Assignment 1

Research Proposal

Choose an area of Internet governance which interests you and provide a 1000-word research proposal to explore the issue further.

Name: Beau Lebens
Student Number: 09918322
Unit Name: NET23
Email Address: beau@dentedreality.com.au

Date Submitted: 22 October 2003
Word Count: 1,080

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.

Cyber-Interception Capabilities: Legislation For Today and Beyond

Proposed Project

With the Internet proving itself to be a core part of business, personal and political life within Australia, law enforcement agencies must ensure that they are well-equipped to deal with the requirements placed on them to investigate and access details regarding people's behaviour online. It is recommended that a detailed comparative-analysis of current local and international legislation relating to the interception and analysis of Internet-based communications needs to be performed. This will ensure that Australia is keeping in step with the rest of the world and is well placed to move forward. It will also help identify any areas of legislation which are lacking, or which are too strict and may harm business, privacy or personal freedoms within the country.

Definitions

For the purpose of this proposal, the following terms are defined:

AHTCC

> The Australian High Tech Crime Centre is a joint effort between the police agencies of all of Australia's states and territories. Their aim is to provide a cohesive approach to the investigation of cross-jurisdictional, technology based or aided crimes within Australia.

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 and must be physically installed on a network segment to be operational (http://www.fbi.gov/congress/congress00/kerr090600.htm).

DSD

> The Defence Signals Directorate is Australia's primary electronic telecommunications expert facility. The DSD processes and analyses communications in relation to 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 the USA, UK, Australia, New Zealand and Canada) (http://fly.hiwaay.net/~pspoole/echelon.html).

Packet Sniffing

Packet sniffing is the practice of intercepting all traffic (packets) passing through a network and either saving or temporarily analysing the contents of the packets.

SCALEplus

A public access, searchable, online database containing all federal legislation within Australia.

Background

Given the current global reliance upon the Internet and emerging, related technologies for business, personal and political communications and data transfers, law enforcement agencies are coming under increasing pressures to ensure that they have the ability to adequately investigate suspects who may also be using these methods of communication. Legislation is already in place in a number of countries around the world including, but not limited to, the United States of America (http://www4.law.cornell.edu/uscode/47/ch9schI.html), the United Kingdom (http://www.hmso.gov.uk/si/si2000/20002699.htm), and Australia itself (http://www.aca.gov.au/aca_home/licensing/radcomm/about_radcomms_licensing/law_enforcement.htm). With these and other policies already existing, it is imperative that Australia moves forward to ensure that our businesses and citizens are on an equal footing with our international partners, and that the privacy and freedom of our constituents are maintained, while allowing law enforcement agencies to effectively perform their duties in the areas of electronic investigation and forensics.

The global security climate has changed significantly since the September 11 terrorist attacks in the United States and more recently, the Bali Terrorist Attacks in October

2002. Since those events, a number of legislations have been introduced or amended around the world, including but not limited to Australia's *Intelligence Services Act 2001* (http://scaleplus.law.gov.au/html/pasteact/3/3483/top.htm), the United States' *Executive Order 13231 -- Critical Infrastructure Protection in the Information Age* (http://www.ncs.gov/ncs/html/eo-13231.htm) and New Zealand's *Telecommunications Act 2001* (http://www.legislation.govt.nz/libraries/contents/om_isapi.dll?clientID=339357511&infobase=pal_statutes.nfo&record={1BDB8FB6}&hitsperheading=on&softpage=DOC). These and other legislations and amendments give government and law enforcement agencies more power to intercept, decode and analyse the communications taking place over the Internet. These powers need to be carefully balanced with the desire to maintain a relatively high level of personal freedom and privacy within Australia, and to ensure that our businesses and corporations are able to compete internationally on even terms.

Considerations

The following considerations (in no particular order) will be of direct importance in this analysis of existing and proposed legislation;

1. Maintaining personal privacy and freedom both physically and on the Internet for the citizens and businesses of Australia;
2. Allowing businesses to continue to operate on an even playing field with international partners and competitors;
3. Providing law enforcement agencies with the tools and abilities they require to effectively complete investigations into the actions of suspects of terrorism, cyber-crime and other criminal activities online;
4. Existing infrastructure and legislation (both local and international), and how it relates to, or is excluded from discussions of new and existing legislation;
5. Bringing Australia into line with partner nations such as the United States, New Zealand, Canada and the United Kingdom (as per the "UKUSA Alliance" http://www.cyber-rights.org/interception/stoa/ic2kreport.htm#_Toc448565515); and
6. Avoiding the creation of a 'surveillance society' where civilians are of the impression that they are under constant scrutiny in their daily activities.

Methods/Resources

Given the nature and scope of the project, it is suggested that the Internet itself will be the most valuable research tool available. Initial data mining reveals resources such as SCALEplus (http://scaleplus.law.gov.au/), which contains in particular the *Intelligence Services Act 2001* (http://scaleplus.law.gov.au/html/pasteact/3/3483/top.htm) and the *Telecommunications (Interception) Act 1979* (http://scaleplus.law.gov.au/cgi-bin/download.pl?/scale/data/pasteact/0/464), amended in 1997.

Other online resources such as heavily researched reports written relating to Echelon (http://fly.hiwaay.net/~pspoole/echelon.html) and Congressional Statements on Carnivore (http://www.fbi.gov/congress/congress00/kerr090600.htm) will also aid in this project. There are websites for existing agencies in Australia such as the AHTCC (http://www.ahtcc.gov.au/), DSD (http://www.dsd.gov.au/) and the Australian Communications Authority (http://www.aca.gov.au/), which provide valuable information about existing laws and regulations.

Where appropriate, legal libraries and other offline sources may also be required to provide a complete picture of the current state of legislation on the topic.

Drawing similarities to other nations, it is proposed that a report be prepared outlining the current legislation in the field of communications interception and analysis, both within Australia, and abroad, and that the report be used to determine what additional (if any) legislation is required. Based on the recommendations of this report, changes to existing laws may be required to ensure that privacy and freedom are protected, while terrorism and cyber-crime are prevented and combated to the best of our abilities.

Intended Outcome

A report will be produced outlining the current legislation around the world and within Australia, in relation to the topics of telecommunications interception and analysis. This report can be used to guide decisions around the amendment or addition of future legislation.

References

Australian Attorney Generals Department. (n.d.). *Telecommunications (Interception) Act 1979.* Retrieved October 20, 2003, from http://scaleplus.law.gov.au/cgi-bin/download.pl?/scale/data/pasteact/0/464

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

Australian Communications Authority. (2003). *Telecommunications and Law Enforcement.* Retrieved October 20, 2003, from http://www.aca.gov.au/aca_home/licensing/radcomm/about_radcomms_licensing/law_enforcement.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

Executive Order 13231 -- Critical Infrastructure Protection in the Information Age. (2001). Retrieved October 20, 2003, from http://www.ncs.gov/ncs/html/eo-13231.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

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

Telecommunications Act 2001. (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

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

United States of America Law, Title 47, Chapter 9, Subchapter I. (n.d.). Retrieved October 20, 2003, from http://www4.law.cornell.edu/uscode/47/ch9schI.html