised by the LEA under the relevant provisions of the TIA Act.[64] These methods of disclosure exist as exceptions to the general prohibition in the Telco Act (Pt 13, Div 2) which proscribes disclosure or use of telecommunications data. They are distinguishable from data access pursuant to a warrant because they relate only to data which is already in existence and has been stored by the service provider at the time the authorisation is made. For this reason, the quantum of data to which the interface allows access is limited as service providers' data retention policies are non-uniform.[65] Furthermore, in line with recent technological developments, many service providers are increasingly unlikely to retain large quantities of traffic data.[66]

Telecommunications data is not specifically defined in the Telco Act or the TIA Act based on a bid for the term to remain 'technology neutral'.[67] The TIA Act provides only (in ss 171 and 172) that such data does not include the substance of the communication. Therefore it is essentially *traffic data*[68] or "metadata".[69]

Where disclosure of this data is authorised by a LEA, it may be accessed either on a retrospective or prospective basis. Where data is accessed on a retrospective basis it is referred to as 'stored data' (historical telecommunications data) insofar as it is already in existence at the time the request for access was made. This data may be disclosed where an

---

[57] *Equipping Australia Against Emerging and Evolving Threats,* above n 46, 10.
[58] *Telecommunications Act 1997* (Cth) s 313(3)(c) and (4)(c).
[59] *Telecommunications Act 1997* (Cth) s 313(7)(b).
[60] *Telecommunications Act 1997* (Cth) s 313(7)(c)(ii).
[61] *Telecommunications Act 1997* (Cth) s 313(7)(d).
[62] *Telecommunications Act 1997* (Cth) s 313(7)(ca).
[63] *Telecommunications (Interception & Access) Act 1979* (Cth) s 177(1).
[64] *Telecommunications (Interception & Access) Act 1979* (Cth) ss 178, 178A, 179, 180.
[65] See, eg, Law Council of Australia, Submission No 96 to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into Potential Reforms to the National Security Legislation*, 2012, 37 [167].
[66] Australian Federal Police, Submission No 163 to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into Potential Reforms to the National Security Legislation*, 2012, 15–6.
[67] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice,* Report. No. 108 (2008) 2485 [73.32].
[68] Rodrick, above n 45, 388; Rob Nicholls & Michelle Rowland, 'Regulating the Use of Telecommunications Location Data by Australian Law Enforcement Agencies' (2008) 32 *Criminal Law Journal* 343; Commonwealth, *Parliamentary Debates*, Senate, 22 August 2012, 11–12 (Joe Ludwig); *Telecommunications Act* 1997 s 276.
[69] Commonwealth, *Parliamentary Debates*, Senate, 22 August 2012, 12 (Joe Ludwig).

"authorised officer" is "satisfied" that disclosure is reasonably necessary for (inter alia) the enforcement of the criminal law.[70]

In aid of this power, the new amendments under the Bill allow interception and preservation of 'stored communications' (per articles 16 and 17 of the Convention). Domestic LEAs who are investigating a 'serious contravention'[71] of the criminal law may compel an internet service provider or cloud service provider to retain and preserve historic computer data for a period of 90 days[72] by issuing a historic preservation notice.[73] This power is separate to any disclosure required pursuant to a warrant (see below) and has been criticised for failing to distinguish between content and traffic data,[74] thus threatening privacy in relation to access by authorities to content data, which is accorded greater protection than traffic data under Australian law.[75]

Powers of this nature have previously received support from the Joint Committee on the Australian Crime Commission[76] which concluded that that it was highly desirable for service providers to maintain a log of traffic data in order to identify the origin and destination of a given communication. However, it also found that given the low up-take of the industry codes of practice on this issue, it was more desirable for the government to have sufficient powers to make targeted requests for information. In order to do this however, there must be a co-existent power to require that information be preserved and logged while the legal machinery for such a request is initiated.

Prospective data collection on the other hand relates to a situation where the service provider is called on to proactively monitor an individual's activities and record in real time all the data they can in relation to that individual. It applies to data which is not already in existence at the time the request for access is made.[77] This effectively allows for the live tracing of a person's online movements and associations.[78] It has been likened by some[79] to active surveillance of a person, rather than data collection; this raises significant privacy concerns because such conduct need not be authorised by the issuing of a warrant.[80] This lack of judicial oversight has been attributed to a governmental preference for security over privacy.[81] Although it arguably allows police to respond quickly to suspected criminal activity, obtaining access to critical data before the trail of evidence goes cold. In deference to such concerns, section 180(5) requires the person making the authorisation to first consider how it would impact on the privacy of any person concerned. Furthermore, authorisation may only be given where the officer is satisfied that 'the disclosure is reasonably necessary for the investigation of an offence…that is punishable by imprisonment for at least 3 years'.[82] The amendments to the TIA Act add to this power in relation to 'interception agencies' such as ASIO by making available ongoing preservation notices which require service providers to

[70] *Telecommunications (Interception & Access) Act 1979* (Cth) s 178(3).
[71] Joint Committee on Cyber Safety, above n 53, 14 [3.16].
[72] *Cybercrime (Legislative amendment) Bill 2011* (Cth) s 107K(b)(i).
[73] *Cybercrime (Legislative Amendment) Bill 2011* (Cth) s 107H(1).
[74] Joint Committee on Cyber Safety, above n 53, 17 [3.51].
[75] Ibid; *Explanatory Report to the Convention on Cybercrime*, para 210.
[76] Joint Committee on the Australian Crime Commission, Parliament of Australia, *Cybercrime* (2004) 30.
[77] *Telecommunications (Interception & Access) Act 1979* (Cth) s 180(2).
[78] Nicholls & Rowland, above n 68, 345–6.
[79] See eg. Rodrick, above n 45, 401.
[80] Ibid.
[81] Nicholls & Rowland, above n 68, 348.
[82] *Telecommunications (Interception & Access) Act 1979* (Cth) s 180(4).

'preserve communications on an ongoing basis in relation to a specified individual'.[83] This power is not available to LEAs and will thus not be investigated further.

However, it is arguable that if the planned amendment to the national security legislation is passed requiring service-providers to retain log files on users' data for a period of two years, the utility of this interface might be significantly increased in relation to LEAs.[84] In response to this though, concerns have been expressed that such a reform, in addition to potentially being technologically unfeasible, may not be a 'necessary or proportionate response to investigating serious criminal activity'.[85] Aside from the implications for privacy, it stands to reason that by collecting vast quantities of data about individuals such as their movements (through location data obtained from mobile phones), their social networks (through call logs) and their internet browsing habits, service providers would themselves become targets for cybercriminals intent on gaining access to data in order to facilities crimes such as identity theft.

Finally, the third interception and access interface pertains to the ability of LEAs to obtain a search warrant requiring disclosure of content data stored by service providers. [86] The application of the relevant sections is uniform across all Federal, State and Territory LEAs.[87] Part 2.5, Division 4 of the TIA Act provides the legislative basis on which a warrant may be issued authorising a LEA to intercept telecommunications in real time. The use of a real-time telecommunication intercept may allow access to data stored on a cloud server. However, this is complicated by the fact that many CSPs provide encryption services, making interception very difficult in such cases.

Warrants requiring the disclosure of stored communications are regulated by Part 3-3 of the TIA Act. These warrants may only be granted under s 116 TIA Act where the LEA is investigating a "serious contravention" of the criminal law and allow access to data retained pursuant to a historic preservation notice (above) under the new Part 3–1A of the TIA Act.

5.2. Access to Data from an Individual's Private Property

After a LEA has sourced data pertaining to a group or individual and decided there is sufficient evidence to continue the investigation and potentially prosecute, they may seek a warrant under the legislation applicable to the relevant jurisdiction, authorising them to carry out certain investigative functions on private property.

In order to tackle cybercrime, for example, Governments across Australia and New Zealand have enacted legislative mechanisms which give LEAs powers to investigate crimes that involve ICT. Some jurisdictions have specific provisions for dealing with the issue while others rely on general investigative powers applicable to traditional offences. Furthermore, a number of Australian jurisdictions have based their legislation on the recommendations found in the *Model Criminal Code* (see eg. Commonwealth, ACT, NSW Vic), while others have adopted a different suite of provisions.

Given the limited scope of this paper, what follows is a brief synopsis of the investigative powers as they stand under the Commonwealth legislation as the relevant provisions deal

[83] Joint Committee on Cyber Safety, above n 53, 12–13 [3.05].
[84] Ibid.
[85] Law Council of Australia, above n 63, 37; and see Eileen Ormsby, 'Big Brother Laws Grossly Disproportionate to any Threat', *The Age* (Melbourne) 31 August 2012, 13.
[86] Nicholls & Rowland, above n 68, 345.
[87] *Equipping Australia Against Emerging and Evolving Threats,* above n 46, 24.

specifically with access to and investigation of electronic devices. Once a search warrant in respect of a premises[88] is issued under s 3E of the *Crimes Act 1914* (Cth) ("the Act"), an executing officer named in the warrant as being responsible for executing the warrant[89] becomes authorised to exercise the powers which appear in the relevant section so Part 1AA, Division 2 of the Act.

5.2.1. Use of Electronic Equipment at Premises

When investigating the commission of a crime, an executing officer is authorised under the terms of the warrant[90] to 'operate electronic equipment[91] at the warrant premises to access data[92] (including data not held at the premises) if he or she suspects on reasonable grounds that the data constitutes evidential material'. In circumstances where assistance is required in order to operate the equipment or access specific date held on it, the officer can apply to a magistrate under s 3LA(1) for an order requiring a specified person to assist in accessing that data, copying it or converting it into documentary form.

This power is intended to allow the officer/s to require a person with knowledge of the computer or network to provide access to data stored therein if that data is, for example, encrypted or password protected.[93] Its inclusion was justified in part, by reference to the inclusion of a similar power in the Cybercrime Convention art 19 developed by the Council of Europe.[94] However, privacy advocates and academics have raised concerns about such power.[95] Where assistance is required in operating the equipment and the executing officer believes on reasonable grounds that the material is liable to be destroyed, modified or tampered with they may 'do whatever is necessary to secure the equipment, whether by locking it up, placing a guard or otherwise'[96] for a period of up to 24 hours or until expert assistance can be obtained, whichever happens first.[97]

Once the data has been accessed the executing officer is authorised to make copies of it either on the premises or after removing the equipment, with the owner's consent if they suspect on reasonable grounds that it constitutes evidential material.[98] If evidential material does emerge, the officer may seize the electronic equipment and any disk or (if possible) convert the material into documentary form and seize that.[99] This is subject to s 3L(3) which makes seizure an option of last resort if it is not practicable to copy the data or place it in documentary form, or if it would be an offence for the occupier to go on possessing the

---

[88] *Crimes Act 1914* (Cth) s 3F(1).
[89] *Crimes Act 1914* (Cth) s 3C(1).
[90] *Crimes Act 1941* (Cth) s 3L(1).
[91] This should include a computer or data storage device as defined in s 3C(1).
[92] Defined in *Crimes Act 1941* (Cth) s 3(1) as including (a) data in any form; and (b) any program (or part of a program).
[93] Explanatory Memorandum, Cybercrime Bill 2001 (Cth), 20. Similar provision is found in s201A of the *Customs Act 1901* (Cth) and part III of the *Regulation of Investigatory Powers Act 2000* (UK).
[94] Ibid.
[95] See. eg. Nickolas James, 'Handing Over the Keys: Contingency, Power and Resistance in the Context of Section 3LA of the Australian Crimes Act 1914' (2004) 23 *University of Queensland Law Journal* 7; *Commentary on the Cybercrime Bill 2001* (23 July 2001) Electronic Frontiers Australia <https://www.efa.org.au/Publish/cybercrime_bill.html>.
[96] *Crimes Act 1941* (Cth) s 3L(4).
[97] *Crimes Act 1941* (Cth) s 3L(6). This period may be extended under sub-section 7. Notice of these arrangements must also be given to the occupier under sub-sections 5 and 8.
[98] *Crimes Act 1941* (Cth) s 3L(1A).
[99] *Crimes Act 1941* (Cth) s 3L(2).

equipment. Similar powers exist in relation to equipment which has been removed from the premises over which the warrant was exercised.[100]

5.2.2. Exercise of Investigative Powers in Cooperation with LEAs in Other Jurisdictions

For cybercrime cases including online child exploitation, international cooperation is usually required at the beginning of the investigation process as demonstrated by the recent success of "Operation Rescue" in 2011.[101] This can, however, pose a challenge for traditional criminal law which is generally regarded as being designed to maintain internal order, while external threats have traditionally been dealt with by the military.[102]

Where cybercrime originates from a jurisdiction other than Australia, the official arrangements in place for cooperation between LEAs depend largely on the status of Australia's relationship with the country of origin. Where diplomatic ties exist, official protocol requires that a request for assistance be made via the Mutual Legal Assistance unit in the Attorney General's Department pursuant to the *Mutual Assistance in Criminal Matters Act 1987* (Cth). Where an accused is located in another country, however, it may be necessary to seek extradition. Australia, for example, may request the extradition from other countries of persons who have committed acts online that adversely affect Australian citizens or interests for them to be returned to Australia to face prosecution as governed by the *Extradition Act 1988* (Cth).

Smith[103] has explained that the utility of this procedure however, is undermined by the cumbersome and often ineffective nature of these official requests. Delay of several weeks or even months may be commonplace, leading the trail of evidence to turn cold before assistance is secured. This leads law enforcement officials to increasingly rely on personal, informal networks in order to gain access to the necessary material. These have been shown to be the most effective means available for dealing with trans-border criminal activity in lieu of more formalised linkages and procedures.

In addition, concerns exist in relation to the rule of law in certain countries where conduct which may be prohibited in Australia is not considered illegal in another jurisdiction. For example, Grabosky[104] has explained that '[t]he person who released the I LOVE YOU virus in May 2000, for example, could not be prosecuted in the Philippines because there was no law in that country at the time that prohibited the release of malicious code.'

Satisfying the criterion of dual criminality — the alleged misconduct must constitute an offence under both the laws of the extradition country and the requesting country — is therefore, necessary in both extradition and mutual assistance requests. The United Kingdom ("UK") is, perhaps, one of few jurisdictions to have abolished the criterion of dual criminality for sexual offences involving children tried under extraterritorial jurisdiction. Subsection 72(1) of the *Criminal Justice and Immigration Act 2008* (UK) states that if a UK national

[100] *Crimes Act 1941* (Cth) s 3LAA.
[101] Commonwealth, *Parlaimentary Debates*, Senate, 22 August 2012, 6 (Matt Thistlewaite); Karen McVeigh, 'Police shut Down Global Paedophile Network in operation Rescue', *The Guardian* (online) 16 March 2011 <http://www.guardian.co.uk/society/2011/mar/16/global-paedophile-ring-smashed>.
[102] Susan Brenner & Joseph Schwerha, 'Cybercrime Haven' (2008) 25(9) *The Computer & Internet Lawyer* 19–21
[103] Russell Smith, 'Investigating Cybercrime: Barriers and Solutions' (Paper presented at the Pacific Rim Fraud Conference, Sydney, September 11, 2003).7.
[104] Peter Grabosky, 'Requirements of Prosecution Services to Deal with Cyber Crime' (2007) 47(4–5) *Crime, Law & Social Change* 201, 208.

does an act in a country outside UK, and the act, if done in England and Wales or Northern Ireland, would constitute a sexual offence to which this section applies, the UK national is guilty in that part of UK of that sexual offence. This procedural safeguard has been the subject of criticism however on the basis that is undermines cooperative investigations across jurisdiction.[105]

Schedule 2, Part 1 of the Bill makes dual criminality a threshold requirement for the issuing of a 'stored communications warrant'.[106] Some concern was expressed at the committee stage that non-commensurate definitions of offences in other countries may mean that Australia is prevented from providing assistance in relation to offences concerning child exploitation.[107] However, the government expressed the opinion that the Attorney-General's Department is not aware of any child exploitation offences in foreign jurisdictions which would not fall within the definition of 'serious criminal offence' as required by the new provisions.[108]

These warrants related to stored content data may be sought by a LEA where a foreign LEA has made a formal request for assistance to the Attorney-General in accordance with the *Mutual Assistance in Criminal Matters Act 1987* (Cth) where certain conditions are met as required by newly amended provisions of the TIA Act are met.[109]

In order to allow for compliance with these requests for assistance, the Bill amends the TIA Act to require the Australian Federal Police ("AFP") to issue a service provider with a foreign preservation notice[110] in response to a request for a foreign country.[111] These function in much the same way as a domestic preservation notice (see above). Although the AFP has no discretion to refuse such a request, disclosure of the stored information can only be given in response to a formal request for assistance to the Federal Attorney-General by the foreign LEA and the investigation must relate to a 'serious foreign contravention' of the criminal law.[112] Access to the information is then regulated by the mutual assistance regime which arguably affords a sufficient safeguard against access that might otherwise be 'inconsistent with Australian values'.[113]

This international cooperation is facilitated by a 24/7 network operation in each country that is a party to the Convention.[114] This is designed to facilitate immediate responses to requests for assistance.[115] Australia is already compliant with this requirement and provides this service through the AFP Operations Coordination Centre.

Hufnagel[116] has pointed out that in addition to jurisdictional barriers in place between nation states, irregularities within domestic jurisdictions such as Australia also pose problems. However, jurisdictional conflicts between the AFP and State/Territory police are largely

---

[105] Yvon Dandurand, Gherardo Colombo & Nikos Passas, 'Measures and Mechanisms to Strengthen International Cooperation Among Prosecution Services' (2007) 47(4–5) *Crime, Law & Social Change* 261, 268.
[106] Explanatory Memorandum, Cybercrime (Legislative amendment) Bill 2011 (Cth), 21.
[107] Joint Committee on Cyber Safety, above n 53, 29.
[108] Commonwealth, *Parliamentary Debates*, Senate, 22 August 2012, 8 (Joe Ludwig).
[109] See *Cybercrime (Legislative Amendment) Bill 2011* (Cth) ss116(1)(d)(ii), 142A.
[110] *Cybercrime (Legislative Amendment) Bill 2011* (Cth) s 107N(1).
[111] *Cybercrime (Legislative Amendment) Bill 2011* (Cth) s 107P(1).
[112] *Cybercrime (Legislative Amendment) Bill 2011* (Cth) s107P(1)(c).
[113] Joint Committee on Cyber Safety, above n 53, 22 [3.53].
[114] *Convention on Cybercrime*, above n 3, Chapter III, Title 4.
[115] *Explanatory Report to the Convention on Cybercrime*, para 298; Commonwealth, *Parliamentary Debates*, Senate, 22 August 2012, 6 (Matt Thistlewaite).
[116] Saskia Hufnagel, 'Cross-Border Police Co-Operation: Traversing Domestic and International Frontiers' (2011) 35 *Criminal Law Journal* 333.

resolved informally through agreements between the relevant authorities as to who will take carriage of a particular matter. This horizontal cooperation is facilitated by several national organisations such as the Australian Crime Commission.[117]

Disparities within and between countries will continue to create risks of criminal exploitation and pose a challenge for law enforcement investigations. We may not have fully harmonised cybercrime legislation due to the different judicial and legal systems internationally, but we need to have a coordinated international approach to principles of cyber security, and privacy and data protection. Once we are able to achieve some measure of uniformity (e.g. developing internationally accepted "cyber norms" that would serve as a guide to acceptable cyber behaviour), we would create an environment which is hostile to cybercrime, and minimise the risk of so-called 'jurisdiction shopping' in which offenders seek out countries from which to base their activities that have the least severe punishments or which have no extradition treaties.

6. Analysis and Implications for Cloud Computing

The advent of cloud computing poses a number of significant issues for cybercrime investigations. With private individuals, companies and groups placing an ever-increasing volume of data into cloud systems,[118] LEAs are increasingly finding that the data in question can become either inaccessible or at least very difficult to access.[119] The process of data distribution leads to a situation where information may be disseminated across a huge number of physical machines, some of which may be outside of the investigating body's national or even international jurisdiction.[120] As part of the operations of a cloud computing environment, a provider may store a customer's data across multiple servers (that may result in "trans-border data-flow"), challenging the ability of LEAs to enforce seizure warrants and rendering access to the data difficult without infringing on the privacy of innocent individuals or breaching confidentiality laws. Furthermore, the global nature of data storage in clouds means that in some cases, the legislative frameworks of various jurisdictions apply to different packets of information.[121] This requires increased communication and cooperation between various LEAs.

6.1. Cloud Computing and the Relationship between LEAs and the Private Sector

This paper proceeds on the assumption that the private sector may be involved in the investigation of cybercrime offences by LEAs in three capacities: as an internet service provider ("ISP") or telecommunications service provider ("TSP"); although firms may provide both services simultaneously (eg. Telstra); and as a cloud service provider. Companies who act as an ISP/TSP facilitate the passage of information from personal computers or other electronic devices to the cloud and vice versa. As data passes across these firms' networks or infrastructure, the interception and access regime set out above in Australia would apply to require them to maintain the capacity to give LEAs access to this data as mandated by the relevant legislation. Furthermore, under the proposed changes to the national security legislation, further requirements could be placed on these firms requiring them to maintain a log of each user's traffic data for a period of two years so as to facilitate

[117] Ibid, 337.
[118] Sean Harrington, 'Collaborating with a Digital Forensics Expert: Ultimate Tag-Team or Disastrous Duo? (2011) 38(1) *William Mitchell Law Review* 354, 393.
[119] Ibid.
[120] Vincent, above n 24, 52.
[121] Ibid.

investigations into suspects (see above). In the context of cloud computing, these mechanisms appear to be designed to enable LEAs to determine the path that a given data packet has followed, the substance of that data packet (where the content data has been retained), and the ultimate location of that data.[122]

Thus, ISP/TSPs serve an intermediary function insofar as we are here concerned with cloud computing and its consequences for law enforcement investigations. The more complicated problem is, what laws apply to the interaction between LEAs and cloud service providers ("CSP"). The interception and access regime in Australia applies only to companies who operate a 'telecommunications service'[123] which enables communications to be carried across a 'telecommunications system'[124] operated by the carrier. Importantly for our purposes, a 'communication is defined in s 5 of the TIA Act to include data[125] and not simply speech or sound. However, it is thought that CSPs such as Google, Amazon and Dropbox are not involved in the provision of such services and so the data interception and access regime outlined above would not apply to them insofar as those firms have a presence in Australia.

The consequence of this is that LEAs would have obtained sufficient evidence from client devices and ISP/TSPs to identify the subject of their investigations using the interception and access regime. LEAs would therefore, be relying on the search warrant provisions under the *Crimes Act 1914* (Cth) (see above) in order to procure the evidence they need to proceed with prosecution.

In the case of domestic operations, it is submitted that cloud computing would not impose significant investigatory barriers to LEAs. The powers conferred under the *Crimes Act 1941* (Cth) ss 3L(1) or 3LAA(1) allow the investigating officer to access data which is not held on the premises to which the warrant applies subject to the notification requirements in s 3LB. In practice, these provisions would allow an officer to access data remotely from an individual's computer where a link to that data is provided on the machine in question and to carry out their search warrant powers at the site on which that data is located. Therefore, if an individual had a link to data which may constitute evidential material on their computer, but the physical data were located within a CSP's infrastructure based within Australia, LEAs could, pursuant to their powers under the search warrant, go to the CSP's premises and gain access to the relevant data. Importantly, the reasonable assistance provisions contained in s 3LA would also probably apply.[126] It is likely that this link would be discovered as part of forensic procedures on devices physically accessed by the suspect (such as computers and mobile devices). It is expected that case processing tools will automatically detect cloud computing usage as part of the analysis of these evidence items.

6.2. Multi-Jurisdictional Issues

This picture becomes significantly more complicated however if the investigation involves ISP/TSPs who have networks which span multiple jurisdictions or where the CSP is located in a jurisdiction other than that in which the investigation is taking place. As explained above,

---

[122] See, eg, Australian Federal Police, above n 66, 16.
[123] *Telecommunications (Interception and Access) Act 1979* (Cth) s 5.
[124] *Telecommunications (Interception and Access) Act 1979* (Cth) s 5 defines this as a telecommunications network that is within, or partly within Australia. 'Telecommunications network' is defined in s 5 also.
[125] As "data" is not defined in the TIA Act, we apply the definition found in s 3C of the *Crimes Act 1914* (Cth) which includes 'information in any form'.
[126] See Stephen Biggs, *Red Tape: will Current Legislation Isolate Cloud Computing Data From the Forensic Gaze?* (17 July 2009) Digital Forensic Investigator News <http://www.dfinews.com/article/red-tape-will-current-legislation-isolate-cloud-computing-data-forensic-gaze>.

the practice of data distribution makes this latter situation commonplace. These trans-border data-flows highlight the need for international cooperation when investigating cybercrime generally and crimes which make use of cloud technology more specifically.

The current state of the law in Australia as it pertains to mutual legal assistance has been summarised above. The inefficiencies of that system in relation to cybercrime investigations have led to calls for reform from various interested parties. In response, the Australian government in 2011 to draw up the Bill which, among other things, purported to affect changes in the way Australian LEAs interact with LEAs from other jurisdictions in relation to the investigation of cybercrime.

The Bill seeks to give effect to the Convention's desire for a regime of international communications and mutual assistance which aims to redress the inefficiencies in the current process of diplomatic cooperation and to some extent,[127] formalise the ad-hoc cooperative practices between different LEAs. The objective of the proposed regime is to aid international investigations by making the investigatory tools available to domestic authorities, equally available to overseas authorities on request (see article 23). The Bill seeks to give effect to this goal through its provision for historic preservation notices and stored communications warrants (see above).

6.3. Implications for Law Enforcement Investigations Involving Cloud Computing

The Explanatory Report to the Convention on Cybercrime makes clear in several sections that the operation of these provisions is subject to the treaty-based relationships currently in place between State Parties. The provisions pertaining to articles 30, 31 and 33 above for example, require that a request for assistance be made to the Commonwealth Attorney-General. While this approach resembles the ordinary diplomatic process, the provision for expedited disclosure in certain circumstances may go some way to redressing the extensive delay associated with diplomatic channels.

Furthermore, the Bill purports to go further in establishing a regime for the disclosure of certain data without the need for a formal request under the mutual assistance regime. Above, this paper explains the regime which allows LEAs to require a telecommunications service provider to disclose specific telecommunications/traffic data without the need for a formal warrant. This "historic" (i.e. stored) data may be disclosed to a foreign authority pursuant to ordinary diplomatic channels under the *Mutual Assistance in Criminal Matters Act 1987* (Cth) section 38C. Data may also be disclosed under the new s 15D of that Act where the requirements in s 180B(3) of the TIA Act are met.

Under the Bill requests for assistance may be made on a police-to-police basis in relation to 'historical telecommunications data' and 'existing telecommunications data'.[128] These terms are not specifically defined but refer to *traffic* data which has already been stored subject to a request by a domestic or foreign LEA. The provisions would abolish the current oversight requirements (i.e. initiation of diplomatic process) in favour of a regime allowing the Commissioner, Deputy Commissioner or senior executive of the AFP to authorise disclosure of specified historical telecommunications data for the purposes of enforcing a foreign criminal law.[129] A concurrent section allows for the provision of information to foreign LEAs

[127] *Explanatory Report to the Convention on Cybercrime*, para 242.
[128] *Telecommunications (Interception and Access) Act 1979* (Cth) s 180A.
[129] Joint Committee on Cyber Safety, above n 53, 39 [5.9].

where that information has already been disclosed for the purposes of domestic law enforcement.[130] These provisions apply to traffic data only and not content data.

The amendments were the subject of strident debate before the Parliamentary Joint Committee.[131] In particular, the removal of the oversight otherwise provided by the Federal Attorney-General was a cause for concern and led to calls for strict regulation and specific guidelines in this area in order to prescribe the appropriate decision-making process. More recently a submission to the Parliamentary Joint Committee on Intelligence & Security Inquiry into potential reforms of National Security Legislation by Australian Federal Police acknowledged the importance of accountable use of powers and independent oversight.[132]

The Bill provisions may be characterised as allowing for more expeditious and streamlined cooperation between LEAs from a number of jurisdictions. The discussion above shows that criminal activity which utilises cloud technology will commonly occur across State borders and may in some cases trade on the inefficiencies which currently exist. Delays in gaining access to data may lead a trail of evidence to go cold or even prevent the detection of a crime in the first place. These issues must of course be balanced against privacy concerns (see generally, Rodrick, 2009)[133] and it should be noted that this report acknowledges the different privacy concerns which exist in relation to "content" data as opposed "traffic" data; this is generally reflected in the relevant legislative provisions.

7. Conclusion

Reforms such as those constituted by the Cybercrime Bill and those proposed under the current inquiry into the national security legislation are frequently generative of understandable concerns around privacy and security of personal information. One might be forgiven for thinking on just how much free publicity goes to George Orwell's *1984* at times like this. Justified though such concerns may be, it is easy to get distracted from the fact that cybercrime is a vastly profitable and infinitely complex affair. Tailoring legislative and policy responses to such a volatile and rapidly changing issue is fraught with difficulty and uncertainty. It may be trite to say that knee-jerk reactions to sometimes sensationalist data must be avoided, while deliberative solutions based on consultation must be promoted.

For a nebulous issue such as cloud computing, the appropriate policy and legislative response seems to be promoting greater harmonisation of substantive and criminal law across jurisdictions and the formation of linkages between LEAs to allow investigations to occur at an international level.

Little can be done to disentangle the complex web of relationships which allow for service delivery and use of cloud infrastructure. Economic efficiency, technological capabilities and other practical considerations all function in a way which ensures that cloud services will largely be provided on a global scale and involve multiple jurisdictions. Importantly though, steps need to be taken to reduce the opportunities for criminals to abuse the privileges offered by this technology.

This paper has set out Australia's response to the issues posed by cybercrime and its connection to cloud computing. Providing LEAs with the necessary tools and relationships to effectively police illicit activity online will inevitably involve striking a balance between

[130] Ibid, 39 [5.14]; *Telecommunications (Interception and Access) Act 1979* (Cth) s 180C.
[131] Joint Committee on Cyber Safety, above n 53, 40–5 [5.19]–[5.38].
[132] Australian Federal Police, above n 66, 8.
[133] See generally, Rodrick, above n 45.

privacy on the one hand and appropriate police powers on the other. It is submitted that the most recent reforms strike the right balance on this issue and help to ensure that Australia's laws are more harmonious with other countries. This allows us to effectively participate in trans-national investigations into criminal activity and in so doing, may improve our relationship with LEAs in other countries and thereby allow us to more effectively access data held offshore for our own criminal investigations.

An area of concern, however, relates to awareness around the issues created by cloud computing. The law itself and the explanatory documentation accompanying it makes little or no reference to cloud computing. This means that the current mechanisms must be applied in practice to combat criminal activity which occurs on or targets cloud infrastructure. If awareness around the nature and challenges of cloud computing is low, then this may hinder effective police operations. These issues are compounded by the complex nature of cloud computing and the fact that much of literature on it is targeted at people and organisations who already have a relatively sophisticated knowledge of ICT. The terms of the current inquiry into the national security legislation recognises the need to consider extending the interception and access regime to cloud service providers.[134]

It is submitted therefore that more needs to be done to systematise knowledge of cloud computing among LEAs and in the community generally. Agencies such as the National Institute of Forensic Science ("NIFS"), which sits within the Australia and New Zealand Police Advisory Agency have a key role to play in relation to education security personnel and it is noted that a soon-to-be-released report on this very issue has recently been produced by NIFS. Similar documentation ought to be made available to members of the public as one element of a wider general education campaign.

As with many new technologies, people are often quick on the up-take and use of such service, but slow to comprehend or turn their mind to the dangers they pose; cloud computing is no different. In a generation where technology is designed to operate as its own instruction manual in that people learn about the product through use of it, readership of instructional information is low. This poses a risk in relation to cloud computing and it is therefore submitted that more should be done to make the public aware of these concerns and to increase knowledge among LEAs about the functionality and concerns posed by cloud computing.

Christopher Hooper [cahoo1@student.monash.edu.au] BA (Monash University), Undergraduate Honours student in Law (Monash University), Faculty of Law, Monash University, Wellington Rd, Clayton, Victoria 3168, Australia.

Ben Martini [ben.martini@unisa.edu.au] Digital Forensics Research Administrator and PhD Scholar, Information Assurance Research Group, Advanced Computing Research Centre, University of South Australia, Mawson Lakes Campus, South Australia 5095, Australia

Kim-Kwang Raymond Choo (Corresponding Author) [raymond.choo@unisa.edu.au] Fulbright Scholar and Senior Lecturer, Information Assurance Research Group, Advanced Computing Research Centre, University of South Australia, Mawson Lakes Campus, South Australia 5095, Australia

[134] *Equipping Australia Against Emerging and Evolving Threats,* above n 46, 27.

Acknowledgments: The authors wish to acknowledge the useful experience and background information gained from the first author's time at the National Institution of Forensic Science, housed within the Australia and New Zealand Police Advisory Agency, which formed the background for this research. The second author is supported by scholarships from both the University of South Australia and the Defence Systems Innovation Centre. The views and opinions expressed in this paper are those of the authors alone and not the organisations with whom the authors are or have been associated / supported.