6th Annual National Security Conference Australia 2008

Sydney Convention & Exhibition Centre
6-7 March 2008

"This isn't Pinochet's Chile. This is Australia. 2002. We don't pinch our citizens off the street, keep them incommunicado, no lawyers, and try to crush them by keeping them incommunicado."[1]

Daryl Melham MP on the introduction of the ASIO Bill 2002.

Introduction

One year before his death in 1950, George Orwell published a book entitled *1984*. Orwell's book was a seminal work of fiction in the 20th century that predicted the demise of a humane society under a totalitarian government. In this story, we are taken to a society governed by an oppressive force known as "The Party," and an intangible ruler, "Big Brother." The main character, Winston Smith, spends his time throughout the novel trying to overthrow The Party and Big Brother, while running from the "Thought Police," a justice department that monitors the thoughts of citizens. Life for Winston Smith exists within a prism of totalitarianism defined by constant surveillance thru telescreens and reporting of suspicious behaviour where people are detained by authorities and held, tortured and eliminated without any recourse or scrutiny. There are no elections, food is strictly rationed and the country is constantly at war because being at war allows the authorities to take liberties that would not be afforded to them in peacetime. This book, although written in a post-World War II and pre-Cold War environment, presents surprising similarities to today's post-9/11 world.

Since 9/11 the Australian Government has introduced a large amount of legislation aimed at "winning the war on terror." Many of these are arguably necessary, because we know from Bali and Jakarta, the possibility of a terrorist act being committed in Australia is not remote. Governments, morally as well as under international law have a duty to protect persons in their jurisdictions who are threatened by terrorism. The United Nations Human Rights Commission, for example, has said that:

> "No one doubts that States have legitimate and urgent reasons to take all due measures to eliminate terrorism. Acts and strategies of terrorism aim at the destruction of human rights, democracy, and the rule of law. They destabilise governments and undermine civil society.

[1] Parliament deadlocked on ASIO Bill, AM, ABC Local Radio, Friday 13 December 2002

> Governments therefore have not only the right, but also the duty, to protect their nationals and others against terrorist attacks and to bring the perpetrators of such acts to justice."[2]

However, governments also have a duty to ensure that protecting security does not undermine other fundamental rights. Unfortunately this duty is considered less important these days as laws which once would have been considered unthinkable and arguably a violation of fundamental human rights are now being presented by western democratic governments, including the Australian Government, as the norm. These laws have opened the door to arbitrary detention, searches without warrants, and departures from established fair trial procedures so that it is the situation today, in Australia, that an accused could conceivably be charged and tried without knowing what evidence is against him, or without having a lawyer of his choice present to defend him. We have even seen attempts to justify the use of torture against terror suspects, in the name of "national security." According to Justice Michael Kirby, 17 of these Commonwealth anti-terrorism laws directly curb human rights and civil liberties.[3]

For many the introduction of such a large amount of legislation is an unbalanced and disproportionate response. Whilst I personally agree I also believe that taking this legislative approach is an inappropriate response in combating terrorism. It is my view that culture is a better defence against terrorism than legislation. I believe that the Australian culture and the ideals it represents as a tolerant, egalitarian, "fair-go" society have the potential to protect its citizens, more so than any anti-terror legislation can. By upholding human rights standards, maintaining civil liberties, improving communication, dialogue and understanding amongst Australia's diverse community and protecting the privacy of individuals we can fight the war on terror without compromising Australia's national identity. Should we continue to curb the freedoms of our own population, we will lose the war even if we win the battle against terrorism.

The purpose of this paper is to evaluate the impact of the introduction of numerous laws designed to fight and win the "war on terror" on Australian culture and national identity. Part 1 of this paper will look at the security legislation that has been introduced since 9/11 such as the two anti-terrorist Acts introduced in 2002 and 2005 and the ASIO legislation, which was introduced in 2002 and amended thereafter. Part 2 of this paper will discuss the impact of the legislation on fundamental freedoms and the rule of law. This Part will focus on the right to privacy and argue that legislation introduced since 9/11 has seriously eroded the right to privacy, in particular the right to personal information privacy. Part 3 of this paper will then discuss the need for striking a balance. Part 4 of this paper discusses the impact of the legislation on Australia's national identity and culture and conclude by suggesting alternative ways to fight terrorism.

---

[2] Digest of Jurisprudence of the United Nations and Regional Organizations on the Protection of Human Rights While Countering Terrorism, p. 1

[3] Michael Kirby, J *'Terrorism and the Democratic Response'* (2005) 28 (1) UNSW Law Journal 221, 226

Part 1 – Fighting the "War on Terror"

As at September 11, 2001 there was in place in Australia a patchwork of about 35 pieces of Commonwealth legislation which could be considered as broadly relating to anti-terrorist issues such as police powers, chemical and biological weapons, criminal offences, hostages, immigration, border protection, intelligence, nuclear non-proliferation, proceeds of crimes, telecommunications, and weapons of mass destruction.[4] Since September 11, 2001 this is however no longer the case. Following a worldwide trend to toughen laws on terrorism the Australian Government has embarked on a crusade of introducing legislation throughout the ensuing seven years. As at March 2008 there is now in place over 40 specific pieces of legislation relating to terrorism and security related issues alone.[5]

---

[4] See for example, the *Air Navigation Act 1991*; the *Australian Federal Police Act 1979*; the *Australian Radiation Protection and Nuclear Safety Act 1988*; the *Australian Security Intelligence Organisation Act (ASIO) 1979*; the *Chemical Weapons (Prohibition) Act 1994*; the *Crimes Act 1914*; the *Crimes (Biological Weapons) Act 1976*; the *Crimes (Hostages) Act 1989*; the *Customs Act 1901*; the *Intelligence Services Act 2001*; the *National Crime Authority Act 1984*; the *Nuclear Non-Proliferation (Safeguards) Act 1987*; the *Public Order (Protection of Persons and Property) Act 1971* and the *Telecommunications (Interception) Act 1979*.

[5] *Charter of the United Nations A(Anti-terrorism Measures) Regulations 2001; Charter of the United Nations (Sanctions – Afghanistan) Amendment Regulations 2001; Crimes Amendment Act 2002; Criminal Amendment (Anti-Hoax and Other Measures) Act 2002; Criminal Code Amendment (Espionage and Related Matters) Act 2002; Criminal Code Amendment (Offences Against Australians) Act 2002; Criminal Code Amendment (Suppression of Terrorist Bombings) Act 2002; Security Legislation Amendment (Terrorism) Act [No.2] 2002; Suppression of Financing of Terrorism Act 2002; Telecommunications Interception Legislation Amendment Act 2002; Australian Security Intelligence (ASIO) Amendment Act 2003; ASIO Legislation Amendment (Terrorism) Act [No.2] 2003; Australian Protective Service Amendment Act 2003; Crimes (Overseas) Amendment Act 2003; Criminal Code Amendment (Hams and Lashkar-e-Tayyiba) Act 2003; Criminal Code Amendment (Hezbollah) Act 2003; Criminal Code Amendment (Terrorism) Act 2003; Criminal Code Amendment (Terrorism) Act 2003 (Constitutional Reference of Power); Maritime Transport and Offshore Facilities Security Act 2003; Anti-terrorism Act 2004; Anti-Terrorism Act (No.2) 2004; Anti-Terrorism Act (No.3) 2004; Australian Federal Police and Other Legislation Amendment Act 2004; ASIO Amendment Act 2004; Aviation Transport Security (Consequential Amendment and Transitional Provisions) Act 2004; Crimes Legislation Amendment (Telecommunication Offences and Other Measures) (No.2) Act 2004; Criminal Code Amendment (Terrorist Organisations) Act 2004; International Transfer of Prisoners Amendment Act 2004; National Security Information (Criminal and Civil Proceedings) Act 2004; National Security Information (Criminal Proceedings) (Consequential Amendments) Act 2004; Surveillance Devices Act 2004; Surveillance Devices (No.2) Act 2004; Telecommunications Interception (Amendment) Act 2004; Telecommunications (Interception) Amendment (Stored Communications) Act 2004; Anti-Terrorism Act 2005; Anti-Terrorism Act 2005 (No.2); Crimes Amendment Act 2005; Intelligence Services Legislation Amendment Act 2005; Law and Justice Legislation Amendment (Video Link and Other Measures) Act 2005; Maritime Transport Security Amendment Act 2005; National Security Information (Criminal Proceedings) Amendment (Application) Act 2005; National Security Information Legislation Amendment Act 2005; Anti-Money Laundering and Counter-Terrorism Financing Act 2006; ASIO Legislation Amendment Act 2006; Aviation Transport Security Amendment Act 2006; Maritime Transport and Offshore Facilities Security Amendment (Security Plans and Other Measures) Act 2006; Telecommunications (Interception) Amendment Act 2006.*

The first package of security legislation designed to strengthen the governments response to the threat of terror was introduced on 12 March 2002. The package included the following Bills:

- the *Security Legislation Amendment (Terrorism) Bill 2002* [no.2];
- the *Suppression of the Financing of Terrorism Bill 2002*;
- the *Criminal Code Amendment (Suppression of Terrorist Bombings) Bill 2002*;
- the *Border Security Legislation Amendment Bill 2002*; and
- the *Telecommunications Interception Legislation Amendment Bill 2002.*

The introduction of the legislation brought a mixed reaction resulting in widespread debate largely focusing on the need for such legislation. The International Commission of Jurists, of which I am Chairman, for example expressed deep concern and anxiety about the legislation, as did other governmental and non-governmental organisations. [6] Most controversial of the Bills was the *Security Legislation Amendment (Terrorism) Bill 2002*. This Bill for the first time in Australia's history inserted into the *Commonwealth Criminal Code Act 1995* a new category of "terrorism offences." In its initial form the Bill defined terrorism so broadly and vaguely that it could cover many traditional forms of political protest. These new offences included:

- Terrorist acts - where in order to advance "a political, religious or ideological cause" serious harm is done to a person, or serious damage is done to property, or a person's life is endangered, or a serious risk to the health or safety of the public is created, or there is serious disruption to an electronic system for information, telecommunications, finance or serious disruption to systems for government services, public utilities or transport;
- Providing or receiving training connected with terrorist acts;
- Directing organisations concerned with terrorist acts;
- Possessing things connected with terrorist acts;
- Collecting or making documents connected with terrorist acts; and
- Acts done in preparation or planning of terrorist acts.

The legislation also permitted the Federal Attorney General to proscribe (ban) organisations if an organisation was involved in the following;

- Directing the activities of a proscribed organisation;
- Receiving funds for or making funds available to a proscribed organisation;
- Membership of a proscribed organisation;
- Provision of training or training with a proscribed organisation; and
- Assisting a proscribed organisation

[6] See for example, Castan Centre for Human Rights Law, Submission to Senate Legal and Constitutional Committee Regarding the Security Legislation Amendment (Terrorism) Bill 2002 [No. 2] available at http://www.law.monash.edu.au/castancentre/publications/anti_t2.html ; Public Information Advocacy Centre (PIAC), Submission to the Inquiry into the Security Legislation Amendment (Terrorism) Bill 2002 [No. 2] and Related Bills, April 2002 available at www.ag.gov.au/.../$file/02.04-PIACAntiTerrorismsub.pdf

The Attorney General did not have to provide any reasons for banning an organisation.

After much debate the Terrorism Bill was finally amended and introduced into Parliament on 12 March 2002 as the *Security Legislation Amendment (Terrorism) Act 2002*. The amended Act watered down many of the most controversial provisions. For example the new legislation removed the power to proscribe an organisation. However, despite being watered down the legislation still contained a number of provisions that continue to be of great concern. The legislation still for example, contains criminal sanction for involvement with a "terrorist organisation." Such involvement, according to the legislation includes recruiting members, providing support or funds, directing their activities or being a member.[7] A "terrorist organisation" is defined as "an organisation that is directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act (whether or not the terrorist act has occurred or will occur)."[8]

The rationale for the Terrorism Bill and the other Bills that were introduced was, according to the Australian Government, in response to *Resolution 1373* of the United Nations Security Council. *Resolution 1373* "'decided' that 'all States shall … prevent and suppress the financing of terrorist acts [and shall] [c]riminalize the wilful provision or collection … of [terrorist] funds by their nationals or in their territories'. It also required States to ensure that terrorists, their accomplices and supporters are brought to justice, and that 'terrorist acts are established as serious criminal offences in domestic laws … and that the punishment duly reflects the seriousness of such terrorist acts'. The Bills were 'designed to strengthen Australia's counter- terrorism capabilities'.[9]

On introducing the Terrorism Bill the then Federal Attorney General, Daryl Williams stated:

> "Since September 11 there has been a profound shift in the international security environment. This has meant that Australia's profile as a terrorist target has risen and our interests abroad face a higher level of terrorist threat.
>
> Australia needs to be well placed to respond to the new security environment in terms of our operational capabilities, infrastructure and legislative framework.
>
> This package and other measures taken by the government are designed to bolster our armoury in the war against terrorism and deliver our commitment

[7] *Security Legislation Amendment (Terrorism) Act 2002 (Cth)*, ss 102.2 – 102.7.
[88] *Security Legislation Amendment (Terrorism) Act 2002(Cth)*, s 102.1(1).
[9] Peter Slipper, MP, Security Legislation Amendment (Terrorism) Bill 2002 [No. 2], Second Reading Speech, House of Representatives, *Debates*, 13 March 2002, p. 1041.

> to enhance our ability to meet the challenges of the new terrorist environment."[10]

Despite these concerns, some nine days later on 21 March 2002, the Government introduced a second package of anti-terrorist legislation. This package however only contained one piece of legislation, the *Australian Security Intelligence Organisation (ASIO) Legislation Amendment Bill 2002*, arguably the most controversial of them all.

The Australian Security Intelligence Organisation (ASIO) Legislation

Described as the most draconian piece of legislation ever introduced by the Australian Government[11], the *ASIO Bill 2002* in its original form allowed adults (and even children from 10 years of age) to be detained and strip-searched for rolling two-day periods that could be extended indefinitely. Such persons could be detained if they had useful information about terrorism or potential terrorist acts. The Bill as drafted applied to all Australians. There was no right to silence, and a failure to answer any question put by ASIO would have been punishable by five years in prison. While the Bill stated that detainees "must be treated with humanity and with respect for human dignity," there were no penalty provisions in the Bill for ASIO officers who subjected detainees to cruel, inhuman or degrading treatment despite the fact that detainees have the right to be free from such treatment under international human rights law.

The Bill was referred to the Parliamentary Joint Committee (PJC) as well as the Senate Legal and Constitutional References Committee for comment. The PJC conducted a number of hearings and produced a bipartisan report focusing in particular, on the human rights implications of the Bill. According to the PCJ the Bill "would undermine key legal rights and erode the civil liberties that make Australia a leading democracy."[12] The PJC thus recommended a number of amendments. The Government accepted only some of the PCJ's recommendations. The Bill was then referred to the Senate Committee. With heavy amendment, the Bill was finally passed fifteen months later.

The *Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2002 [No.2] [2003]* was introduced into Parliament on 20 March 2003. The Act permits arbitrary detention of people - including children aged 16

---

[10] The Hon Daryl Williams, Security Legislation Amendment (Terrorism) Bill 2002, Second Reading, 12 March 2002, House of Representatives, Official Hansard, No. 3 2002 at 1040.

[11] See for example, Senator Brian Greig, The New ASIO powers; A Democrats Perspective, July 2003 available at http://www.democrats.org.au/campaigns/new_asio_powers/ ; The Hon John Von Doussa, President, Human Rights and Equal Opportunity Commission, Australia, Conflict and Countering Terrorism; Civil and Political Rights and the Rule of Law, Seventh International Conference for Human Rights Institutions, Seoul, South Korea, 14-17 September 2004, available at http://www.hreoc.gov.au/about/media/speeches/speeches_president/2004/koreaterrorismworkshop.html

[12] Parliamentary Joint Committee on ASIO, ASIS and DSD, *An Advisory Report on the Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill 2002*, at vii.

and over – in order to collect intelligence in relation to terrorist offences. The Act stipulates that detainees could have access to a lawyer of their choice, although ASIO may request that access be denied to a specific lawyer where that lawyer poses a security risk and that Australians may be questioned by ASIO for 24 hours over a one-week period. The Act states that once a person is questioned s/he must then be released. A person can only be re-questioned if a new warrant can be justified by fresh information. The Act further states a judicial officer is required to be present during interrogation only if practicable. This officer can be a judge, retired judge or legally qualified member of the Administrative Appeals Tribunal. The questioning must be videotaped and the whole process will be subject to the ongoing scrutiny of the inspector-general of intelligence and security, who is effectively the ombudsman for ASIO.

In 2003, the Act was amended to increase the time allowed for the questioning of non-suspects by ASIO from 24 to 48 hours when an interpreter is involved. A second amendment made it an offence, for two years after someone has been detained, to disclose any information about that detention or warrant.[13] Even if the information is provided as part of a media story on the detention regime, the penalty for doing so is a maximum of five years' imprisonment. In 2004 further amendments to the Act enabled terrorist suspects to be questioned without charge by the police for 24 hours, double the maximum time currently allowed for other criminal suspects.[14]

One of the greatest concerns about the legislation is the fact that it impacts all Australians whether or not they are involved in planning a terrorist attack. Under the legislation any Australian citizen – whether a doctor, lawyer, journalist, religious leader, community worker, health worker, friend or relative - can be whisked off for questioning without a lawyer and with no notice to friends or family on the belief or allegation that they may have evidence or information obtained in their professional or personal lives in relation to a suspected terrorist act without a lawyer and with no notice to friends or family. Such persons can therefore effectively disappear for at least several days. This is a standard practice of such vilified regimes such as in Chile under General Pinochet and Zimbabwe under President Mugabe.

In my view these detention powers can be seen as a form of torture. Torture is a serious violation of human rights and is strictly prohibited by international law. Article 1 of the *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment* (CAT), to which Australia is a party,[15] defines torture as follows:

---

[13] See ASIO Legislation Amendment Act no 143, 2003.
[14] See Anti-Terrorism Act 2004; See G Williams, Responding to Terrorism without a Bill of Rights: The Australian Experience, Asia Rights Journal, Issue 2, September/October 2004 available at http://rspas.anu.edu.au/asiarightsjournal/Williams.html
[15] Australia ratified the CAT on 8 Aug 1989.

> "any act by which severe pain or suffering, whether physical or mental, is intentionally inflicted on a person for such purposes as obtaining from him or a third person information or a confession, punishing him for an act he or a third person has committed or is suspected of having committed, or intimidating or coercing him or a third person, or for any reason based on discrimination of any kind, when such pain or suffering is inflicted by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity."

The detention power is also a violation of Article 10 of the *International Covenant on Civil and Political Rights* (ICCPR) to which Australia is also a States Party[16] and Principles 15, 16(1), 18 and 19 of the *Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment*, adopted by the United Nations General Assembly 43/173 on 9 December 1988. These Principles provide that a detained or imprisoned person has the right to communicate with his/her lawyer and the right to be visited by and to correspond with, in particular members of his family as well as the outside world.[17]

Another major concern about the legislation is that there is no right to silence. The right to silence is guaranteed under federal, state and territory legislation and also in international law. The ASIO legislation however ignores this fact. Under the legislation failing to give particular information or giving a false or misleading statement has been made an offence punishable by imprisonment for five years. There are also concerns that there is no clear right to have a lawyer of choice present during questioning and that where a lawyer is permitted, there are strict rules about what that lawyer can and cannot do. For example, the lawyer cannot say anything during the interrogation, except to ask that a question be clarified; any communication between the lawyer and client will be monitored; and if it is considered that the lawyer is being disruptive, the lawyer will be ejected from the proceedings. There is also the concern about a two-year ban on detainees and their lawyers, which prevents them from talking about what goes on during questioning and detention. Because of this, there is little public scrutiny of the operation of the questioning powers. Notwithstanding these serious concerns the legislation is now in force.

<u>The Anti-Terrorism Act (No.2) 2005</u>

---

[16] Australia ratified the *International Covenant on Civil and Political Rights* (ICCPR) on 13 August 1980. Article 10 specifically provides that "All persons deprived of their liberty shall be treated with humanity and with respect for the inherent dignity of the human person."

[17] Principle 15 for example states that "communication of the detained or imprisoned person with the outside world, and in particular his family or counsel, shall not be denied for more than a matter of days." Principle 16(1) states as follows;

"Promptly after arrest and after each transfer from one place of detention or imprisonment to another, a detained or imprisoned person shall be entitled to notify or to require the competent authority to notify members of his family or other appropriate persons of his choice of his arrest, detention or imprisonment or of the transfer and of the place where he is kept in custody."

In September 2005 the Australian Government announced in a media release that further anti terror laws had been drafted. The media release gave little information on the nature of the proposed legislation. The ACT Chief Minister, Jon Stanhope MLA, controversially published a draft of the proposed legislation on 14 October 2005. In response to the leak the Government attempted to declare that the leaked legislation was not in fact the final version that was to be tabled. After much debate the Bill was eventually introduced on 3 November 2005. Once again the proposed legislation contained a number of provisions that appeared to violate human rights and the rule of law, particularly in relation to the new regime of control orders and preventative detention orders.

The legislation introduced for the first time in Australian history the concept "control orders" or "house arrest." A control order is an order by the court that restricts what a person can do, including where they can go and to whom they can talk. A control order can thus prohibit or restrict a person from:

- "Being at specified areas or places or leaving Australia;
- Communicating or associating with certain people;
- Accessing or using certain forms of technology or telecommunications (including the internet); possessing or using certain articles or substances; and;
- Carrying out activities, including work activities."[18]

Controversially a control order may also include a requirement that a person;

- "Remain at a premises between certain times each day, or on certain days;
- Wear a tracking device;
- Report to someone at a certain time and place;
- Allow himself or herself to be photographed; and
- Participate in counselling or education, if the person consents."[19]

The order can last for up to 12 months for people aged 18 years or older and be used "where it would substantially assist in preventing a terrorist act or where a person has trained with a terrorist organisation which is listed in the Criminal Code Regulations." [20]

The legislation also introduced the concept of preventative detention orders, that is, detention without charge. Under the proposed laws a person can be detained if the Australian Federal Police (AFP) suspect that that person will engage in a terrorist act, possesses a thing that is connected with a terrorist act, or if the person has done, or will do, an act in preparation for a terrorist act. The terrorist

[18] See Attorney General's Department, Australian Government, "Anti-Terrorism Act (No.2) 2005 Questions and answers", at p. 3 available at www.ag.gov.au/.../$file/Anti-Terrorism+Act+(No2)+2005.pdf
[19] Id
[20] Id.

act must be imminent, and expected to occur in the next 14 days or have occurred in the last 28 days.

The proposed preventative detention regime set out two types of preventative detention: initial preventative detention; and continued preventative detention. Initial preventative detention orders are granted by a senior member of the AFP on an application by an AFP member and could be renewed for up to 24 hours. Continued preventative detention orders are granted by a federal judge or magistrate appointed in their personal capacity by the Attorney-General and applied to a person already under an initial preventative detention order.

Since the introduction of the *Anti-Terrorist Act (No.2) 2005* the Australian Government has issued two control orders. The Federal Magistrates Court in Canberra issued the first control order to Jack Thomas on 28 August 2006. The control order was imposed, according to the court, because it was "reasonably necessary" to protect the public and prevent a terrorist act. Under the order, Mr Thomas must abide by a curfew and be confined to his house between midnight and 5am. Mr Thomas must also report to police three days a week, is banned from leaving Australia without permission, and is restricted in what phones he can use. Mr Thomas is also banned from any contact with members of banned terrorist groups.[21]

The second control order was issued to David Hicks by an Adelaide court on 21 December 2007. Under the order Hicks is fingerprinted three times a week and is banned from leaving Australia. Mr Hicks also has to live at a secret address approved by the AFP and abide by a curfew from midnight to 6am. Mr Hicks has been banned from communicating with known terrorists and is banned from owning or communicating information about weapons, explosives, combat skills and military tactics. He is also banned from having firearms, ammunition or explosive devices. He is restricted to using a single mobile phone and SIM card issued by the AFP, an approved email account and internet server. He must not use a payphone or a satellite phone. If Mr Hicks breaches any terms of the order, he can be jailed for up to five years.[22]

The introduction of such orders is a serious inroad into fundamental human rights, such as the right to liberty, to be free from arbitrary detention and to the presumption of innocence. They impose sanctions not for what someone has done or due to what they are preparing to do, but because of what they might do in the future. They remove the presumption of innocence and limit a person's freedom even where there is not enough evidence to convict them under one of our many new terrorism offences. The orders were introduced on the basis that they replicate similar legislation in the United Kingdom. Whilst this may be the

[21] See Curfew Order for Jack Thomas, The Sydney Morning Herald, 28 August 2006 available at http://www.smh.com.au/news/national/curfew-order-for-jack-thomas/2006/08/28/1156617254376.html

[22] See Gavin Lower, Control order placed on David Hicks, Adelaide now, 21 December 2007, available at http://www.news.com.au/adelaidenow/story/0,22606,22958558-5006301,00.html

case there is major problem with the introduction of such legislation in Australia - unlike the legislation in the UK, it does not come with an adequate safeguard such as the *Human Rights Act 1988 (UK)* or the *European Convention of Human Rights*.[23] In the United Kingdom all British law must be read against these two instruments to ensure that tough terror laws do not undermine human rights and the rule of law. Australia does not have a Human Rights Act or any similar safeguard. Consequently as The Hon Nicola Roxon MP has commented;

> "These news types of orders based on what someone is expected to do, rather than the allegation of a crime already committed, challenge many of the concepts we have in criminal law to ensure fairness, such as proof beyond a reasonable doubt….
>
> [t]errorism may be an argument to depart from some of the established norms of criminal law, but it is not an excuse to abandon their purpose – ensuring fairness and protection from arbitrary police or Government interference."[24]

The introduction and eventual enactment of this legislation over the last seven years heralded a new era for Australia. We are arguably no longer a 'she'll be right mate" society, that is a society in which no problem is hard to fix without it being a problem, but are now a society who through the fear of terrorism rely on restrictive legislation to make us feel safe and confident. And as a result of that fear we have failed to question whether the legislation really is necessary, particularly where it abrogates human rights, the rule of law and the civil liberties of Australians - foundation elements of Australian culture.

Part 2 – Impact of the legislation – the erosion of fundamental freedoms and the rule of law

No one can argue that since 9/11 the world has dramatically changed. The evidence is everywhere - security cameras are observing us from almost every angle in the CBD, police can get warrants to tap our phone calls (and on occasion, without the necessity of a warrant), search our homes and bodies, employers can monitor our computer usage, marketing companies can create profiles on our spending habits through credit card purchases and internet use and people can hijack our whole identities using basic technology and information that we have freely given or unknowingly given away without a second thought. We are also being encouraged to spy on our neighbor and report possible signs of terrorism to the National Security Hotline, which provides a freecall service for all Australians. In scenes reminiscent of Orwell's 1984 we are reminded that, *'Some of the best people to spot things that are out of the*

[23] See for example the submission by The Centre for Human Rights Education to the Senate Legal and Constitutional Committee on the Anti-Terrorism Bill 2005 (Cth), available at http://info.humanrights.curtin.edu.au/pdf/SenateAntiTerror05.pdf.

[24] The Hon N. Roxon MP, "Prevention or punishment; terrorism's challenge to criminal law", Human Rights Defender, 2005.

ordinary in a neighbourhood or workplace are those who are there everyday. As we go about our daily lives, we can keep an eye out for anything that may seem unusual or suspicious. Whether or not something is suspicious can depend on the circumstances. Look at the situation as a whole. If it doesn't add up, call the 24-hour National Security Hotline.'[25]

The 24-hour National Security Hotline is one component in the Australian Government's campaign to fight terrorism. Another component of the campaign is an anti-terror kit. In 2003 the anti-terror kit was sent out to 8 million households. The kit included a letter from then Prime Minister John Howard advising people to call the Hotline and a fridge magnet with the relevant phone numbers. The kit also included a 20-page booklet offering tips on first aid, how to react in a crisis, and how to spot and report possible signs of terrorist activity, such as "unusual purchases of large quantities of fertilizer, chemicals or explosives." The kits were not a hit with the Australian public. A large majority of them were marked "return to sender."[26] This is not surprising to me. These 'spy on your neighbour measures' are seen by many to be somewhat "un-Australian" and goes against the ethos of Australian culture. While we certainly need to be vigilant against unlawful conduct, we perhaps need to focus more on programs and policies which will encourage communication, understanding and information exchange between the diverse sectors of our community.

Over the last seven years these unprecedented new laws enacted to fight the "war against terror" have begun to erode the building blocks of democracy - freedom of speech, freedom of association, freedom of assembly, freedom of religion and freedom of movement - and undermine our national identity. These five fundamental freedoms are guaranteed by international human rights law and are subject to the general rule that no-one has the right to 'engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms.'[27] Despite this guarantee these rights are slowly being eroded as we overlook their importance and focus on "fighting terrorism". One of the best examples of this erosion is the erosion of the right to privacy.

The Right to Privacy

Privacy is a fundamental human right. It underpins human dignity and other values such as freedom of association and freedom of speech.[28] The right to

---

[25] Australian National Security website http://www.nationalsecurity.gov.au/agd/www/nationalsecurity.nsf/AllDocs/868AD1272BCDEA15CA256FBF007DC082?OpenDocument

[26] See M.Shaw, Post office to destroy returned anti-terror kits, The Age, 5 March 2003 available at www.theage.com.au/cgi-bin/common/popupPrintArticle.pl?path=/articles/2003/03/04/1046540188964.html Returned anti-terror kits destroyed for safety: Govt, ABC News, 4 March 2003 available at http://www.abc.net.au/news/stories/2003/03/04/797931.htm

[27] See Article 5 of the International Covenant on Civil and Political Rights (Covenant) available at http://www1.umn.edu/humanrts/instree/b3ccpr.htm

[28] Privacy International, Overview, 16 December 2007 available at http://www.privacyinternational.org/

privacy is recognised in a number of international instruments, many of which Australia is a signatory to, as a human right. Article 12 of the Universal Declaration of Human Rights (UDHR), which Australia played an important role in drafting, for example provides:

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

Article 17 of the ICCPR reiterates Article 12 of the UDHR stating;

> "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks."[29]

The Australian Law Reform Commission (ALRC) in their Discussion Paper no. 72 entitled Review of Australian Privacy law noted that privacy has been defined as containing a number of separate but related concepts. These concepts include:

- Information privacy – which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as 'data protection'
- Bodily privacy – which concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches
- Privacy of communications – which covers the security and privacy of mail, telephones, e-mail and other forums of communication and
- Territorial privacy – which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.[30]

Whilst there is no actual constitutional right to privacy in Australia, the right to privacy is protected to a certain extent in both Commonwealth and State legislation. Such legislation for example limits interference with bodily privacy

---

[29] The Australian Law Reform Commission, Review of Australian Privacy Law, Discussion Paper 72, September 2007 (hereafter ALRC Discussion Paper 72) notes at page 279 (5.11) that in 1988 the OHCHR released General Comment Number 16, which discussed how the UN interprets art 17 and how it should be promoted through domestic law. It is noted in the General comment that art 17 should protect a nation's citizens against all interference and attacks on privacy, family, home or correspondence, 'whether that emanate from State authorities or from natural or legal persons.' To this end, all member states are required 'to adopt legislative and other measures to give effect to the prohibition against such interference and attacks as well as to the protection of this right.' Furthermore, 'state parties are under a duty themselves not to engage in interference inconsistent with article 17 of the Covenant and to provide the legislative framework prohibiting such acts by natural or legal persons.'

[30] ALRC Discussion Paper 72 page 114, at paragraph 1.29.

(assault laws), protects territorial privacy to some extent, and prohibits interfering with the privacy of communications. Over the past few years Federal and State governments have also introduced a range of legislation protecting the privacy of personal information (information privacy) due to a growing awareness of the need to protect personal information and intrusion by the State. As the Australian Privacy Charter Council has stated:

> "A free and democratic society requires respect for the autonomy of individuals, and limits on the power of both State and private organisations to intrude on that autonomy.
>
> Privacy is a value which underpins human dignity and other key values such as freedom of association and freedom of speech ...
>
> Privacy is a basic human right and the reasonable expectation of every person. It should not be assumed that a desire for privacy means that a person has 'something to hide'. People who wish to protect their privacy should not be required to justify their desire to do so."[31]

The principal piece of legislation relating to the protection of information privacy in Australia is the *Privacy Act 1988 (Cth).* This Act regulates the handling of personal information by the Australian Government, the ACT Government and the private sector. The Act contains numerous privacy principles that relate to Australian and ACT Government agencies (the Information Privacy Principles (IPP)) and the private sector (the National Privacy Principles (NPP)) to ensure that personal information held will be stored, used and disclosed in a fair and appropriate way. Similar legislation has been enacted in other Australian States and Territories.[32]

The IPPs are based on international guidelines established by the Organisation for Economic Cooperation & Development (OECD) on *the Protection of Privacy & Transborder Flows of Personal Data* which were adopted by the Australian Government in 1984. The Honourable Justice Michael Kirby was a key figure in the development of those guidelines. The guidelines stipulate that personal information must be collected fairly and lawfully, used only for the purpose specified during collection, adequate, relevant and not excessive to that purpose, accurate and up to date, accessible (eg for verification and correction), kept secure and be subject to disposal after the purpose is completed. The IPPs thus regulate all aspects of personal information including collection, use and disclosure, data quality, data security, openness, access and correction, unique identifiers, anonymity, transborder data flows and sensitive information.[33] The

---

[31] See Australian Privacy Charter Council, Australian Privacy Charter, 6 December 1994 available at http://www.privacy.org.au/apcc/Charter.html

[32] See for example *The Privacy and Personal Information Protection Act 1998 (NSW),* which was enacted in NSW in 2002.

[33] The Information Privacy Principles can be found at http://www.privacy.gov.au/publications/ipps.html

NPPs set out similar minimum standards for handling personal information by private sector organisations, including all private health service providers.[34]

Although the legislation has been a positive step towards ensuring that the right to privacy is an enforceable right, the legislation is severely compromised by the fact that it contains a number of exemptions and exceptions for some Australian Government agencies. These exemptions are largely directed at those organisations with an intelligence function. The acts and practices of the Australian Secret Intelligence Service, the Australian Security Intelligence Organisation and the Office of National Assessments are completely exempt from the Privacy Act.[35] These exemptions are common to other jurisdictions such as the UK, Canada and HK however Australian privacy laws go further than those jurisdictions and provide exemptions from the Act for defence agencies and Auditors-General, small businesses, as well as the Australian Crime Commission and royal commissions s7(1)(a)(i)(B), (iv), (v), (2)(a), (c).[36] The problem with these exemptions and exceptions is that privacy no longer becomes a relevant issue for these organisations. So when ASIO for example decides to incept an email or hack into a computer it does not have to think or consider the privacy implications of doing so. This is hardly, in my view, a proportionate or balanced response.

The Anti-Money Laundering legislation

Another potential example of the erosion of the right to privacy is the enactment of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)* (the AML/CTF Act).

The AML/CTF Act designed to enable individual businesses to manage money laundering and terrorism financing risks came into force on 13 December 2006. At present only the first 'tranche', or stage, of the legislation which relates to the financial services sector, the gambling sector and bullion dealers has come into effect. A second tranche of legislation, which is to effect lawyers, accountants, trust and company service providers, real estate agents and jewellers has recently been drafted and was released for public comment in August this year.[37] The consultation period has now finished and we understand that the Attorney General's Department is now considering the submissions received concerning the proposed reforms.[38]

---

[34] The National Privacy Principles can be found at http://www.privacy.gov.au/publications/npps01.html
[35] See section 7.
[36] ALRC Discussion Paper 72 page 888 (30.41)
[37] See Attorney-General's Department, "Second Tranche of Reforms", Australian Government, available at http://www.ag.gov.au/www/agd/agd.nsf/Page/Anti-moneylaundering_SecondTrancheofReforms
[38] The submissions can be found on the Attorney General's website at http://www.crimeprevention.gov.au/www/agd/agd.nsf/Page/Anti-moneylaundering_SecondTrancheofReforms

The legislation imposes obligations on "reporting entities" offering specific services that could be exploited to launder money or to finance terrorism. "Reporting entities" are defined in the Act as a "person who provides a designated service." "Person" is defined as "an individual," "a company", "a trust", "a partnership", "a corporation sole" or "a body politic".

In the first tranche legislation there were more than 70 specific services identified as "designated services."[39] These services are set out in section 6 of the Act and include for example, opening an account; accepting money on deposit; making a loan; issuing a debit card; issuing travellers' cheques, and sending and receiving instructions on electronic funds transfers.

The proposed second tranche amendments, which directly relate to the professions, identify a new range of services as "designated services." Such services could include for example, managing on behalf of a person, or giving advice on the management of, accounts, physical currency or property of that person; making arrangements or preparations on behalf of a person in connection with the sale or purchase of a business; making arrangements or preparations on behalf of the promoters of a new company, in connection with the formation of a new company; giving or directing tailored advice to the promoters of a new company, in connection with the formation of the company and making arrangements or preparations on behalf of the promoters of a new company, or providing tailored advice to the promoters of a new company in relation to equity finance or debt finance for the new company.[40]

Unlike the previous anti-money laundering legislation, the obligations under the new regime are no longer linked to 'significant cash transactions'. Instead, an 'activities' based definition is used where a person who provides, deals in or handles a 'financial product' will be subject to customer due diligence (CDD) and enhanced reporting obligations to report suspicious transactions[41].

A "reporting entity" is required under the Act to establish, maintain and comply with an anti-money laundering program. There are three different types of anti-money laundering compliance programs under the Act. These 3 programs, which are set out in Part 7 include a standard program that applies to a particular reporting entity[42]; a joint program that applies to each reporting entity within a designated business group[43]; and a special program that applies to a particular reporting entity that is an AFS Licensee who arranges for a person to receive a designated service.[44]

---

[39] See sec 5 of the AML/CTF Act 2006.
[40] See Attorney-General's Department, "Second Tranche of Reforms", Australian Government, available at http://www.ag.gov.au/www/agd/agd.nsf/Page/Anti-moneylaundering_SecondTrancheofReforms
[41] Part 3, Division 2, section 41.
[42] Part 7, Division 3, section 83
[43] Part 7, Division 3, section 85.
[44] Part 7, Division 3, section 86.

Prior to the commencement of the AML/CTF legislation an extensive consultation process took place. One of the major concerns about the legislation was the effect on the requirements on the right to privacy. The Australian Privacy Foundation for example submitted that privacy was not adequately protected under the anti-money laundering and counter-terrorism laws. The Office of the Victorian Privacy Commissioner submitted that there is a significant risk that the proposed measures will lead to pervasive monitoring of the financial affairs of ordinary citizens – not necessarily due to any suspicion that they are financiers of terrorism or money launderers, but simply by virtue of their engaging in what may be ordinary everyday transactions.[45]

Noting this concern the Senate Legal and Constitutional Legislation Committee recommended that an independent privacy impact assessment be conducted. In September 2006 an independent privacy impact assessment was conducted. The impact assessment made 96 recommendations all pointing to the overly invasive nature of the legislation. Noting for example that some of the aspects of legislation were overly intrusive into people's personal affairs compared with the current risks posed by money laundering and terrorism financing, the assessment recommended that the scheme should be proportionate to the risk. The assessment also expressed significant concerns about the collection, use and disclosure of personal information for purposes that were unrelated to the objectives of tackling money laundering and terrorist financing and recommended that personal information should be limited to the stated objectives of the scheme. [46]

In response to the Impact Assessment the Australian Government published a Privacy Impact Statement adopting 30 of the 96 recommendations. Despite the Impact Statement there continues to be some concern about the impact of the legislation on privacy related issues. The Australian Law Reform Commission has recommended further consultation and review of the following issues:

(a) "whether reporting entities and designated agencies are appropriately handling personal information under the legislation;
(b) whether the number and range of transactions for which identification is required should be more limited than currently provided for under the legislation;
(c) whether it remains appropriate that reporting entities are required to retain information for seven years; and
(d) whether it is appropriate that reporting entities are able to use the electoral roll for the purpose of identification verification."[47]

The ALRC has further asked "whether the legislation should be amended to provide that state and territory agencies that access personal information provided to the Australian Transaction Reports and Analysis Centre under the Act be regulated under the Privacy Act in relation to the handling of that personal

[45] ALRC Discussion Paper 72 page 513.
[46] ALRC Discussion Paper 72 page 512
[47] Id at p. 517.

information, except where they are covered by obligations under a state or territory law that are, overall, at least the equivalent of the relevant obligations in the Privacy Act."

The basis of these concerns is really the need for balance. The obligation to report suspicious transactions for example is an overwhelming obligation for reporting entities to comply with. The obligation to report suspicious transactions requires a reporting entity to report certain 'suspicious matters' that are related to the provision or prospective provision of a designated service. Clause 41 thus requires a reporting entity to report customers where there are reasonable grounds to suspect that information obtained may be relevant to the following:

- The potential evasion of taxation law[48];
- Offences against the law of the Commonwealth or a Territory[49];
- Enforcement of the Proceeds of Crime Act 2002[50];
- Preparatory to or the past commission of a financing of a terrorism offence[51], and
- Preparatory to or the past commission of a money laundering offence[52].

Where these conditions are satisfied, a reporting entity is required to provide a report to AUSTRAC containing details specified in the AML/CTF rules within 24 hours in relation to section 41(1)(g) or (h) or within three days of the reporting entity forming the suspicion for offences in sections 41(1)(d), (e), (f), (i) or (j). This is not a balanced response.

The obligation to report such suspicious circumstances is a big ask. It basically requires reporting entities to have knowledge about all of the offences that they are required to report on. A reporting entity would thus have to have knowledge of all of the offences that could amount to an evasion of taxation law, all offences that could amount to an offence against the Commonwealth or a Territory, all offences in relation to the Proceeds of Crime Act and all offences that could amount to terrorism. I doubt whether there are many other than a select few criminal lawyers who would have this kind of knowledge.

Secondly, even if reporting entities did have the requisite knowledge the legislation gives no guidelines as to what one should report. Neither the Government nor AUSTRAC has provided any examples of the type of transactions it would define as suspicious. According to CPAA the uncertainty as to what may amount to a suspicious transaction will lead to "defensive reporting" - that professionals will report anything because of the fear of being penalised if they don't. CPAA submits that this type of reporting will only add to a reporting

[48] Section 41(1)(f)(i)
[49] Section 41(1)(f)(iii)
[50] Section 41(1)(f)(iv)
[51] Section 41(1)(g)
[52] Section 41(i)

entities compliance burden and create more work for AUSTRAC. CPAA is thus calling on AUSTRAC to share the information and examples of the types of suspicious transactions it would like reported and provide clear guidelines. As CPAA states:

> "Leaving it to business to determine what is suspicious without providing examples and guidance on what is money laundering, imposes an avoidable burden on business."[53]

These new reporting requirements differ significantly from the previous money laundering legislation, the *Financial Transactions Reports Act 1988 (Cth)*. Unlike the old regime, which focused on the reporting of transactions and transfers with no mention of terrorism or counter-terrorist financing, the AML/CTF Act is risk-based and focuses heavily on counter-terrorist financing. Accordingly the legislation represents what the Government believes to be "a balanced and fair approach to ensuring that money laundering and terrorist financing risk in Australia is identified, managed and mitigated. It balances the needs of law enforcement agencies with the day-to-day realities of businesses that are covered by the legislation."[54] The amount of effort that will be required to comply with the requirements of the legislation however makes it unclear whether the effort is really in proportion to the risk that money laundering and counter-terrorist financing activities will take place in Australia.

Smart Card Legislation

The possible introduction of a Smart Card in Australia could be another example of the erosion of the right to privacy. Based on an idea that dated back to the Hawke Government in the 1980s[55], the smart card proposal was reignited again in 2005 after the terrorist bombings in London and the wrongful detention of Cornelia Rau.

According to the ALRC the use of smart cards raise several privacy concerns. Firstly, the smart card system may threaten anonymity and enable information about the activities of cardholders to be collected and stored. The smart card regime if implemented has the potential to generate 'records of the date, time and location of all movements on public and private transport systems, along with details of all goods purchased, telephone use, car parking, attendance at the cinema, and any other activities paid for by smart cards. These records will also be processed and stored in central databases, where they will be used to create

[53] K. Deane, "Terror laws snare small business", Australian IT, 4 September 2007, available at http://www.australianit.news.com.au/story/0,24897,22357168-24169,00.html

[54] As cited in the Replacement Explanatory Memorandum to the then Anti-Money Laundering and Counter-Terrorist Financing Bill 2006, available at http://www.commlaw.gov,au

[55] The Hawke Government tried to introduce a national ID card in the mid 1980s. The Liberal Government however fiercely opposed the idea.

detailed customer profiles.'[56] Once these profiles are created they can then be accessed by law enforcement bodies for crime investigation, by government departments for monitoring and by private citizens in litigation.

Secondly, the ALRC explains that that smart card technology will allow for the dangerous situation of function creep and the potential to read smart cards without the cardholder's knowledge or consent.[57]

Lastly, the smart card system prevents effective accountability of the information gathered. This concern arises because smart card schemes are commonly used by numerous agencies or organisations that may not have a central data controller. This concern became very apparent in the UK last year when two computer discs holding the personal details of families in the UK with a child under 16 went missing. The data included the names, addresses, date of birth, national insurance number and bank details of 25 million people. The problem was so bad that a child benefit information hotline had to be set up. The incident was described as a "catastrophic mistake" and a "final blow for the ambitions of this government to create a national ID database…"[58] This concern is not unfamiliar to Australia where research has revealed that data losses are common.[59]

Despite these concerns the proposal to introduce a smartcard once again has received much positive support. A Morgan Poll of an Australian wide cross-selection of 651 men and women conducted a on 23 July 2005**,** as reported in *The Canberra Times* indicated that 62% of Australians agreed with the introduction of a national ID card with a photograph, while 32% opposed it, and 6% were undecided. Pollster Gary Morgan said, "Australians are clearly in favour ... This is driven by the fear of terrorist attacks and illegal immigration. ... Clearly many people would like to see the identification card replace other forms of identification, but there are still some concerns regarding privacy and the effectiveness of the card in combating terrorism".[60]

This support is of no surprise to me. The concept of the right to privacy has changed considerably over the past few decades. What we once considered private is no longer thanks to technology advances in the international marketplace. We seem happy to give our personal details to any service provider that asks, and to some that don't… we give online authorisations for our details to be sold to marketing companies, we rely on security camera's to catch

---

[56] The Privacy Committee of New South Wales "*Smart Cards: Big Brother's Little Helpers*" No. 66 August 1995 at ii.
[57] ALRC, Discussion Paper 72, September 2007 at p.329.
[58] UK families put on fraud alert, BBC News, 20 November 2007 available at http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm
[59] See Explanatory Memorandum, *Privacy (Data Security Breach Notification) Amendment Bill 2007*
[60] see Australian Privacy Foundation, Australia Card Mark II, available at http://www.privacy.org.au/Campaigns/ID_cards/NatIDScheme.html#CaseFor

criminals (without thinking that we are being watched as well), we welcome technology that allows banks to track our spending habits so that when something 'out of the ordinary' is purchased they can contact us, fearing our cards may have been stolen. Technology is advancing so quickly that we don't even realise when we are being watched and tracked.

So what does privacy mean to Australian's today? Elizabeth Farrelly states, "that we grumble about government surveillance and invasions of privacy but, in fact, privacy is the last thing we seem to want. Anonymity is anathema. Increasingly what we seek is the right, and the opportunity to self-expose…some say that the blog generation, being over parented, has never known privacy (and therefore needs none);"[61] Contrasted to this sentiment is Professor Ruth Gavison, writing in 1980, arguing that the modern concern for the protection of privacy can be attributed to "a change in the nature and magnitude of threats to privacy, due at least in part to technological change…Advances in the technology of surveillance and the recording, storage, and retrieval of information have made it either impossible or extremely costly for individuals to protect the same level of privacy that was once enjoyed.'[62] This being so it is still difficult to see how the anti-terrorist legislation can validly be introduced and accepted by our democratic society without any justifiable risk.

Part 3 - Striking a Balance

In his opening speech to the International Commission of Jurists' Biennial Conference on Human Rights and Counter-terrorism held recently in Berlin, Nicholas Howen, the Secretary General of the ICJ, noted the importance of maintaining the rule of law in any counter-terrorist activity. Howen said:

> "We have seen the return of a disturbing rhetoric [in the war on terrorism]… [It is a security dominated discourse which] says that rights and freedoms interfere with security of state. It pushes aside the usual laws and norms because they seem to constrain the unfettered discretion of the executive to take any action it thinks necessary".

We are reminded, however, that:

> "… any state of emergency must be an extension of the rule of law, not an abrogation of it."[63]

---

[61] Farrelly, E '*Exposed: affairs of the look-at-me generation'* SMH 8 Jan 2008
[62] ALRC Discussion Paper 72 page 115 (1.32)
[63] See International Commission of Jurists Australian Section, Submission to the Joint Parliamentary Committee on ASIO, ASIS, and DSD: Review of Division 3 of Part 3 of the ASIO Act 1979, available at www.aph.gov.au/HOUSE/committee/pjcaad/asio_ques_detention/subs/sub60.pdf

Howen's words reiterated the rhetoric of numerous international rules, which emphasise the need for an appropriate balance between the protection of individual rights and national security whilst fighting "the war on terror." Under international law States may suspend certain rights during a state of emergency which threatens the life of the nation. At the same time however, states of emergency are bound by strict rules to prevent violations of rights. Article 4 of the *International Covenant on Civil and Political Rights* (ICCPR) provides that derogation from human rights protections is permitted "in times of public emergency which threatens the life of the nation". This means that any suspension of rights must be necessary and proportionate; they cannot discriminate against people because of their race or similar grounds; and they must respect the principle of legality. Some rights however can never be derogated from whether in peacetime or war, such as the prohibition on torture or cruel, inhuman or degrading punishment or treatment (Article 7). Other articles which may not be derogated from include the right to life (Article 6), guarantee against retrospective criminality (Article 15) and freedom of thought, conscience and religion (Article 18).

The need for balance has also been reinforced by the United Nations on numerous occasions. On 13 February 2002 for example Resolution A/RES/56/160, UN General Assembly, *Human Rights and Terrorism*, referred to the need to ensure that efforts to combat terrorism did not amount to breaches of human rights:

> "Reaffirming that all measures to counter terrorism must be in strict conformity with the relevant provisions of international law, including international human rights standards."

Similar sentiments were expressed by the Security Council in Resolution 1456 on 20 January 2003 and by the United Nations General Assembly (A/RES/58/187) on 22 March 2004 as follows:

> "States must ensure that any measure taken to combat terrorism comply with all their obligations under international law, and should adopt such measures in accordance with international law, in particular international human rights, refugee, and humanitarian law."

To effect this balance both the the Human Rights Committee and the European Court of Human Rights have established a number of safeguards. These safeguards include:

- The restrictions must be prescribed by law;
- They must be necessary in a democratic society;
- They must accord with the principle of proportionality (between the right to be protected and the general interest);
- The restriction should not limit the human right more than is necessary to achieve the aim;

- The means chosen should be appropriate to achieve the aim.

The United Nations High Commissioner for Human Rights on 27 February 2002 issued a statement of criteria for protecting human rights while States implement measures against terrorism. The statement was issued in light of *UN Security Resolution 1373* (28 September 2001) which calls on States to bring to justice those involved in terrorist acts and to establish such acts as serious criminal offences. The criteria set out in the statement by the UN High Commissioner replicate many of the safeguards for the protection of human rights set out above, and require that any restrictions for public security purposes shall be:

- Prescribed by law;
- Necessary for public security or public order;
- Not impair the essence of the right;
- Are necessary in a democratic society;
- Conform to the principle of proportionality;
- Appropriate to achieve their aim;
- The least intrusive means to achieve the aim of the measures;
- Respect the principle of non-discrimination; and
- Not be arbitrarily applied.

Similar safeguards were also adopted by the Council of Europe on 11 July 2002 and 5 March 2005.[64]

Unfortunately the Australian government has been contradictory in its achieving this balance. Whilst the Government has said that we must protect against those who would threaten our way of life, it has been supportive of the treatment of those Australians who were held at Guantanamo Bay. The same contradiction appears in the nature of the security legislation. Whilst the Government asserts on one hand that it is committed to defending our democratic way of life, on the other hand, it has enacted laws which, more than at any other time in our history, attack the same values and principles which make Australia one of the most successful free societies in the world. This is clearly demonstrated in the enactment of the types of legislation and their impact on human rights as discussed above. Whilst it is true that to a large extent many of the historical concerns about privacy are no longer as relevant as they once were, there is still need to protect privacy as a fundamental human right and strike a fair balance.

Part 4 – the un-Australian response to the "war on terror"

Disproportionately harsh security legislation threatens the basic rights and fundamental freedoms of every Australian citizen. That threat is most visible to those in our society who are, by practical application, most affected by the

[64] See Council of Europe, The Guidelines on human rights and the fight against terrorism, adopted by the Committee of Ministers on 11 July 2002 and The Guidelines on the protection of victims of terrorist acts, adopted by the Committee of Ministers on 5 March 2005, available at http://www.coe.int/T/F/Droits_de_l'Homme/Guidelines.asp#TopOfPage

legislation – our Muslim community. Notwithstanding the fact that many Muslim leaders in our community have come out strongly against terrorism and have declared that such acts have no place in Islam, many Muslims feel shock and fear at the way they are portrayed in the media, at work and in general and feel that they bear the brunt of this legislation. According to researcher Luke Howie discrimination in the workplace for example, is a real problem. Racist sentiments towards Muslim co-workers have been reported in Australia. Such sentiments upset workplace dynamics and cause alienation and emotional ramifications. During Howie's study of workers in Melbourne he had one manager in a retail firm say:

> "I certainly treated people differently (after September 11). As soon as an Arabian, a Musso, as soon as a Muslim walked in, what I classify as a Mussi, I would generally try to stay away from them only because I didn't want to come into contact or have to deal with people like that. It sounds a bit racist, but, just the mentality after September eleven and what you see on TV does make me have this kind of…feeling… When you see things like big headlines, things in Iraq. They take this particular person, execute them, suicide bombings. Then you go off to work and think to yourself f*%#! Something like that could happen today. As soon as you see that race of people you think to yourself, what have they got planned next? What are they doing? What are they conspiring to do? That's it."[65]

The impact of the legislation and the threat of terrorism has also had a significant affect on Australian society including the way we work and live day to day. According to Howie CBD workers, such as those in Melbourne have increased fear and anxiety and have decreased job satisfaction and increased occupational stress. Howie comments;

> "Fear and anxiety due to the terrorist threat is creating an uncertain and hesitant workforce. Leave is taken as soon as it accrues, work is a lower priority, and psychological wellbeing is deteriorating. People are less willing to travel for business, commute to work, and work in prominent or tall buildings. This creates problems of lower job satisfaction and more alarmingly, increased occupational stress."[66]

Fear has been an effective tool used by both the Australian government and its allies to raise awareness and fight the war on terror. Deception was used to enhance that fear. As the Former Prime Minister of Australia, Malcolm Fraser commented in the 2005 University of Melbourne Chancellor's Human Rights Lecture,

> "Fear was created by pretence that Saddam Hussein could drop chemical or biological weapons on the city of London within 45 minutes...

[65] Respondent 2, interview in retail firm, December 5, 2004 in L. Howie, Terrorism and Social Change, Human Rights Defender, 2005.
[66] L. Howie, Terrorism and Social Change, Human Rights Defender, 2005.

> No one had said Saddam Hussein could do that - but the British Government had left, hanging in the air, the strong impression that he could deploy such weapons within 45 minutes, even though the Government knew Iraq had no missiles that could achieve that result.
>
> My friends in London were fearful, believing that such a possibility justified war against Iraq. Deception was allowed to stand.
>
> Serious qualifications placed by intelligence agencies on the possession of weapons of mass destruction were not heeded by the Coalition of the Willing. Arrangements were put in place to provide "intelligence" to justify policy already determined."[67]

It is my belief that security is perhaps 90% psychological and 10% physical. This applies to the security of workplaces, relationships and countries. There is a psychological need for people to feel safe; however the meeting of that need requires a balanced approach. For example, in my office, some members of staff are concerned that irate members of the public or disgruntled lawyers may cause them harm. I could put in security guards, bulletproof glass and metal bars but that would create an environment where our clients thought they were feared. The environment we wish to create is one of calm and reason where problems can be solved peacefully.

Should clients approach an office that looks like a bunker they could be forgiven for perceiving that the office must be protected from them and the temperature of their interactions with staff could consequently rise. Further, we resist the temptation to install heightened security as a result of a 'one-off' incident or concerns about potential incidents without a proper risk analysis being done. The approachability of an office can reflect the contract that individuals make with society to act appropriately.

This analogy of my office can apply to national security. We need to ask 'why' we are building up our defenses, allowing our security services greater powers of detention and investigation and tightening our borders. What is the purpose that is trying to be fulfilled? Is it towards a more secure nation or the 'feeling' of a more secure nation – and security from what? The anti-terror legislation affects our culture, civil liberties and human rights and yet our strongest defense against terrorism is our culture. The role of culture as a defence against terrorism is not just an idealistic concept. The events surrounding the arrest of Ahmed Ressam is testament to this fact.

In December 1999, an Algerian man was arrested while attempting to cross the border from Canada into the United States with more than 20 kilograms of explosives in the trunk of his car. Ahmed Ressam, aka the 'Millenium Bomber"

---

[67] The Rt Hon Malcolm Fraser, Human Rights and Responsibilities in the Age of Terror, The Chancellor's Human Rights Lecture, University of Melbourne, 29 November 2005 available at http://www.safecom.org.au/malcolm-fraser-rights.htm

left Algeria in 1992, after civil war broke out when an Islamic fundamentalist party won national elections but was prevented from taking power by the military government. He had trained in an Al-Qaeda camp in Afghanistan, learning skills in weapons, explosives, and poisons, and was intending to blow up Los Angeles International Airport on New Years' Eve, 1999.[68]

Ressam was charged with conspiracy to commit an act of terrorism, among other offences. Instead of being killed or tortured, as he might have expected due to his background and indoctrination, Ressam was given the right to silence, was appointed a lawyer, and accorded due process. This amazed Ressam, and so impressed him with the fairness with which he had been treated, that, eventually -notwithstanding the fact that he was sentenced to 130 years' imprisonment - he became one of the principle informants against Al-Qaeda operatives in the United States. Information which he gave authorities revealed Al-Qaeda sleeper cells operating in that country, and led to the convictions of four operatives on terrorism charges. In addition, he gave authorities inside information about the inner workings of Al-Qaeda, as well as details of his training in the camp in Afghanistan.

Ressam's case is a prime example of how respect for the rule of law - in other words, being true to our culture and identity - does not make us more vulnerable, but can strengthen in a real way our ability to counter terrorist activity.

Conclusion

The Australian Government has said that in this so-called "war on terrorism", because our adversaries do not believe in the Geneva Conventions and the rule of law, we can justifiably depart from them in our response. But how much of our belief in the rule of law and in human rights, how much of our culture, are we prepared to abandon in this fight? If the only way to fight terrorists is to become like them, then what will ultimately remain of Australia as a tolerant, egalitarian, "fair-go" society?

Australia is one of the oldest democracies in the world, having been established in 1901. The historical origins of our democracy, however, stretch back centuries and can be traced back to 1215, to the signing of the Manga Carta, the first document which limited the power of the English King from absolute rule. The Magna Carta was the first step in a long historical process leading to the rule of constitutional law, the development of parliamentary democracy, and is today the source of tradition for our system of government.

The introduction of the type and extent of "security legislation" that we have seen in Australia shakes the foundations of our system of government – the separation of powers and the rule of law and ignores major developments in governance,

[68] PBS – Frontline, Ahmed Ressam's Millenium Plot, available at http://www.pbs.org/wgbh/pages/frontline/shows/trail/inside/cron.html

human rights and the rule of law since the Magna Carta in 1215. The introduction of such legislation also impacts heavily on our culture and our way of life. This is a situation that must be addressed. I believe that our Government and society as a whole need to strike the balance between protection from terrorism and the support of human rights and freedoms so that our Australian culture can be enhanced and recognized as the first line of defense against security threats.

In trying to find this balance the test lies in the nature of our culture and identity: we have to ask, what do we believe in, and what are we willing to give up? If we agree that we value our identity as a tolerant, egalitarian, “fair-go” society, then this can anchor our response to terrorism. In this light, respecting the rule of law, by, for example, affording even terrorist suspects full fair trial guarantees, is not evidence of weakness, but is a sign of strength of character, culture and identity. If, on the other hand, we take away those rights to an extent that our basic beliefs and principles are compromised, then, in fighting this war on terrorism, we are at a risk of losing ourselves.