Assignment 2

Research Paper

Internet Telecommunications Interception Regulations

Name: Beau Lebens

Student Number: 09918322

Unit Name: NET23

Email Address: beau@dentedreality.com.au

Date Submitted: 25 November 2003

Word Count: 3,766

By submitting this assignment, I declare that I have retained a suitable copy of this assignment, have not previously submitted this work for assessment and have ensured that it complies with university and school regulations, especially concerning plagiarism and copyright.

Internet Telecommunications Interception Regulations

1. Executive Summary

Technological developments in Internet-related technologies, especially its use as a communications medium, have raised the requirements for law enforcement agencies to be able to intercept communications in an attempt to enforce the law and investigate criminal activities. This paper will explore the legislation related to the legal interception and analysis of communications via the Internet and the related groups and issues relating to personal privacy. It will compare legislation in place around the world with that in place within Australia, while offsetting potential concerns with a look at the personal privacy advocate group Electronic Frontiers Australia and the public press that these issues receive. Finally, it will provide an overview of Australia's apparent current standing with regards to these issues, and a look at what the future may hold.

2. Background

In the past, telecommunications interception legislation has only been able to intrude on a small portion of our lives. Our main form of interceptable communication was telephone conversation, which although private, is more likely to be personal chit-chat than it is business transactions, anonymous admissions, or anything we hoped to keep specifically private. Laws have existed within Australia for many years (i.e. the *Telecommunications (Interception) Act 1979*) relating to the interception of telephone and radio communications, with a relatively small amount of resistance. With the advent of the Internet and the perceived privacy (Frankel, M. & Siang, S. 1999, pp. 7) while using the facilities therein, people express dissatisfaction with any sort of legislation that allows government to intercept their communications or activities while online. Australian law enforcement agencies (LEAs) have always maintained their requirement to be able to intercept communications to assist in legal investigations, and recent world developments such as the September 11 terrorist attacks and the Bali Bombings have only highlighted this requirement. With increased tensions relating to global security, and accusations that terrorism networks are making use of secured Internet communications (Kelley, 2001), the need for Australia's law enforcement agencies to be able to intercept and analyse online communications is greater than ever.

3. Definitions

For the purposes of this paper, the following terms are defined:

Australian Security Intelligence Office (ASIO)

> ASIO is Australia's federal security agency within the country (relating to domestic security, rather than foreign). As a single organization, they have the most intrusive powers of interception within the country (See Cassidy, 1999 for EFA's review of legislation affecting ASIO's powers).

Carnivore

> Carnivore is an FBI-controlled network-monitoring system, which sniffs all packets of data passing its network segment, and passes them via a filter. Data

matching the requirements of the filter are saved for further analysis by the FBI. Carnivore is not omnipresent on the Internet (or within a target network) and must be physically installed on a network segment of an ISP to be operational (Kerr, 2000).

Cybercrime

The act of using computers, computer networks or electronic information to commit criminal acts (paraphrased from Council of Europe: Convention on Cybercrime, 2001).

Defence Signals Directorate (DSD)

The DSD is Australia's primary electronic telecommunications expert facility. The DSD processes and analyses communications in the name of protecting Australia's national security. (http://www.dsd.gov.au/)

ECHELON

Although publicly denied, ECHELON is believed to be a staggeringly expansive network of observation centres, which monitor almost all forms of electronic communications, including radio, telephone and Internet. As with Carnivore, ECHELON matches communications using 'Dictionaries' (complex filters) which relate to flagged topics of interest. When matches are found, copies of the communications are forwarded to the interested agencies within a world-wide network of participants, believed to include (at least) the USA, UK, Australia, New Zealand and Canada (Poole, 2000).

Electronic Frontiers Australia (EFA)

A "non-profit national organisation representing [Australian] Internet users concerned with on-line freedoms and rights." (General Information About EFA, Updated 2002)

Internet Service Provider (ISP)

An Internet Service Provider is a commercial organization that provides a point where individuals and business may connect to and gain access to the Internet for a fee.

Law Enforcement Agency (LEA)

In discussions about telecommunications interception, LEA most commonly refers to federal-level agencies such as the Federal Police, ASIO and DSD. It can also include State Police when required, normally upon specific appointment by federal authorities.

4. Current Related International Legislation and Operations

Around the world, there are a number of other countries that are discovering internet-based communications require specific attention in regards to interception laws and regulations. A brief review of current international legislation, operations and systems helps to define the global environment in which Australia exists.

i. United States of America

Despite their strong beliefs in freedom of speech and rights to privacy, the United States is perhaps one of the most active Internet-communication observers in the world. They have developed a number of technologies and legislations specifically targeted at observing their own citizens, as well as observing communications internationally. Since the terrorist attacks in 2001, they have also enacted new legislation, which gives their LEAs sweeping interception and analysis powers. Three key elements are reviewed below:

United States Code: Interception of Digital and Other Communications: Assistance Capability Requirements

Under Section 1002 of the United States Code (US Code, Title 47, Chapter 9, Sub Chapter I, Sec. 1002), telecommunications carriers must basically ensure that their systems are capable of implementing a legally sanctioned electronic wiretap to collect specific information relating to a defined target person or organization. This legislation is similar in effect to Australia's *Telecommunications Act 1997*. If they are not capable of

providing this functionality, the FBI will install their Carnivore system (see below) to allow for communications interception as required.

USA PATRIOT ACT

The *'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism' (USA PATRIOT) Act of 2001*, enacted in the wake of the September 11 terrorist attacks, provides American LEAs with significant powers in relation to the investigation and prosecution of potential terrorist activity (amongst other things) within the United States of America. Of particular note is Title II: Enhanced Surveillance Procedures, which provides significant powers for authorities to intercept wire, oral, and electronic communications relating to both terrorism and computer fraud (a modification to *The United States Code, Title 18, Part I, Chapter 119, Sec. 2516*).

Carnivore

"Carnivore is a very effective and discriminating special purpose electronic surveillance system" developed by the United States' Federal Bureau of Investigation (FBI) to assist in wiretaps on Internet-based communications. The Carnivore system is a single-machine filtering unit, which is placed on the network of an ISP, where it has a portion of all network traffic passed through it. The device filters all data passing through it to determine a match against a set of rules, most specifically a target person under investigation. All communications matching the requirements of the operation are stored to disk, where they are available for later thorough investigation. Communications that do not match the filters are discarded. The FBI is allowed to use Carnivore in investigations on persons within the United States, but requires the full knowledge and assistance of ISPs to implement it within their networks. If an ISP is capable of complying with an information requirement using their own lawful methods, then Carnivore is not used (paraphrased from Kerr, 2000).

ECHELON

The ECHELON system, although publicly denied, is believed to be the most comprehensive communications surveillance network in the world. It is controlled by a group of countries, the core five being the United States of America, Canada, the United Kingdom, Australia and New Zealand. This intelligence network is believed to have been instigated by the US, and solidified through the so-called "UKUSA Alliance" (Cyber

Rights & Cyber Liberties, 2000). Based on this agreement, the five core nations participate in a global surveillance network, where each collection station automatically processes communication signals and passes collected samples on to interested nations. This filtering and processing is performed via complex 'Dictionaries' that are based on keywords and powerful artificial intelligence algorithms (Poole, 2000). It is believed that the primary targets of ECHELON are personal and commercial communications (as opposed to military targets of any kind).

ii. United Kingdom

The UK's primary legislation dealing with the interception of communications is the *Regulation of Investigatory Powers Act 2000*. In the first section of this legislation, (Chapter 1 of Part 1), interception of communications is discussed in relation to law enforcement procedures and regulations. The Act covers the situations and restrictions under which LEAs may obtain a warrant to intercept communications, and where they may intercept without a warrant. This legislation is similar to that of the US and Australia, in that generally interception may not take place without a written warrant. The UK has not pursued interception capabilities to the extent of the US (as in the *USA PATRIOT Act*), leaving their legislation based on normal domestic operations, rather than making modifications due to major disturbances to the normal way of life.

iii. New Zealand

New Zealand's *Crimes Act 1961* has provisions for the application to a judge for a warrant to intercept private communications, only in the cases of either organised crime or serious violent offences (Part 11A). The *Government Communications Security Bureau Act 2003* also covers communications interception (Part 3), however this only allows warrants to be granted for the interception of communications in relation to foreign citizens, not New Zealanders. New Zealand does not appear to have made any modifications to their legislation in this area, so the situation should remain than only quite serious offences may justify the issuance of a warrant.

These legislative samples have only been taken from other well-developed nations who seem to make use of the Internet heavily. Most notable are the United States and the United Kingdom. The *USA PATRIOT Act* appears to be the most invasive and far-

reaching legislation amongst the countries reviewed, giving US LEAs far more power to intercept and interpret personal communications in the name of law enforcement.

5. Current Relevant Australian Legislation and Operations

There are already a number of legislative documents in place within Australia, which govern the interception and use of internet-based communications. Following are brief analyses of those documents and their particular effects on the privacy of Australians.

i. Telecommunications (Interception) Act 1979

The *Telecommunications (Interception) Act 1979* provides the avenues required for law enforcement agencies such as ASIO, federal police and state police to monitor the communications of citizens believed to be involved in "activities prejudicial to security". Citizens are considered to be "involved in an offence" if they are "suspected on reasonable grounds of having committed, of committing, or of being likely to commit, the offence" (Sec. 6B). This flexibility allows law enforcement agencies to obtain a warrant to intercept the communications of someone who is *suspected* of being involved in an offence, without real evidence. Since its inception in 1979, the *Telecommunications Interception Act* has been amended either directly or indirectly (through amendment of related legislation) no less than 50 times (Notes to the Act). These changes indicate that the Act is in a constant state of flux, and is likely to continue to be so, due to the changing nature of the subject (communications technologies) to which it relates. One of the most recent amendments, the *Telecommunications (Interception) Legislation Amendment Act 2002*, acted to refine the definitions of certain parts of the legislation, and to expand powers in areas such as terrorism investigations and child pornography. These emerging new areas exposed weaknesses in the legislation, which were countered by increasing the power of LEAs in these matters. This is a relatively positive indication that Australia is willing to modify its legislation to keep up to date with changes in the environment.

ii. Telecommunications Act 1997

The *Telecommunications Act 1997* governs the operation and responsibilities of telecommunications providers within Australia, including their obligations to assist LEAs in investigations. Part 14 of the Act defines issues in relation to "National interest matters", and covers the provision of interception services and the rendering of "such help as is reasonably necessary" to enforce criminal law, protect public revenue and safeguard national security. This legislation applies to telephone system operators, Internet Service Providers and indeed all 'carrier service providers' which appears to include suppliers of all forms of communication from any point to any other point (via any number of points), where any of those points exists within Australia. This effectively means that all suppliers of all forms of communication services within Australia are under legislative requirement to provide the ability to intercept communications over their networks to LEAs when appropriate.

iii. Australian Security Intelligence Organization Act 1979

Enacted in the same year as the *Telecommunications (Interception) Act 1979*, the *Australian Security Intelligence Organization Act 1979* defines the roles, responsibilities and powers of ASIO. Of specific interest to this report are Sections 25A and 26 in Division 2 of the Act (Special Powers). These sections cover computer access warrants and the use of listening devices, respectively. In Section 26, ASIO is given the power to "use a listening device for the purpose of listening to or recording words, images, sounds or signals communicated by or to" a target person. The inclusion of "words, images, sounds or signals" indicates that this power would extend to computer/internet-based communications, and there doesn't appear to be any restriction on future technologies which would most likely be based on one of these communicative mediums.

iv. Cybercrime Act 2001

In 2001, the *Cybercrime Act 2001* was passed to allow for amendments to the *Criminal Code 1995*, repealing previous offences in relation to computer crime, replacing them with expanded definitions, new offences and "enhanc[ing] investigation powers relating to the search and seizure of electronically stored data". The Cybercrime Act defines penalties ranging from 2 to 10 years imprisonment, based on the seriousness of the offence. It covers such acts as the unauthorised modification of data to cause

impairment, unauthorised impairment of electronic communication and possession or control of data (including programs) with the intent to commit a computer offence. This last offence is particularly broad in that a penalty of up to 3 years imprisonment can be applied to someone who is in possession of an electronic tool that *may* be used to commit a crime, if an LEA could prove they had intent to commit such an act. This could potentially mean that a person with a copy of Notepad installed on their computer (installed by default on all Windows-based computers) could be charged with possessing potentially harmful data, since Notepad can easily be used to write malicious code. This Act provides adequate justification for domestic signal interception and analysis, in the name of law enforcement. With a new suite of 'cybercrimes' to investigate and prosecute in relation to, LEAs would certainly require the ability to intercept internet-based communications.

Clearly, legislation already exists within Australia in relation to the use of computers to access the Internet, to communicate via the Internet, and to intercept those communications. Given the perceived privacy of those communications (Frankel, M. & Siang, S. 1999, pp. 7) and known concerns over their privacy (as voiced by individuals, lobby groups and the press), it is not surprising that organizations such as EFA have proven to be popular and powerful within Australia (more about EFA in the following section).

6. Personal Privacy Concerns and Actions

Given the relatively invasive nature of communications interception and wiretapping, the public has strong opinions relating to the preservation of their privacy and their ability to communicate with others in confidence. These concerns must continually be balanced against the need for LEAs to be able to perform their functions in investigating and prosecuting criminal activity. Following is a summary of the groups who are raising concerns in relation to personal privacy, electronic surveillance and communications interception, with some of the issues they are raising.

i. Press Coverage

Personal privacy, surveillance and related issues are regular appearances in Australian commercial press. Regular articles discussing legislative changes and recent

developments, generally in a negative light, appear in state and national publications to remind Australians of the existence (and details) of the legislations that governs their lives. Dearne's *Backlash on spy powers* (2003), discusses growing public opposition to new legislation being enacted around the world, while her article *How governments spy on us* (2001) discusses the ECHELON network and the surveillance tactics of governments.

An example of commercial press coverage portraying government telecommunications interception in a positive light is a rare thing indeed. *How governments spy on us* suggests possible benefits from a global surveillance system such as ECHELON (catching terrorists), but is very quick to point out that in the case of the September 11 attacks, it outright failed. With this being one of the only avenues of education for a large portion of the public in regards to these issues, it is not surprising that they hold a relatively negative opinion about the topic.

ii. Public Opinion/Surveys

According to a poll completed by The Roy Morgan Research Centre in late 1999, 56% of Australians were "worried about invasion of privacy issues created by new information technologies". The poll asked respondents to rate their response to the statement "I'm worried about invasion of my privacy through new technology" on a scale ranging from 'Strongly Agree' through to 'Strongly Disagree'. Further breakdown of the results reveals:

> Farm owners (77%) and skilled workers (60%) were the most likely occupational groups to agree or strongly agree with the statement, while professional/managers (50%) and those not employed (55%) were the least likely to be worried about invasion of privacy through new technology.

This poll appears to be indicative of the public opinion of Australians in 1999, however there hasn't been a similar poll conducted since then, in a time when attitudes towards intelligence agencies, national security and surveillance have changed significantly in both business and personal spheres (DeWeese, 2003).

iii. Electronic Frontiers Australia

The EFA is perhaps the most active and prolific political lobby-group and activist organization within Australia targeting privacy issues specifically in relation to the Internet and computer users. Their official objectives include reference to promoting and protecting civil liberties of computer users, and educating "the community at large about the social, political, and civil liberties issues involved in the use of computer based communication systems" (Electronic Frontiers Australia's Objectives, Updated 2002).

Also within EFA's objectives is a statement regarding their intention to "[t]o research and advise on the application of the law (both current and proposed) to computer based communication systems and related technologies". It is with this in mind that they have issued a number of statements directed at policy-makers and legislative bodies in recent years, including a number relating to privacy and surveillance concerns. Recent submissions have included discussions about federal cybercrime investigation and prosecution procedures and a proposed Code of Practise for ISPs. Both of these submissions included comments on communications interception or surveillance issues, which relate directly to existing or proposed legislation.

In their *Inquiry into recent trends in practises and methods in Cybercrime* (2003), the EFA discuss proposed changes to legislation "seeking to remove the existing requirement that law enforcement agencies obtain an interception warrant prior to accessing the content of email, SMS and voice mail messages". Their concerns centre on amendments to legislation that would allow LEAs to access data which is stored or delayed in transit with no warrant whatsoever. This stems from the following situation:

> S282(1) and (2) of the Telecommunications Act permit carriers and carriage service providers (including ISPs) to disclose documents and information to agencies on request (without a warrant or even written request) if the service provider considers the disclosure or use is "reasonably necessary" for the enforcement of the criminal law, or the enforcement of a law imposing a pecuniary penalty, or the protection of the public revenue

In an effort to ensure a safe and secure environment for computer users, the EFA reviewed and commented on a proposed *Code of Practice from the Internet Industry Association of Australia* (IIA), issued 21 July 2003. Their comments explored inaccuracies and inconsistencies in the IIA's proposed code, when combined with federal legislation such as the *Telecommunications (Interception) Act 1979* and the *Telecommunications Act 1997*. The IIA appears to be recommending that ISPs act in a manner that would potentially expose them to prosecution due to breaches of the two Telecommunications Acts, as well as the *Privacy Act 1988*.

The existence of lobby groups such as the EFA is a critical part of ensuring that both LEAs and the personal privacy of citizens is protected in the creation and enactment of legislation within Australia. The country is currently reasonably well represented, and should remain so if the EFA and partner organizations can maintain their momentum. Even internationally, they are acclaimed for their work here and for the accolades they have achieved (as in Oram, 1998).

7. Summary Of Issues

Australia's current position in relation to online privacy and legal communications interception appears to be stable and consistent with similarly developed countries throughout the World. Our laws are relatively conservative when compared to those such as the United States' *USA PATRIOT Act*, while being more defined and specific than New Zealand's *Crimes Act 1961*. Australia's continuous amendments to legislation such as the *Telecommunication (Interception) Act 1979* are a positive indication of a desire to ensure that new developments in technology (and indeed society and social practises) are catered for in the laws of the country. This will need to continue in the coming years when there are more advances in digital technologies, especially in the emerging fields of wireless networking and personal area networks (networked devices such as smart phones, personal digital assistants, cameras and wristwatches), which will no doubt be subjected to regulations and legislation of their own.

Lobby groups such as Electronic Frontiers Australia provide a valuable voice to the concerns of the public in the political and legislative process, which is possibly missing in some other countries, giving us a chance to have the citizens of the country represented

in the process that governs the laws that will govern them. Provided the EFA can maintain its position and apparent political power, it will be well-placed to represent the public in the future, when its role will become increasingly important.

Given the extremes of an Orwellian state of surveillance, or a free-for-all where LEAs have no power to perform their duties in the digital world, Australia appears to be comfortably seated towards the middle of the spectrum. The coming years will reveal just how difficult it is to maintain that position, but if the current balance can be maintained, then Australia's citizens and LEAs should continue to co-exist in relative peace.

8. References

Note: The following abbreviations have been used to indicate the countries to which certain legislative documents belong;

AU = Australia

NZ = New Zealand

UK = United Kingdom

US = United States of America

Cassidy, D. (1999). *Submission to the Parliamentary Joint Committee on Review of the Australian Security Intelligence Organization (ASIO) Legislation Amendment Bill 1999.* Retrieved November 22, 2003, from http://www.efa.org.au/Publish/ASIObillsubm99.html

Council of Europe: Convention on Cybercrime. (2001). Retrieved November 20, 2003, from http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Crimes Act 1961 (NZ). (1961). Retrieved November 24, 2003, from http://www.legislation.govt.nz/libraries/contents/om_isapi.dll?clientID=844517745&advquery=interception&infobase=pal_statutes.nfo&record={A899A64A}&softpage=DOC&wordsaroundhits=6#JUMPDEST_JUMPDEST_

Cybercrime Act 2001. (AU). (2001). Retrieved November 22, 2003, from http://scaleplus.law.gov.au/html/pasteact/3/3486/top.htm

Cyber-Rights & Cyber-Liberties. (UK). (2000). *Interception Capabilities 2000 Report.* Retrieved October 20, 2003, from http://www.cyber-rights.org/interception/stoa/ic2kreport.htm

Dearne, K. (2001). How governments spy on us. *The Australian,* 33, Tuesday September 25.

Dearne, K. (2003). Backlash on spy powers. *The Australian*, 4, Tuesday September 16.

DeWeese, T. (2003). *Total Surveillance Equals Total Tyranny.* Retrieved November 24, 2003, from http://www.intellectualconservative.com/article2597.html

Electronic Frontiers Australia. (Updated 2002). *EFA's Objectives.* Retrieved November 23, 2003, from http://www.efa.org.au/AboutEFA/object.html

Electronic Frontiers Australia. (Updated 2002). *General Information About EFA.* Retrieved November 15, 2003, from http://www.efa.org.au/AboutEFA/

Electronic Frontiers Australia. (2003). *Inquiry into recent trends in practises and methods in Cybercrime.* Retrieved November 20, 2003, from http://www.efa.org.au/Publish/efasubm-acc2003.html#intercept

Frankel, M. S., & Siang, S. (1999). *Ethical And Legal Aspects Of Human Subjects Research On The Internet.* Retrieved November 9, 2003, from http://www.aaas.org/spp/sfrl/projects/intres/report.pdf

Government Communications Security Bureau Act 2003 (NZ). (2003). Retrieved November 23, 2003, from http://www.legislation.govt.nz/libraries/contents/om_isapi.dll?clientID=844517745&infobase=pal_statutes.nfo&jd=a2003-009%2fs.14&record={22C98868}&softpage=DOC&wordsaroundhits=6

Intelligence Services Act 2001. (AU). (2001). Retrieved October 20, 2003, from http://scaleplus.law.gov.au/html/pasteact/3/3483/top.htm

Kelley, J. (2001). Terror groups hide behind Web encryption. *USA Today.* Retrieved November 24, 2003 from http://www.usatoday.com/tech/news/2001-02-05-binladen.htm

Kerr, D. M. (2000). *Statement for the Record on Carnivore Diagnostic Tool.* Retrieved October 20, 2003, from http://www.fbi.gov/congress/congress00/kerr090600.htm

Morgan Poll (1999). *"Big Brother"; Bothers Most Australians*. Finding No. 3221. Retrieved November 22, 2003, from http://oldwww.roymorgan.com/polls/1999/3221/

Oram, A. (1998). *In Australian Battle, Privacy Advocates Won't Back Away*. Retrieved November 22, 2003, from http://www.praxagora.com/andyo/ar/privacy_australia.html

Poole, P. S. (2000). *ECHELON: America's Secret Global Surveillance Network.* Retrieved October 20, 2003, from http://fly.hiwaay.net/~pspoole/ECHELON.html

Regulation of Investigatory Powers Act 2000. (UK). (2000). Retrieved November 23, 2003, from http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Telecommunications Act 2001. (NZ). (2001). Retrieved October 20, 2003, from http://www.legislation.govt.nz/libraries/contents/om_isapi.dll?clientID=339357511&infobase=pal_statutes.nfo&record={1BDB8FB6}&hitsperheading=on&softpage=DOC

Telecommunications Act 1997. (AU). (1997). Retrieved November 23, 2003, from http://scaleplus.law.gov.au/html/pasteact/2/3021/top.htm

Telecommunications (Interception) Act 1979. (AU). (1979). Retrieved November 22, 2003, from http://scaleplus.law.gov.au/html/pasteact/0/464/0/PA000370.htm

Telecommunications (Interception) Legislation Amendment Act 2002. (AU). (2002). Retrieved November 24, 2003, http://scaleplus.law.gov.au/html/comact/11/6501/top.htm

Telecommunications (Lawful Business Practise) (Interception of Communications) Regulations 2000. (UK). (2000). Retrieved October 20, 2003, from http://www.hmso.gov.uk/si/si2000/20002699.htm

United States of America Code, Title 47, Chapter 9, Subchapter I. Sec. 1002. (US). (n.d.). Retrieved November 24, 2003, from http://www4.law.cornell.edu/uscode/47/1002.html

United States of America Code, Title 18, Part I, Chapter 119, Sec. 2516. (US). (n.d.). Retrieved November 18, 2003, from http://www4.law.cornell.edu/uscode/18/2516.html

USA PATRIOT Act, 2001. (US). (2001). Retrieved November 23, 2003, from http://www.epic.org/privacy/terrorism/hr3162.html