The War on Terrorism Versus Cyber Liberties: Extended Abstract

Julie Cameron[1] and David Vaile[2]

[1] Info.T.EC Solutions Pty Ltd, Sydney, Australia. infotec_solutions@yahoo.com.au
[2] Baker & McKenzie Cyberspace Law & Policy Centre, Faculty of Law, University of NSW, Sydney, Australia. d.vaile@unsw.edu.au

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 (eg 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.

2. Legislative Changes in Australia and United Kingdom

The changes in legislation in Australia and the United Kingdom (UK) illustrate the types of change to laws and regulation that impact directly on cybercitizens.

The Australian government moved fast. Immediately after the attack on 11 September the Commonwealth Parliament (comprising the House of Representatives and Senate) passed a raft of Acts related to security and border protection including the:

- *Migration Legislation Amendment Acts 2001*[2] - changes include authorising an airline operator, shipping operator, travel agent or proscribed organisation to disclose information 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*[3] - 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).

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 http://www.austlii.edu.au/cgi-bin/disp.pl/au/legis/cth/num_act/mlaormsa2001n332001709/

3 http://www.austlii.edu.au/au/legis/cth/consol_act/mtcsaoca2001436/index.html

– *Intelligence Services Act 2001*[4] – 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 but initially not the Senate:

– *Security Legislation Amendment (Terrorism) Bill 2002 (No 2)* [5]
– *Suppression of the Financing of Terrorism Act 2002*[6]
– *Criminal Code Amendment (Suppression of Terrorist Bombings) Bill 2002*[7]
– *Border Security Legislation Amendment Bill 2002*[8]
– *Telecommunications Interception Legislation Amendment Bill 2002*[9].

Members of the Senate referred these Bills to Senate Legislation Committee (a body of 6 senators from the main political parties represented in Parliament). Despite only a weeks notice to 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 2002. The committee reported in May 2002, and after some amendments most of the bills were subsequently passed. The most contentious aspects, in relation to detention without charge, trial, or legal representation, were excised and deferred. At the time of writing (May 2003) this separate *ASIO Amendment (Terrorism) Bill* had not been passed.

Key terrorism acts in the United Kingdom are the:

– *Terrorism Act 2000*[10]
– *Anti-Terrorism, Crime and Security Act 2001*[11]
– *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*[12]. UK citizens were threatened by a proposal whereby, 'all telecommunications firms including mobile phone operators and Internet

4 http://www.austlii.edu.au/au/legis/cth/consol_act/isa2001216/index.html

5 http://scaletext.law.gov.au/html/pasteact/3/3496/top.htm

6 http://scaletext.law.gov.au/html/comact/11/6500/top.htm

7 http://scaletext.law.gov.au/html/comact/11/6497/top.htm

8 http://scaletext.law.gov.au/html/comact/11/6498/top.htm

9 http://scaletext.law.gov.au/html/comact/11/6501/top.htm

10 http://www.hmso.gov.uk/acts/acts2000/20000011.htm

11 http://www.hmso.gov.uk/acts/acts2001/20010024.htm

12 http://www.cyber-rights.net/

Service Providers would keep the number and addresses of all calls and emails made and received by EU citizens' for at least a year[13].

There is, officially acknowledged by Australia, involvement of the UK and Australian Governments with the Echelon communication interception systems. The UK government's preferred practice in relation to the existence and use of Echelon was 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."

3. Implications for Cybercitizens

Significantly, the implications of these legislative changes for cybercitizens appear to be not fully understood by either the governments concerned or the users of cyberspace. The result is the loss of cyber liberties[14]. The key implications for cybercitizens (not in order of importance) are:

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

   The new offences with which cybercitizens may be charged are not necessarily those within the country of citizenship. There is a major issue related to what is "connected" in cyberspace and which jurisdiction should apply at any time. For example, in the case of offences related to:
   - Disruption or destruction of Information Communication Technology (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 organisations. Each government retains its own list of proscribed organizations not necessarily known by their own citizens let alone cybercitizens 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 organisations and people outside national borders (Australia - *Intelligence Services Act 2001*)
   - Access "required identity information" from airline reservation systems and lists of ships passengers prior to arrival (Australia - *Migration Legislation Amendment Act 2001 (No 5)*)
   - Additional sharing of personal data from private and public sectors among agencies at all levels of government (Australia, Canada, UK and USA).

---

13 Richard Norton Taylor and Stuart Miller, 'Privacy Fears over EU plan to store email' *The Guardian Weekly*, August 22 2002, p1.

14 "Cyber liberties" are defined as the extension of the rights stated in the Declaration Human Rights to cyberspace.

3. Increased powers of defence, security and police organisations 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 (eg "suspicious" transactions, key words)
   - Powerful ongoing global surveillance of communications (eg Echelon)
   - Use of system audit and security tools including transaction history and logs
   - Use of systems capabilities regardless of proven need (eg mobile phones /GPS)
   - 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 organisations have been reduced (eg in Australia – security agencies need to obtain only an administrative warrant and not a warrant issued by the relevant Tribunal to question people, and 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 cybercitizens 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 to cybercitizens must be the:
   - Impossibility of nations to protecting the cyber liberties of their citizens, due to the extra-territoriality of some of the responses
   - Lack of certainty when the laws of more than one jurisdiction may apply
   - Loss or enclosure of the information "commons"
   - Claim by owners of infrastructure to rights to surveillance of users (to avoid misuse).

4. Benchmarking the Impacts on Cyber Liberty

It is acknowledged that countries that ignore civil liberties are unlikely to adhere to cyber liberties. Nevertheless, the United Nations *Universal Declaration of Human Rights* can be adopted as a benchmark to assess the appropriateness of 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. Although the UN *Universal Declaration of Human Rights* was developed prior to the use of the Internet and predates 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. We can therefore establish Principles[15] of Cyber Liberty within the existing framework of the *Universal Declaration of Human Rights* by clarifying relevant Articles so that they protect the rights of cybercitizens.

The following Principles of Cyber Liberties are 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)
3. Right to free exchange of knowledge, opinion and expression in cyberspace without fear (Article 19)
4. Right of cybercitizens 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[16]).

5. Conclusions

Terrorists aim to disrupt and displace ways of life. Over-reaction by governments ensures they achieve this goal without further effort. A reality check is required. Terrorism is often not "high tech," and technical responses are not necessarily effective. Significant intrusions on both civil and cyber liberties have resulted from the war on terrorism. There is growing concern even amongst 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.[17]

The *Universal Declaration of Human Rights* provides a benchmark against which the impacts of reactions of governments on the civil rights 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.

---

15 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

16 (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.

17 'Terrorism did not begin on September 11', *Guardian Weekly* September 12, 2002, p,22.