THE IMPACT OF SECURITY CONCERNS ON CYBER LIBERTIES

Julie Cameron and David Vaile
Julie Cameron is with Info.T.EC Solutions Pty Ltd, Sydney, Australia, infotec_solutions@yahoo.com.au and Vaile is with Baker & McKenzie Cyberspace Law & Policy Centre, Faculty of Law, University of NSW, Sydney, Australia, d.vaile@unsw.edu.au

Abstract: Case studies from Australia, Canada, United Kingdom and USA are used to illustrate the impact of the "war on terrorism" on cybercitizens. The authors use relevant Articles of the *Universal Declaration of Human Rights* as a benchmark against which to assess new and changed legislation in democratic societies. It is proposed that "Principles of Cyber Liberty" be articulated within the framework of the *Universal Declaration of Human Rights* by providing adjuncts to the relevant Articles to clarify the application of these liberties and rights in cyberspace, and the potential conflicts between these rights and the new "war on terrorism" initiatives.

1. INTRODUCTION

The attack on the World Trade Centre in New York on 11 September 2001 was a shocking assault on civilians in a country that was not at war. It has resulted in extraordinary impacts on the lives of citizens throughout the world. Some impacts were a direct response to the events and could reasonably be expected (e.g., increased security around key buildings) but other consequences resulting from government reaction appear only indirectly related to the attack and/or can be described as opportunistic and unjustified.

The declaration of war on terrorism by many nations and United Nations' Security Council Resolution 1373 has resulted internationally in

governments demanding increased surveillance of cyberspace[1], global intrusion and claims for jurisdiction outside national territories which threaten the liberties and rights of cybercitizens. The challenge for both citizens and cybercitizens is to understand the consequences of these demands and to limit or reduce any harm, including impacts on their liberties.

This paper which is developed from an extended abstract entitled 'The War on Terrorism versus Cyber Liberties' published in the conference proceedings[2] of the Second International Summer School organized by IFIP-WG9.2 & 9.6/11.7, presents brief case studies that examine legislative reactions to the war on terrorism and outcomes in Australia, Canada, United Kingdom and the USA. The United Nations *Universal Declaration of Human Rights* has been adopted as a benchmark to assess the appropriateness of this legislation because it provides an ethical and legal framework that is generally accepted as a definitive statement of the expectations citizens should have of their government. The authors focus on the consequences of the new legislation for cyber liberties. Currently "Principles of Cyber Liberty" have not been adopted internationally. Increased surveillance of cyberspace, global intrusion and claims for jurisdiction outside national territories threaten the liberties and rights of cybercitizens.

2. CASE STUDIES

2.1 Australia

The Australian government moved fast. Immediately after the attack the Commonwealth Parliament (comprising the House of Representatives and Senate) passed a raft of Acts related to security and border protection including the:

[1] "Cyberspace" is defined as "the electronic environment established by and/or within the information and communications technologies and infrastructure and associated peripheral equipment".

[2] Fischer-Hubner, Simone (editor) August 4-8, 2003, "Risks and Challenges of the Network Society", Proceedings of the Second International Summer School organized by IFIP-WG9.2 & 9.6/11.7 published by Karlstad University. This subsequent paper is published with the permission of the editor and publishers.

- *Migration Legislation Amendment Acts 2001*[3] – changes include authorising an airline operator, shipping operator, travel agent or proscribed organisation to disclose information from their databases about any matter relating to travel by persons to or from a migration zone to an officer, even if information is personal as defined in the *Commonwealth Privacy Act 1998.*
- *Measures to Combat Serious and Organised Crime Act 2001*[4] - changes include exempting law enforcement officers and authorized persons from criminal liability for offences committed in the process of an operation for the purposes of obtaining evidence (including electronic material) that may lead to the prosecution of a person for a serious offence (including threats to national security punishable by imprisonment for 3 years or more).
- *Intelligence Services Act 2001*[5] – changes include expanding the functions and services of the Australian Security and Intelligence Service (ASIS) and Defence Signals Directorate to include intelligence and counter intelligence (in the form of electromagnetic, electric, magnetic or acoustic energy) within and outside Australia.

At the time these laws were passed, Australia was in the midst of both an election campaign and controversy over immigration and "illegal" boat people. There was no time for public debate.

Justified by United Nations Security Council Resolution 1373, the following additional legislation was passed by House of Representatives in March 2002:

- Security Legislation (Terrorism) Act 2002 (No 2) [6]
- Suppression of the Financing of Terrorism Act 2002[7]
- Criminal Code Amendment (Suppression of Terrorist Bombings) Act 2002[8]
- Border Security Legislation Amendment Act 2002[9]
- Telecommunications Interception Legislation Amendment Act 2000[10].

[3] http://www.austlii.edu.au/cgi-bin/disp.pl/au/legis/cth/num_act/mlaormsa2001n332001709/
[4] http://www.austlii.edu.au/au/legis/cth/consol_act/mtcsaoca2001436/index.html
[5] http://www.austlii.edu.au/au/legis/cth/consol_act/isa2001216/index.html
[6] http://scaletext.law.gov.au/html/comact/11/6499/top.htm
[7] http://scaletext.law.gov.au/html/pasteact/3/3496/top.htm
[8] http://scaletext.law.gov.au/html/comact/11/6497/top.htm
[9] http://scaletext.law.gov.au/html/comact/11/6498/top.htm
[10] http://scaletext.law.gov.au/html/comact/11/6501/top.htm

Members of the Senate referred the Bills to Senate Legislation Committee (a body of 6 senators from the main political parties represented in Parliament). Despite a short one weeks notice period for the public, 431 public submissions were received in writing by 19 April and/or put verbally to a public hearing in Sydney on 1 May (Senate Consideration, 2002).

Key adverse provisions of Australian bills identified in the submissions that relate to cybercitizens and the online domain [1] were:

- Reversal of the traditional criminal onus of proof from "innocent until proven guilty", and removal of the need of the prosecution to prove "intent" to commit a deed, including for online activities. This reversal combined with broad definitions of "terrorist" and "terrorist acts" including online actions would have also make it easier to use digital evidence.
- Overruling of Information Privacy Principles of *Privacy Act* 1988 (e.g., collection, retention, use of personal data).
- Contravention of *Telecommunications (Interception) Act* 1979 (that provided protections against interception of communications passing over a telecommunications system without the knowledge of the person making the communication – subject to exceptions related to law enforcement).
- Power for one government Minister to "proscribe" an organization, and power to imprison any individual for life for supporting such organizations. This included online communications and accessing websites.
- Immunity for law enforcement officers from civil and criminal liability for breaches of privacy and data protection and other authorized activities provided a warrant has been obtained.
- Additional powers to ASIS (Australian Secret and Intelligence Service[11]) including the power to move and retain things and records (e.g., computers and files).
- Creation of an offence making it illegal to provide information (including emails and electronic documents) related to security and defence, and removal of the need to prove a recipient knew or had grounds to believe information involved a breach of official secrets.
- Permission to refer financial information and personal information to foreign nations.

[11] http://www.asis.gov.au/

As a result of arguments from the public, the *Report of the Senate Legal and Constitutional Legislation Committee* May 2002 recommended the Bills [2] be amended to provide:

- Requirements for tighter definitions to restrict offences (e.g., "conduct that assists", "terrorist act") and for an "intention" for an act to cause (not just "involve") serious harm.
- Removal of "absolute liability" for "terrorist acts" and presumption of guilt (reversal of presumption of innocence and onus of proof for criminal offences).
- Limitations to the right of the Attorney-General to "proscribe" organizations with terrorist connections.
- Review of the provisions of the Bills that provide access by agencies to stored communications or delayed message services by "search warrant" or "seizure order" (may be issued administratively) rather than by a "telecommunications interception warrant" (which requires judicial approval).

2.2 Canada

Like Australia, the Canadian Government quickly passed "anti-terrorist" legislation.

Bill C-36 was passed in December 2001 with very broad definitions of 'unlawful activity' and 'groups', which was watered down after protest [3, p139]. In addition to restrictions to civil liberties, this bill as passed in December 2001 provides for:

- The Attorney General of Canada to issue certificates to prohibit disclosure of information related to international relations, defence or security – after a proceeding and subject to review of a judge of the Federal Court of Appeal.
- Restrictions related to computing networks and cyberspace.

Amendments to the Criminal Code place restrictions on content and give power to the court to subpoena copies of electronic material and to a judge to determine whether content can be considered as "hate speech".

Bill C-55, and its replacement the Bill C-17, Public Safety Act 2002, (which lapsed at the end of the Parliamentary session) included controversial provisions like:

- Power to share passenger lists among security agencies and federal departments for restricted purposes (eg transportation security).
- Establishment of "controlled access military zones" on grounds of protection of international relations, defence or security [3, p142].
- Due to strong opposition the government did not proceed to pass the legislation.

Significantly it was reported on CNET News.com, August 27, 2002 that "the Canadian government is considering a proposal that would force Internet providers to rewire their networks for easy surveillance by police and spy agencies. A discussion draft ... contemplates creating a national database of every Canadian with an Internet account, a plan that could sharply curtail the right to be anonymous online. ..." and "compelling Internet providers and telephone companies to reconfigure their networks to facilitate government eavesdropping and data-retention orders. The United States has a similar requirement, called the *Communications Assistance for Law Enforcement Act*, but it applies only to pre-Internet telecommunications companies.[12]"

2.3 United Kingdom

Key terrorism acts in the UK are the:

- Terrorism Act 2000[13].
- Anti-Terrorism, Crime and Security Act 2001[14].
- Regulation of Investigatory Powers Act 2000.

Following the introduction of the *Regulation of Investigatory Powers Act 2000* security and privacy of communications has become a real concern for Internet users in the UK. The monitoring of communications including interception of content data under the *Regulation of Investigatory Powers Act* 2000, and the retention of communications data under the *Anti-Terrorism, Crime, and Security Act* 2001 can constitute an interference with the right to respect for private life and correspondence in breach of Art. 8(2) of the *European Convention on Human Rights* [4]. UK citizens are to be affected by a proposal whereby 'all telecommunications firms including mobile phone operators and Internet Service Providers will have to keep the

[12] Declan McCullagh, 'Will Canada's ISP become Spies?' CNET News.com, August 27, 2002 http://www.statewatch.org/news/2002/aug/10can.htmUSA

[13] http://www.hmso.gov.uk/acts/acts2000/20000011.htm

[14] http://www.hmso.gov.uk/acts/acts2001/20010024.htm

number and addresses of all calls and emails made and received by EU citizens' for at least a year[15].

There is alleged involvement of the UK Government, a member of both the European Union and the Council of Europe, with the Echelon interception systems. So far, the UK government's preferred practice in relation to the existence and use of Echelon systems has been not to comment on such allegations. However, in September 2001, the European Parliament in a resolution concluded that "the existence of a global system for intercepting communications, operating by means of cooperation proportionate to their capabilities among the US, the UK, Canada, Australia and New Zealand under the UK-USA Agreement, is no longer in doubt."

2.4 USA

As would be expected, the legislators of the USA acted rapidly to tighten security and surveillance after the events of September 11. Major themes were increased surveillance and monitoring of all forms of electronic communication.

The key legislation is the USA is the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act* of 2001[16] "The *USA PATRIOT Act* is a synecdoche for the freedom-for-safety swap. Among many other things, it sanctioned roving wiretaps (which allow police to track individuals over different phones and computers) and spying on the Web browsers of people who are not even criminal suspects. It rewrote the definitions of terrorism and money laundering to include all sorts of lesser and wider-ranging offences. More important, as EFF underscored, 'In asking for these broad new powers, the government made no showing that the previous powers of law enforcement and intelligence agencies to spy on U.S. citizens were insufficient to allow them to investigate and prosecute acts of terrorism.'"17 Not only does it expand the government's power to tap phones, monitor the Internet, conduct 'sneak-and-peak' searches, it even gives the FBI power to force librarians and bookstores to reveal the names of customers.

Michelle Wibisono [5] summarized provisions of the *PATRIOT Act* that contributed to the expansion of surveillance:

[15] Richard Norton Taylor and Stuart Miller, 'Privacy Fears over EU plan to store email' The Guardian Weekly, August 22 2002, p1.
[16] http://www.epic.org/privacy/terrorism/hr3162.html
[17] http://www.reason.com/0210/fe.ng.freedom.shtml

- Terrorism is now included in a list of crimes for which authority is given to intercept wire, oral and electronic communications.
- Routing and addressing information, e[mail] and electronic communications can be obtained on a appropriate Court order, but not the "contents" of the communications.
- The *Electronic Communications Privacy Act* is amended to expand the classes of records that can be sought without a court order including cables.
- Internet service providers and other telecommunications providers can voluntarily disclose to the government both content and customer records if there is reason to believe the emergency involves danger of death or serious physical injury.
- Foreign intelligence gathering needs only to be a "significant purpose" of surveillance to invoke powers under the *Foreign Intelligence Surveillance Act* 1978 (FISA).
- Increased disclosure of surveillance or intelligence (whether foreign or not) evidence to State agencies involved in intelligence or national defence or security is permitted.

Extraordinary power to utilize biometrics, including fingerprint, voice recognition, face recognition and retinal scanning has been implemented.

> "A measure was introduced in the Virginia legislature requiring a judge's approval to use FRT... Then the terrorists attacked, and everything seemed to change. The Virginia legislature dropped the bill requiring judicial approval."[18]

eBusiness has also been affected by security concerns. "Much of the past decade has been spent opening up databases ... through ... data warehouses ... and Internet-enabled B2B (business to business) exchanges. It's already evident that terrorists can buy a plane ticket with a credit card via Internet travel sites; ... the chemical industry is now examining its B2B exchanges to ensure that their security systems and business practices will prevent terrorists from using such 'anonymous' marketplaces to purchase materials for chemical or biological attacks". [6, p81-82]. Reflecting these concerns *Cyber Security Enhancement Act*, US House of Representatives passed July 15 2002 increases penalties for hackers up to life imprisonment. [19]

[18] http://www.reason.com/0210/fe.dk.face.shtml

[19] Ira Slager, "CyberSleaze", Australian Financial Review, September 14 p.44

Cyberspace surveillance has been intensified. Yourdon reports significant increase in the use and retention of computer logs and audit trails. "Inevitably the (huge volume of logging data) will lead to greater emphasis on spotting patterns of behaviour in order to spot security threats after they have occurred, or (ideally) before they have occurred. ... We'll see greater efforts to combine public sector and private sector trend analysis efforts." Search engines may become another focus of concern: "Much of the necessary information about the type, location, and vulnerabilities of critical infrastructure systems needed to organize and launch a serious attack is already available on the Internet."[20]

3. BENCHMARK: THE UNIVERSAL DECLARATION OF HUMAN RIGHTS

The case studies show the adverse affects of government reaction to the war of terrorism in societies considered "democratic". We can measure these impacts of legislation presented in the case studies against an internationally ratified set of standards – the UN *Universal Declaration of Human Rights*.[7] The relevant Articles that have been breached are:

Article 11

1. Everyone charged with a penal offence has the right to be presumed innocent until proved guilty according to law in a public trial at which he has had all the guarantees necessary for his defence.
2. No one shall be held guilty of any penal offence on account of any act or omission which did not constitute a penal offence, under national or international law, at the time when it was committed. Nor shall a heavier penalty be imposed than the one that was applicable at the time the penal offence was committed.

Article 12.

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

[20] J Hernandez, Sierra and Ribagorda 'Search engines as security threat?', IEEE Computer, Oct. 2001, p.25, in Yourdon p.109.

Article 13

1. Everyone has the right to freedom of movement and residence within the borders of each state.
2. Everyone has the right to leave any country, including his own, and to return to his country.

Article 19

Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Article 20

1. Everyone has the right to freedom of peaceful assembly and association.
2. No one may be compelled to belong to an association.

The concern is that, in their response to the recent terrorist events, most governments that have ratified these Articles appear to have ignored or constrained these clearly stated and recognized rights – with apparent impunity.

4. IMPLICATIONS FOR CYBER CITIZENS

Significantly, the implications for cyber citizens appear to be not fully understood by either the governments concerned or the users of cyberspace. The result is:

- Decreased human rights, civil liberties and cyber liberties[21] including reduced freedom of speech and association and presumption of innocence.
- Significantly increased use of surveillance.
- Increased willingness of citizens to trade civil liberties for security.
- Increased opportunity for security and administrative "function creep" related to government activities including those related to the online domain.
- Increased move to self censorship by citizens and cyber citizens.

[21] Cyber Liberties are defined as "the extension of the rights stated in the Declaration of Human Rights to cyberspace".

The key implications for cyber citizens (not in order of importance) are:

1. Creation of new offences that apply outside the country of citizenship.

The new offences with which cyber citizens may be charged are not necessarily those within the country of citizenship. Major issues relate to what is "connected" in cyberspace and which jurisdiction should apply at any time for example, in relation to:

- Disruption or destruction of ICT systems and infrastructure. How will e-protest and "hacktivism" be viewed by different jurisdictions?
- Possession or creation of documents related to or connected with terrorism or proscribed organizations. Presumably each government will retain its own list of proscribed organizations that will not necessary be known by their own citizens let alone cyber citizens from other countries. Some offences created may relate to:
  Receipt of emails (solicited or unsolicited)
  Access to "proscribed" websites (knowingly or unknowingly)
  Access to "proscribed" chat sites (knowingly or unknowingly)
  Membership of, or connection with proscribed "groups"
  "Misuse" of services, without knowledge of offence.

2. Incursions into rights to "privacy" for citizens and non-citizens.

These incursions include the transfer of personal data outside national borders. Governments are claiming the right to:

- Access intelligence (including in electronic form) related to capabilities, activities or intentions of organizations and people outside national borders (Australia – *Intelligence Services Act* 2001 Cth; US – *US Patriot Act*)
- Access "required identity information" from airline reservation systems and lists of ships passengers prior to arrival (Australia – *Migration Legislation Amendment Act* 2001 (No 5) Cth[22]; Canada – *Public Safety Act 2002*)
- Additional sharing of personal data from private and public sectors among agencies at all levels of government (Australia, Canada, UK and USA).

[22] http://scaletext.law.gov.au/html/comact/9/4574/top.htm.

3. Increased powers of defence, security and police organizations to undertake electronic surveillance.

These increased powers include the use of sophisticated "surveillance" technologies and techniques like:

- Data mining, matching and trawling (regardless of errors, mismatches and wrong identifications that result from using these methods).
- Intelligent agents/bots (i.e., just looking!).
- Intelligent contact mapping (i.e., guilt by association).
- Intelligent "rule based" applications (e.g., "suspicious" transactions, key words).
- Powerful ongoing global surveillance of communications (e.g., use of the Echelon systems by the United States, and to a lesser degree by United Kingdom, Canada, Australia and New Zealand to intercept communications).
- Use of system audit and security tools including transaction history and logs.
- Use of systems capabilities regardless of proven need (e.g., mobile phones and global positioning systems).
- Shift from ad hoc monitoring of communications to continual reporting (to gain additional data – just in case).
- Increase in requirements for retention of records and extension of time the archives must be held and made accessible on demand.
- Loss of anonymous transactions.

In some cases the checks on existing powers of defence, security and police organizations have been reduced (e.g., USA and Australia – security agencies need to obtain only an administrative warrant and not a warrant issued by the Court to detain and question people, remove and retain records and things). Even more serious is the granting of immunity from civil and criminal proceedings for unintended consequences of obtaining intelligence. We must ask, "who guards the guardians"?

4. Risk of detention when travelling without appropriate rights of redress or protection of citizenship.

If cyber citizens have committed offences in another country they may not be aware of the risk of apprehension when they enter the territory of jurisdiction. For some, the fear of contravening terrorist laws may lead to caution and failure to act or protest.

Issues of equal concern, particularly to the growing number of cyber citizens, must be the:

- Impossibility of nations to protecting the cyber liberties of their citizens, due to the extra-territoriality of some of the responses.
- The lack of certainty when the laws of more than one jurisdiction may apply.
- Loss or enclosure of the information "commons" which means that cybercitizens are no longer free to use cyberspace and content in their preferred manner.
- Claim by owners of infrastructure to rights to surveillance of users (to avoid misuse).

5. SOLUTIONS

Although the UN *Universal Declaration of Human Rights* was developed prior to the use of the Internet and predates the period known as the "information age", its Articles are expressed in broad terms and in many cases can be reasonably interpreted to cover the events and circumstances encountered by cybercitizens – individuals that use cyberspace[23]. We can establish Principles[24] of Cyber Liberty within the existing framework of the *Universal Declaration of Human Rights* by clarifying the application of the relevant Articles to clearly specify they protect the rights of cybercitizens.

5.1 Principles of Cyber Liberties – Proposed Statement of Rights Based on the UN *Universal Declaration of Human Rights*

1. Right to freedom from electronic and other forms of surveillance and fear of surveillance unless accused under a legitimate law of the country of citizenship or international law, and surveillance is undertaken with appropriate judicial authority obtained from any country affected (Article 12).
2. Presumption of a right to privacy and anonymity in cyberspace (Article 12).

[23] "Cyberspace" is defined as the electronic environment established by and/or within the information and communications technologies and infrastructure and associated peripheral equipment.

[24] Principles are statements that may provide international guidance, or act as a reference document, or provide a basis for the development of legal instruments in particular jurisdictions.

3. Right to free exchange of knowledge, opinion and expression in cyberspace without fear (Article 19).
4. Right of cyber citizens to protest in cyberspace without fear, limited only by proven intent to commit a criminal or terrorist act as defined by a legitimate law of the country of citizenship or international law (Article 19).
5. Right to freedom of association within cyberspace (Article 20).
6. Right to transparency within cyberspace, including the right to know the governing laws of any site (Article 11).
7. Protection from arrest or detention outside the country of citizenship or residency for actions undertaken within cyberspace unless those activities contravene international law (Article 11).
8. Right to trial by country of citizenship or international law and treatment in accordance with the Declaration of Human Rights (Article 11).
9. Right to appropriate representation and knowledge of evidence (Article 11).
10. Right of the data subject to ownership of personal data (Article 17[25]).

6. CONCLUSIONS

Terrorists aim to disrupt and displace ways of life. Over-reaction by governments can ensure they achieve this goal without further effort. A reality check is required. We need to consider a number of issues:

- "Terrorism" is an emotional concept; one that is often selectively applied and dependent on historical and political context. There is a high risk of previously acceptable online activity and use of information and communications technology being stifled without adequate justification.
- Prevention of terrorism requires the causes of terrorism to be addressed. What triggers terrorism? Why are terrorists targeting particular groups? Attempts to suppress it by hyper-vigilance, implementing technologies of universal surveillance and control, may be ineffective and counterproductive to the extent they distract from efforts to address the causes.
- Proportionality and appropriateness of response to threat is imperative. Terrorism is often not 'high tech', and technical responses are not effective (e.g., SMS message: code word 'suit' was used to refer to the payment of bribes to a local councillor in Sydney, Australia; open email messages that avoid key words that could be used by Echelon and

[25] Article 17: (1) Everyone has the right to own property alone as well as in association with others; (2) No one shall be arbitrarily deprived of his property;

surveillance software to trigger 'alerts', were thought to be used by Al Qa'eda; the most successful spy in recent US history used 'dead drops', paper copies of sensitive material in envelopes left for collection by Russian agents!).

- Governments need to consider the lack of success of existing surveillance (e.g., outcomes for the Australian government compared with data collected and scanned under the *Australian Financial Transactions Reporting Act* provisions.) Lack of data is not the key problem in preventing terrorist acts. Recent reviews of security functions in the US and other countries found that bureaucratic and human intervention, and misinterpretation prevented or hindered the use of available information.

Significant intrusions on both civil and cyber liberties have resulted from the war on terrorism. There appears to be growing concern even among the security elite that extreme measures may be counterproductive. "To behave differently [than to always lean towards providing maximum civil liberty] is to let terrorism win its war against democracy before the first shot is fired" writes Stella Rimington, former head of MI5.[26]

The *Universal Declaration of Human Rights* provides a benchmark against which the impacts of reactions of governments on citizens can be assessed but we do not have a similar comparison for cyber liberties. By extending the Articles to specifically address cyber liberties we would at least provoke debate and at best achieve acceptance of the Rights of cybercitizens and the protection of legitimate actions in cyberspace. Cyber liberties are required to facilitate an equitable, democratic global information society.

[26] 'Terrorism did not begin on September 11', *Guardian Weekly* September 12, 2002, p22."