CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES
JCSP 35 / PCEMI 35

MDS

SURVEILLANCE & INFORMATION EXPLOITATION TO COMBAT THE NEW TERROR THREAT: THE ETHICAL AND LEGAL WAY TO ENSURE VICTORY

By/par LCol/Lcol Darren L. Harper

24 April 2009

CONTENTS

ABSTRACT

Surveillance and information exploitation are two of the most important tools in the fight against the new terror threat worldwide. The terror threat to western nations comes not only from outside our borders, but also from within. Countering this threat requires the use of technologies that some westerners find invasive and concerns about privacy issues have become increasingly apparent. This paper will review the ethical, moral and legal issues related to information collection and exploitation and seeks to determine if it is possible for privacy and security to coexist in the current climate of the war on terror.

> "Law-abiding citizens value privacy. Terrorists require invisibility. The two are not the same, and they should not be confused."[1]
>
> - Richard Perle

INTRODUCTION

In today's information dominated, interconnected world the effort to combat global terrorism using information collection and exploitation tools causes the lines between private and public information to become increasingly blurred. National security is not just the purview of the government in power, but also the responsibility of the individual. Governments are charged with the enormous and important task of protecting all of their citizens, but it is becoming increasingly clear that the average citizen must accept some intrusion into their privacy to provide security, since the collection of large amounts of information is the only way to reveal patterns that raise concerns for intelligence agencies. In the democratic state, individual privacy is one of the tenets of liberty that must always be considered, however, global terrorism has now forced a wedge between a state's requirement to protect its citizens and the right of said citizens to maintain their liberties.

Are we in an Orwellian state?[2] No, provided that clear boundaries for exercising executive powers and guidelines with reasoned justification for surveillance and information collection are established, it is possible to avoid this dystopian society. Democratically elected governments are bound by their populaces to build trust and to be

---

[1]David Frum and Richard Perle, *An End to Evil: How to win the war on terror* (New York: Ballantine Books, 2004), 60.

[2]George Orwell, *Nineteen Eighty Four* (New York: Penguin Books, 1976), 5. In his book Nineteen Eighty-Four, George Orwell hypothesized an all-seeing State, known as "Big Brother" whose intense and intrusive vigilance has become a symbol of the potential horrors of government intrusion into the privacy of individuals.

held accountable for their actions. This requires that effective safeguards be in place. In Canada and the United States (US), these safeguards are provided by royal commissions and/or senate committees, commissioners and/or officers, and judicial oversight. Do we have to give up our liberties to "purchase" a little security?[3] Yes, and this is in keeping with our democratic structure. To provide the required protection of our nation's population in today's conflict with those employing global terror, governments must use the resources available to them. At the same time, individuals want to maintain their privacy; the battle between these two opposing needs has become clouded in the controversy over public surveillance and individual privacy.

In endeavoring to ensure our national security, while striving to maintain our democratic rights, it is necessary to categorize the threats directed towards our nation and the source of those threats. The "fifth column", the spy, the saboteur, the foreign-directed terrorist or subversive, has always been seen as one of the threats that nations need to combat.[4] Once identified as a foreign intelligence agent, the observed actions of a foreign spy allow a nation's intelligence and security services to focus their surveillance and analysis efforts. The difficulty has always been finding the right information to identify the spy and to make a correct, accurate assessment of their targets. In the past, the government could typically identify the threat coming from those nations with a fundamentally different world view e.g. the USSR's long term spying on the USA and vice versa. As James Bamford highlights in his book "The Body of Secrets", the United

---

[3]Francis Jennings, *Benjamin Franklin: Politician* (New York: W.W Norton & Company, 1996), 117. "Those who would give up essential Liberty to purchase a little temporary Safety deserve neither Liberty nor Safety." This philosophy became a watchword for Franklin during his political career, but was used first in his speech to the Pennsylvania Assembly on February 17, 1775.

[4]Reg Whitaker, *The End of Privacy: How Total Surveillance Is Becoming A Reality* (New York: The New Press, 1999), 20.

States executive leadership from Eisenhower to John F. Kennedy and through to George W. Bush Sr. could clearly identify the national threat.[5] These leaders could seek confirmation of their intelligence; whether this included ordering signals intelligence collection on communications beyond the Berlin wall, testing the U.S.S.R.'s radar detection capabilities, monitoring Israeli communications during the six day war or seeking confirmation of North Korean intentions in the 1950s, the threat was categorized as the enemy's national leadership and/or military capabilities. Essentially, governments threatened other governments; nations threatened other nations. Under these conditions, it was possible to focus intelligence gathering by using the national signals traffic of oppositional governments. On the other hand, the covert activities of the modern terrorist challenge our security services' ability to detect and target the individuals and groups who require monitoring. We are no longer living in a world where nations and governments pose the only threat, but rather in a world where the threat comes from many directions.

In his 25 October 2001 speech as part of the 2001 Young Memorial Lecture series, Dr. Michael Ignatieff indicated that we are now faced with an asymmetric war of power, weaponry, organization, and morality in the international as well domestic arenas. Our military organization has tended to protect military targets, but a feature of these asymmetric threats is that the terrorist goes after civilian targets.[6] Enemies now do not

---

[5]James Bamford, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (New York: Doubleday, 2008), ?,

[6]Anonymous, *Through Our Enemies' Eyes: Osama bin Laden, Radical Islam, and the Future of America* (Dulles, Virginia: Brassey's, 2003), 53-66. Osama bin Laden's central position is the "belief that Islam and the Muslim world are being attacked by more modern, powerful, and predatory version of the medieval Catholic Crusaders; the United States, Britain, or the West generally,…"and that "acquiring [chemical biological radiological and nuclear – CBRN] weapons for the defense of the Muslims is a

wear a uniform, are indistinguishable from civilians and hide amongst civilian populations to make our job more difficult.[7] Further difficulties arise from the fact that our own civilian population, our own citizens, often those with strong ties to their nation of origin, but also those born and raised in this country, are involved in these terrorist activities. The problem we are faced with is the identification of this threat "in the heart of our own society, because the battlefront is not out there, it's right here."[8]

Currently, global-terrorism is perceived as one of the most significant threats to national security.[9] Any ongoing discussion of terrorism assumes that we define the concept in a consistent way. According to Bard O'Neill, terrorism is defined as "the threat or use of physical coercion, primarily against non-combatants especially civilians to create fear in order to achieve various political objectives."[10] What does the threat of terrorism look like to Canadians and Canadian interests globally? On October 22, 2001 Ward Elcock, the Director of the Canadian Security Intelligence Service (CSIS) testified before the Special Senate Committee on the Anti-Terrorism Act that "there are terrorist groups with members, adherents, and in some cases, operatives in Canada, as there are in other countries in the world."[11] Stanley A. Cohen's *Privacy, Crime and Terror*, shows

---

religious duty." In February 1998 Osama bin Laden declared "…kill[ing] Americans and their allies – civilian and military – is an individual duty for every Muslim who can do it in any country in which it is possible to do it…".

[7]Dr. Michael Ignatieff, "Ethics and the New War," *Canadian Military Journal* 2, no. 4 (Winter 2001-2002): 7.

[8]*Ibid.*, 7.

[9]Canada, *Securing an Open Society: Canada's National Security Policy* (Ottawa: Privy Council Office, April 2004), 6.

[10]Bard O'Neill, *Insurgency & Terrorism: From Revolution to Apocalypse* (Washington: Potomac Books, 2005), 33.

that the 11 September 2001 instructions for the attack on the World Trade Centre in New York city originated in Afghanistan, planning took place in Italy and Germany, preparations were made in the southern United States (US), but the attack was executed in the northeastern US. [12] According to Richard Mosley, the terrorists who flew the planes on September 11 and others trained by Al-Qaeda in Afghanistan have been found to have connections in dispersed parts of the globe including Canada.[13] In its campaign against terrorism, the Canadian government, through its International Policy on Defence, deploys its political, military and economic resources against al-Qaeda and like-minded groups, as they are identified as one of the faces of terrorism that threatens Canada.[14] Canada has concluded that terrorism is not only an Islamic radical phenomenon, but those threats by individuals and groups inspired by Al-Qaeda ideology are currently a top priority, as they are in the UK, one of our allies in the war on terrorism.[15] As the collaboration between bin Ladin (Al-Qaeda) and Mullah Omar (Taliban) shows, global communication has brought terrorists together and has allowed them to influence terrorist activities globally.[16] Homegrown terrorists, young Canadians who find themselves

---

[11]Stanley A. Cohen, *Privacy, Crime, & Terror: Legal Rights and Security in a Time of Peril* (Markham, Ontario: LexisNexis Canada, 2005), 177.

[12]Cohen, *Privacy, Crime, & Terror*…, 159.

[13]*Ibid.*, 159.

[14]Department of National Defence, *Canada's International Policy Statement: A Role of Pride and Influence in the World – Defence* (Ottawa: Department of National Defence, 2005), 5.

[15]United Kingdom, HM Government, *Countering International Terrorism: The United Kingdom's Strategy July 2006* (Norwich, England: TSO (The Stationary Office), 2006), 6. The United Kingdom's (UK) strategy for countering International terrorism classifies the principle terrorist threat to UK interests and their populations domestically and internationally as those "radicalized individuals who are using distorted and unrepresentative interpretation of the Islamic faith to justify violence" that are known as "Islamist terrorists."

rapidly indoctrinated and radicalized into violent ideologies, are another of the new faces of terrorism in Canada.[17] Further, CSIS recognizes threats from other radical groups coming from within Canada and from other nations; since April 2006, Tamil Tigers, who both recruit and fund-raise in Canada, have been regarded by the Canadian government as terrorists.[18] The destruction of the 1985 Air India flight was caused by Sikh terrorists here in Canada.[19] The conclusion we can make is that Canadians and Canadian interests are not immune to the risk of a terrorist attack and that, despite efforts to profile the threat, the threat is ever changing and has both a domestic and international presence.

Structurally, this paper has five main parts. Section one introduces the new threat and provides a short, concise history of surveillance and information exploitation; the scope of this paper will necessarily keep this to little more than an overview. The history relates events from a Canadian perspective; however, no review of information exploitation would be possible without an understanding of the influential role that US agencies play in this area. While abuse of power and information sharing failures have plagued both Canada and the United States, surveillance and information exploitation have been successful intelligence tools in supporting national security efforts. Section two introduces the concepts of privacy and security and allows for a better understanding of the struggle to maintain these western societal values as we look to use surveillance

---

[16]Janice Gross Stein and Eugene Lang, *The Unexpected War: Canada in Kandahar* (Toronto: Penguin Canada, 2007), 227.

[17]Canadian Security Intelligence Service, *Backgrounder No. 8 – Counter-Terrorism*, Internet; www.csis-scrs.gc.ca/nwsrm/bckgrndrs/bckgrndr08-end.asp, accessed: 10 April 09.

[18]J.L. Granatstein, *Whose War is it*? (Toronto: HarperCollins Publishers, 2007), 196.

[19]Dwight Hamilton, *Inside Canadian Intelligence: Exposing the New Realities of Espionage and International Terrorism* (Toronto: Dundurn Press, 2006), 128.

and information exploitation to counter terrorism. Those who value the concept of privacy as a fundamental right in western society are often in opposition to those who believe in the need for increased surveillance to ensure national security. In the end, privacy and security are "mutually reinforcing" principles that western governments are charged to maintain and support at all costs.[20] Section three deals with the analysis of the ethical dilemma between countering terrorism by using surveillance and information exploitation and the impact this has on individual privacy. Though there are many ethical theories that can be used to analyze the struggle, this study will be limited to Kantian, Utilitarianism and Social Contract theories. An overview of these theories helps to answer the question of how governments can collect and utilize personal information in the war on terror while keeping wrongdoing by the intelligence community in check. Section four investigates the legal position of both the US and Canadian governments respecting the collection of information. A brief review of the US Patriot Act and the Canadian Anti-Terrorism Act looks at how the Acts affect the information gathering and exploitation permissible in the war on terror and seeks to determine if the right to privacy has been eroded too far. The final section presents an overview of the outlook of current thinking on surveillance as a means to counter terrorism and outlines some ideas on the future of information sharing and exploitation. The scope of this paper is restricted to national security issues and will leave the discussion of criminal acts to other authors.

It is incumbent on any government to work from an ethical and legal perspective to seek to provide the appropriate balance between the state's duty to secure the nation

---

[20]Jim Bronskill, "Don't let national security trump privacy: report," *The Canadian Press*, Internet: http://www.metronews.ca/ArticlePrint/138965?language=en, 10 November 2008; accessed: 19 Nov 2008.

against foreign threats; while maintaining the privacy of our citizens, we can increase our use of surveillance and information exploitation to counter the new threat of terrorism.

> "Any sound that Winston made, above the level of a very low whisper, would be picked up by it;…There was of course no way of knowing whether you were being watched at any given moment…You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard,…"[21]
>
> - George Orwell

A SHORT HISTORY OF SURVEILLANCE – A CANADIAN PERSPECTIVE

Surveillance is a primary tool of intelligence gathering and interpretation in the effort to protect national interests. Canadian CF Joint Intelligence doctrine concludes that information collection and exploitation have a direct influence on one of the main aims of intelligence: to warn "of threats in time to take effective (preventive, pre-emptive or protective) counter action."[22] Though sometimes hampered with wrongdoing by those charged with information collection, the history of surveillance and information exploitation shows us that information is a vital resource in providing for national security and as a key enabler in combating terrorism.[23]

Prior to WWI, WWI, and the Inter-War Years

With the invention of radio and telegraph communications, the possibility of electronically intercepting and deciphering an adversary's communication became apparent. The US Civil War saw the creation of the United States Army Signal Corps and US Military Telegraph and, as a result, "the first concerted effort at code-breaking

---

[21]Orwell, *Nineteen Eighty Four*…, 6.

[22]Department of National Defence, B-GJ-005-200/FP-000 *CF Joint Intelligence Doctrine* (Ottawa: DND Canada, 21 May 2003), 1-2.

[23]Nils Petter Gleditsch, Review of "Signals Intelligence in the Post-Cold War Era. Developments in the Asia-Pacific Region by Desmond Ball," *Journal of Peace Research* 31, no. 2 (May, 1994), 229.

and communications penetration, or telegraph line tapping" occurred.[24] This new technology was quickly developed and evolved into a strategic resource. Signal intelligence can be credited with playing a large part in the entry of the United States into World War I. The British interception and decryption of the German "Zimmerman Telegram" encouraged President Wilson to urge congress to declare war on Germany.[25] Though not in time to support America's war effort, the 20's and early 30's saw the formation of the American Black Chamber, an organization whose mission was to "read the secret code and cipher diplomatic telegrams of foreign governments – by [any] such means…" Japanese codes were of special interest and the five thousand decipherments during the Washington naval armament conference gave US negotiators advanced warning of the Japanese position and the upper hand in the negotiations.[26] The Black Chamber fell into disrepute with Secretary of State Henry Stimson and he is quoted as saying "Gentlemen do not read each other's mail." Nevertheless, Stimson came to realize that his position required accurate intelligence information that resulted in the softening of his views. In the 30's improved cipher methods and cipher machines were introduced and radio communications laws, such as the US Congressional

---

[24]Church Committee Reports, "Part One: The Small Beginnings," *Book 6: Supplementary Reports on Intelligence* (Washington: Assassination Archives and Research Center, 1976), 51. Available from http://aarclibrary.org/publib/contents/church/contents_church_reports.htm; Internet; Accessed: 2 April 2009.

[25]Aspin-Brown Commission, "The Evolution of the U.S. Intelligence Community – An Historical Overview," *Strategic Intelligence: Windows Into a Secret World: An Anthology* (Los Angeles: Roxbury Publishing Company, 2004), 6. Intercepted German diplomatic and naval traffic showed Germany enticing Mexico to join the war against the United States in return for Texas, Arizona, and New Mexico if Germany won the war.

[26]Church Committee Reports, "Part Two, The Middle Years (1914-1939)," *Book 6: Supplementary Reports on Intelligence* (Washington: Assassination Archives and Research Center, 1976), 117. Available from http://aarclibrary.org/publib/contents/church/contents_church_reports.htm; Internet; Accessed: 2 April 2009.

Communications Act of 1934, were enacted to protect national information and safeguard personal information privacies.[27] As early as 1928, US Supreme Court Justice Brandeis recognized that new technologies would transcend previously perceived barriers protecting personal information:

> "discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack to obtain disclosure in court of what is whispered in the closet. The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping."[28]

In a Canadian context, prior to 1939 Canada has been categorized as being in a state of "cryptographic innocence." Canadians acted as the "passive consumer" in the business of foreign intelligence; more specifically, the techniques of wireless interception and code-breaking were left to our British counterparts.[29]

World War II and Its Aftermath

As Wesley K. Wark indicates, "[b]etween 1939 and 1945 Canadian cryptographic innocence [was] transformed into cryptographic awareness." Canadians became interested in the use of cryptographic information in the protection of Canadian interests that included concerns of a possible Vichy French campaign of sabotage and subversion

---

[27]Communications Act of 1934, Public Law No. 416, June 19, 1934, 73rd Congress, Internet: http://criminalgovernment.com/docs/61StatL101/ComAct34.html; accessed: 11 April 2009. The Act provided for the regulation of interstate and foreign communication by wire or radio. Sec 605 specifies that "no person not being authorized by the sender shall intercept any communication and divulge the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person…"

[28]Gary T. Marx, "Privacy and Technology," *The World and I*, September 1990; Internet; http://web.mit.edu/gtmarx/www/privantt.html; accessed 3 April 2009.

[29]Wesley K. Wark, "Cryptographic Innocence: The Origins of Signals Intelligence in Canada in the Second World War," *Journal of Contemporary History* 22, No. 4 Intelligence Services during the Second World War: Part 2 (Oct. 1987), 639.

against French Canadians, a Nazi "fifth column" threat, and Japanese progress in the war.[30] It was because of Canada's interception of Japanese diplomatic and military signals that Canada entered the global intelligence conflict and the global intelligence alliance. Canada entered an American intelligence connection which was to prove both beneficial, in the timely exchange of information, and costly, in the loss of Canadian cryptographic independence from the emerging American superpower.[31]

In the years leading up to World War II, American intelligence agents and their allies made arrangements with telegraph companies to obtain copies of telegrams including those sent by foreign governments.[32] The allied interception of information involved US naval and army signals intelligence (SIGINT), British Bletchley Park code breakers and Canadian Communications Intelligence (COMINT), commonly known as the Examination Unit during WWII. These allied organizations regularly read the secret communications of more than forty nations during and following the Second World War.[33] The targeted countries included Italy, Turkey, France, Germany, Yugoslavia, Indonesia, and Uruguay.

Pearl Harbour: Warning and Decision, Wohlstetter's thorough analysis of the trials and tribulations in the world of American signals intelligence prior to the attack on Pearl Harbor, highlights the uncertainty in "…deal[ing] with shifting signals. Its [intelligence's] evidence will never be more than partial, and inference from its data will

---

[30]Wark, "Cryptographic Innocence…", 642.

[31] *Ibid*., 658.

[32]James Bamford, *The Puzzle Palace: A Report on America's Most Secret Agency* (Boston: Houghton Mifflin Company, 1982), 12.

[33] Wark, "Cryptographic Innocence…", 641.

always be hazardous."[34] Limited American military and diplomatic circles had access to deciphered MAGIC codes such as the top-priority Japanese diplomatic PURPLE messages[35]. Hampered by policymakers' limited understanding of information analysis, their lack of ability to interpret the information, and noise (a plethora of irrelevant messages) the Americans were unable to see a clear picture of Japanese capabilities and the Japanese ability to accept very high risks. In 1941, "disparate government agencies had bits of information" that pointed to an attack[36], but no conclusions were drawn that would have allowed the US to anticipate and pre-empt the attack on Pearl Harbor. In 1942, the Americans succeeded in cracking the Japanese code allowing American political and military leadership "to defeat the Japanese at the Battle of Midway and to counter the Japanese during the rest of the war in the Pacific."[37] The evolving collection and use of signal intelligence was seen as essential to the conduct of military and security operations. Admiral Nimitz is reported to have believed that the interception and analysis of coded radio messages had the equivalent value in the Pacific of another whole fleet.[38]

---

[34]Roberta Wohlstetter, *Pearl Harbor: Warning and Decision*, (Stanford: Stanford University Press, 1962), 227. Other theories abound: "Washington's inability to predict such an attack [Pearl Harbor] can easily be made to look like gross stupidity or negligence or a conspiracy to conceal vital information." 187, and Jurgen Rohwer, "Signal Intelligence and World War II: The Unfolding Story," *The Journal of Military History* 63, no. 4 (Oct., 1999), 949, James Rushbridger and Australian cryptanalyst Eric Nave claim that Churchill learned from decrypted Japanese naval message in the JN-25 cipher, a cipher not decrypted by American cryptanalysts until after the war, that Japan planned to attack Pearl Harbor, but did not warn Roosevelt because he wanted to drag the US into the war.

[35]Wohlstetter, *Pearl Harbour: Warning and Decision…*, 170-173. MAGIC was defined as the name given to the Japanese codes and ciphers. PURPLE was the name given to the Japanese cipher system.

[36]Abraham McLaughlin, "It will gather intelligence at home to curb terrorism. Critics see era of Big Trench coat," *The Christian Science Monitor*, 17 December 2001, http://www.csmonitor.com/2001/1217/p2s1-usgn.html,; Internet; Accessed: 2 April 2009. The disparate agencies included the Army and Navy in 1941.

[37]Aspin-Brown Commission, *Strategic Intelligence*…, 8.

Korea, Vietnam and the Cold War Era

Following the Second World War, the Canadian government recognized the need for continued foreign surveillance capabilities even when post-war demobilization was its main focus. Canada joined the UKUSA club with the creation of the Communications Branch of the National Research Council (CBNRC) in 1947.[39] Though always lagging behind the United States National Security Agency (NSA) and the United Kingdom Government Communications Headquarters (GCHQ) in communications surveillance,[40] bilateral intelligence agreements such as the "Canadian-United States Intelligence Estimate of the Military Threat to North America" and the "Canadian-United States Communications Instructions for Reporting Vital Intelligence Sightings (CIRVIS/MERINT)", allowed Canada to build key enablers, such as a CBNRC country wide receiver hunt,[41] for monitoring the Soviet threat including airborne aircraft or missiles approaching Canadian (North American) airspace and Soviet political/diplomatic operations within Canada.[42] In 1945 the defection, to Canada, of Igor Gouzeno, a cipher

---

[38]Church Committee Report, *Volume 5 Intelligence Activities – The National Security Agency and Fourth Amendment Rights* (Washington: Assassination Archives and Research Center, 1976), 6. Available from http://aarclibrary.org/publib/contents/church/contents_church_reports_vol5..htm; Internet; Accessed: 2 April 2009.

[39]James Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency* (New York: Anchor Books, 2002), 394. UKUSA is the acronym for: United Kingdom United States of America. As of 1952 this involved the work of the US NSA in partnership with the UK GCHQ.

[40]*Ibid*., 396.

[41]John Sawatsky, *For Services Rendered: Leslie James Bennett and the RCMP Security Service* (Toronto: Doubleday Canada Limited, 1982), 107-108. Though unsuccessful, this "vacuum cleaner" style activity at tuning into short wave radio transmissions in Montreal, Ottawa, and Toronto via equipment installed on a Beech aircraft focused on "…suck[ing] up illegal's in the act of receiving instructions from Moscow."

in the Soviet embassy in Ottawa, gave the Canadian government confirmation of the clear and present threat of a Soviet spy network in Canada.[43] Surveillance would play a large part in the coming years as Canada countered Soviet espionage with several expulsions.[44] What transpired in the 50's, 60's and early 70's was an allied collaboration on such projects such as Minaret[45], Shamrock[46] and Echelon[47] that targeted foreign enemies. Unfortunately, under these programs, domestic surveillance was conducted on civil rights groups, suspected drug traffickers, celebrities and peace groups; this led to domestic

---

[42]Jeffrey T. Richelson, *The US Intelligence Community 5th Ed.* (Boulder, Colorado: Westview Press, 2008), 346.

[43]Robert Bothwell and J.L. Granatstein, *The Gouzenko Transcripts: The Evidence Presented to the Kellock-Taschereau Royal Commission of 1946* (Ottawa: Deneau Publishers, 1969), 20.

[44]Sawatsky, *For Services Rendered…, 156.* Major Vladimir Vassiliev, Assistant Air Attache, was expelled for attempting to buy classified information from a contact acting as a double agent for the RCMP. Lev Grigoryevich Khvostantsev, a Soviet exchange scientist with the National Research Council, was deported trying to buy secret information about another exchange scientist. Lieutenant-Commander Valerie Smirnov, Soviet Naval Attaché, was publically rebuked for seeking to purchase industrial information from a Bell Northern Research scientist in Ottawa.

[45]Electronic Privacy Information Centre (EPIC), "Legality of NSA's Secret Eavesdropping Program Is Suspect and Cost is Unknown," *Spotlight on Surveillance*, Internet; http://epic.org/privacy/surveillance/spotlight/0106/default.html, accessed 30 Nov 2008. A domestic watch list program that included information collection and illegal wiretapping of civil rights groups and anti-war activities.

[46]Church Committee Report, "*National Security Agency Surveillance Affecting Americans,*" *Book 3: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans* (Washington: Assassination Archives and Research Center, 1976), 740. Available from http://aarclibrary.org/publib/contents/church/contents_church_reports_book3..htm; Internet; Accessed: 2 April 2009. Operation SHAMROCK was conducted from August 1945 until May 1975 that included watch lists development and telegrams and telephone monitoring. In the US, with the NSA pursuit of international communications, what resulted was incidental interception of personal information and highlighted the need "to resolve the dilemma between…effective foreign intelligence and the need to protect the rights of American citizens."

[47]Lawrence D. Sloan, "ECHELON and the Legal Restraints on Signal Intelligence: A Need for Reevaluation," *Duke Law Journal* 50, no. 5 Special Symposium Issue: Congress and the Constitution (Mar., 2001), 1471. ECHELON has never been formally recognized, however, it is alleged to be a worldwide signals intelligence effort to collection foreign intelligence from telephone, facsimile, e-mail and data transmissions interceptions. The program includes the efforts of the US (NSA), UK (GCHQ), Canada (CBNRC), Australia (Defense Signals Directorate – DSD), and New Zealand (Government Communications Security Bureau – GCSB).

watch list programs in Canada and the US, activities that were prohibited by the laws of both countries. Canadian eavesdropping operations under the overall program called PILGRIM, were conducted with embassy based listening for communications to and from India, China, Venezuela, Mexico, the Soviet Union, Romania, Morocco, Jamaica, and the Ivory Coast.[48] As described by the Canadian Civil Liberties Association, this was a period of unlawful misdeeds by the Royal Canadian Mounted Police (RCMP), especially E Special, a subsection of the RCMP Security Service; there were cases of mail-opening, theft, and electronic surveillance against perceived terrorist threats associated with the Parti-Quebecois and communist sympathizers such as the future Quebec Premier, Réné Levesque.[49] Between 1979 and 1981, The Commission of Inquiry Concerning Certain Activities of the RCMP under Justice D.C. McDonald was conducted to investigate illegal acts and improper conduct.[50] This resulted in the separation of intelligence services from the RCMP to the newly created CSIS and saw the institution of reviews of intelligence services by the Security Intelligence Review Committee; these reviews are intended to provide for more public scrutiny of the intelligence service agencies CSIS and CBNRC.[51]

---

[48]Richelson, *The US Intelligence Community*…, 348. In 1996 PILGRIM is credited with enabling Canada to provide the US with the intelligence assessment concerning Afghanistan: "Afghanistan: Taliban's Challenges, Regional Concerns" dated 17 Oct 1996.

[49]A. Alan Borovoy, *The Fundamentals of Our Fundamental Freedoms* (Toronto: The Canadian Civil Liberties Eduction Trust, 2001), Preface. Pierre Cloutier, "1948-1958 – The hunt for communists is open," *Rene Levesque: 38 Years of Federal Police Surveillance*, 15 Feb 2008, Internet; http://www.vigile.net/IMG/doc_Rene_Levesque_-_episode_no_1.doc, accessed: 4 April 2009 and "The magnitude of the federal police surveillance on the movement sovereignist Quebec (10960-1985)," Internet; http://www.vigile.net/L-ampleur-de-la-surveillance, accessed: 4 April 2009.

[50]Security Intelligence Review Committee, *Reflections* (Government of Canada, 2005); Internet; www.sirc-csars.gc.ca, accessed: 14 April 2009. Sawatsky, *Men in the Shadows*…, 238. The question remains, in 1973 why and from what foreign sources did the Parti Quebecois receive $350,000?

The US involvement in the Korean and Vietnam conflicts led to the development of a global electronic web of stations, satellites and submarines for the purpose of signals and communications intelligence by the NSA.[52] This included land-based, antenna-strewn intercept stations, world wide, to home in on Soviet air and naval traffic, commercial communications, and radar signals. According to James Bamford in his book, "The Puzzle Palace", the Vint Hill Farms surveillance site just outside Washington, DC targeted Washington's embassy row and "apparently not even the British are spared in embassy monitoring."[53] The NSA had the ability to continuously monitor every international telephone conversation or message to/from anyone in the US. J. Edgar Hoover is quoted as saying that "such a power could have been fantasized only by Orwell."[54] During this period SIGINT and imagery intelligence (IMGINT) satellites were invented and used to gather information on intercontinental ballistic missile launches. Among other things, this information was used to monitor the USSR's compliance with treaty agreements.[55] U2 flights (such as the Francis Gary Powers USSR over-flight during which he was shot-down in Sverdlovsk), provided photo and signals information.

---

[51]McDonald Royal Commission, "Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police," Internet; http://epe.lac-bac.gc.ca/100/200/301/commissions-ef/mcdonald1979-81-eng/mcdonald1979-81-eng.htm, accessed: 14 April 2009.

[52]Nils Petter Gleditsch, "Review of: Signals Intelligence in the Post-Cold War Era. Developments in the Asia-Pacific Region by Desmond Ball," *Journal of Peace Research* 31, no. 2 (May, 1994), 229.

[53]Bamford, *The Puzzle Palace…*, 163.

[54]Bamford, *The Puzzle Palace…*, 174.

[55]Gregory F. Treverton, "Intelligence: Welcome to the American Government," *Strategic Intelligence: Windows Into a Secret World: An Anthology* (Los Angeles: Roxbury Publishing, 2004), 364.

The cold war years saw domestic surveillance targeted against American citizens to identify and combat communist supporters and anti-war protestors. President Nixon authorized the Bureau of Narcotics and Dangerous Drugs (BNDD) to conduct special domestic targeting of communications traffic involving US revolutionary leaders and organizations suspected of involvement with foreign powers such as Cuba. US Senators and Representatives including Sam Ervin, Frank Church and Otis Pike, took up the case for civil liberties; investigations were made into warrantless surveillance and searches by the FBI, CIA and NSA against "dangerous" individuals such as Mrs. Martin Luther King Jr. [56] Organizations such as the American Civil Liberties Union (ACLU) called for enquiries into these wrongdoings that resulted in the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, known as the Church Committee after the chair Senator Frank D. Church.[57] The Keith case[58] in the US is an example of the way the courts moved to

> "…protect our Government against those who would subvert or overthrow it by unlawful actions…[however] inherent duty does not extend to authorization of warrantless electronic surveillance deemed necessary to protect the nation from subversion by "domestic organization."[59]

---

[56]Karl E. Campbell, *Senator Sam Ervin and the Army Spy Scandal of 1970-71: Balancing National Security and Civil Liberties in a Free Society, 10;* Internet; http://www.cmhpf.org/senator%20sam%sam%20ervin.hym; accessed: 2 April 2009.

[57]Church Committee Report, "Warrantless FBI Electronic Surveillance," *Book 3: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans* (Washington: Assassination Archives and Research Center, 1976), 290. Available from http://aarclibrary.org/publib/contents/church/contents_church_reports_book3..htm; Internet; Accessed: 2 April 2009. Church Committee Report, "*National Security Agency Surveillance Affecting Americans…*" 749-755.

[58]Church Committee Report, "*National Security Agency Surveillance Affecting Americans …*" 757. The US Supreme Court decision upheld the Forth Amendment warrant requirement for electronic surveillance, however, it did not recognize the President's constitutional duty to "protect our Government against those who would subvert or overthrow it by unlawful means." The Court held that this power "did not extend to the authorization of warrantless electronic surveillance deemed necessary to protect the nation from subversion by *domestic* organizations."

Revelations made, during the Keith case, of the arbitrary compilation of watch lists containing names of American citizens, programs including SHAMROCK and MINARET, and warrantless electronic surveillance activities authorized by the President, led to the passage of the Foreign Intelligence Surveillance Act (FISA) in 1978. Under FISA, a secret federal court was set up, the Foreign Intelligence Surveillance Court (FISC), also known as the "spy court." The court has the responsibility to screen and eliminate American identities, both citizens' and holders' of Green Cards, in domestic information collection if there is not a clear relationship between a foreign attack or sabotage, terrorism, or clandestine activities by a foreign agent.[60] This now required the NSA to obtain a secret warrant with "probable cause" to target either an agent of a foreign power or those involved in espionage or terrorism, foreign or domestic.[61]

One of the main communications breakthroughs of this period was the introduction of global microwave and satellite communications such as those satellites operated by the International Satellite Organization (Intelsat). This technological revolution made technologies like fast frequency-hopping, encryption at all levels and low-probability of intercept communications systems available to foreign military forces and terrorists. The airways now became the medium for communications in a much more significant way than in the past and the collection mission of the NSA and its allies' was made more difficult than ever before.[62] Even in the face of this hurdle, as early as the

---

[59]Bamford, *Puzzle Palace*…, 292.

[60]EPIC, *Legality of NSA's Secret Eavesdropping*…, 2-3.

[61]Sloan, "ECHELON and the Legal Restraints…," 1494-1495. President Franklin D. Roosevelt was the 1st President to use this inherent authority argument to justify warrantless surveillance.

1970's, the intelligence community believed that terrorist activities were being hampered by intelligence agencies' use of these covertly acquired signals. General Allen, the NSA director in the 1970's, believed that "a major terrorist act [involving Palestinian terrorists and aimed at American Jews] in the US was prevented."[63]

Post-Cold War and the 9/11 Era

The introduction of fibre-optic cabling in the 1980's connected nations via seabed laid lines and hampered information collection activities because of the technology's immunity to interception; conversely, however, the explosion of cell phone usage at the beginning of the 21st century, again enabled the NSA to build its databanks of information. The security agencies continued to work under the laws designed to protect Americans from surveillance by their own government and the general feeling was that the intelligence community was able to protect the US from terrorist activities with reasonable success.[64] While there had been terrorist attacks on US properties around the world, like the October 2000 bombing of the USS Cole which has been attributed to Al-Qaeda[65], for most North Americans, terrorism happened elsewhere. September 11, 2001 was to fundamentally change that attitude.

---

[62]Matthew M. Aid, "The Time of Trouble: The U.S. National Security Agency in the Twenty-First Century," *Strategic Intelligence: Windows Into a Secret World: An Anthology* (Los Angeles: Roxbury Publishing, 2004), 78.

[63]Bamford, *Puzzle Palace*…, 300.

[64]Aid, "The Time of Trouble: The U.S. National Security Agency…", 79.

[65]CBS News, "Yemen Frees USS Cole Bomb Plotter," *The Associated Press,* Available from http://www.cbsnews.com/stories/2007/10/26/terror/main3414029.shtml; Internet; Accessed 3 April 2009.

As of 10 September 2001, US security agencies had, according to James Bamford in his book "A Pretext For War", collected those information triggers that would link Osama bin Ladin, his Yemen safe-house, and one of the key suicide bombers, Mohamed Atta, into a credible terrorist plot set to strike in the USA. As early as August 6, 2001 President Bush was briefed that "terrorists might be preparing for an airline hijacking in the United States and might be targeting a building in lower Manhattan."[66] As in 1941, intelligence agencies, in this case the NSA, FBI and CIA, failed to protect Americans from a foreign attack on their own soil.[67] Ultimately, this failure was the result of several factors including the inability of intelligence agencies to share information rapidly, the inability of the NSA to turn its listening operations into the US to watch US residents, and a slow moving bureaucracy.[68] What followed that eventful day of 9/11-2001 were new terrorism fighting mechanisms including the introduction of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001.[69]

In Canada, after the Cold War years, the CBNRC transitioned to the Communications Security Establishment Canada (CSEC) as the government's arm in the worldwide signals intelligence network. The activities of the CSEC are controlled by

---

[66]James Bamford, *A Pretext For War: 9/11, Iraq, and the Abuse of America's Intelligence* Agencies (New York: Doubleday, 2004), 242.

[67]McLaughlin, "It will gather intelligence to curb terrorism…" *The Christian Science Monitor*, 17 Dec 2001; Internet; http://www.csmonitor.com/2001/1217/p2s1-usgn.html; accessed: 2 Apr 2009.

[68]Bamford, *A Pretext For War*..., 208.

[69]ABC-CLIO, "USA Patriot Act (2001)," *United States at War: Understanding Conflict and Society* (2009); available from http://www.usatwar.abc-clio.com; Internet; accessed: 13 March 2009.

parliament, the Minister of National Defence (MND) and a special commissioner to review activities to ensure compliance with Canadian laws.[70]

In December 1999, Algerian terrorist Ahmed Ressam was arrested and convicted in the USA of planning the Millennium Plot to bomb the Los Angeles International Airport. Ressam, an Algerian with political refugee status in Canada, has been linked to Al Qaeda and the Algerian terrorist group Armed Islamic Group (GIA).[71] After the 9/11 attack in the USA, in December 2001, Canadian Parliament passed the Anti-Terrorism Act (ATA). This Act "creates offences that criminalize activities…that take place before a terrorist event can occur. That is why the ATA is sometimes described as an Act of prevention."[72] Perpetrating, financing, or contributing to terrorist activities in Canada is a crime under this act.[73]

Prior to the enactment of the ATA, Canadian intelligence agencies had been hampered by the limitations of the Criminal Code; Part Six of the Criminal Code prohibited intercepting private communications.[74] While the Criminal Code had been

---

[70]Office of the Communications Security Establishment Commissioner, *Annual Report: 2007-2008* (Ottawa: Minister of Public Works and Government Services, May 2008), 1. The name changed from Communications Security Establishment (CSE) to CSEC on 27 Sep 2007 to comply with the federal identity program.

[71]*PBS Frontline*, "Trail of a Terrorist: The Millennium Plot: Ahmed Ressam's Millennium Plot," available from http://www.pbs.org/wgbh/pages/frontline/shows/trail/inside/cron.html; Internet; accessed: 16 March 2009.

[72]Department of Justice Canada, "The Anti-Terrorism Act," available from http://canada.justice.gc.ca/eng/antiter/act-loi/contex.html; Internet; Accessed: 14 April 2009.

[73]Cohen, *Privacy, Crime and Terror…*, 455.

[74]Chief CSE, "Special Senate Committee Chief CSE Appearance – 11 April 2005 Speaking Notes," *Parliamentary Review of the Anti-Terrorism Act*, Available from www.cse-cst.gc.ca/home-accueil/nat-sec/review-ata-examen-lat-eng.html; Internet; Accessed: 3 April 2009. 5.

amended as required since 1970 to take advantage of UN counter-terrorism tools[75], the Code was primarily designed for law enforcement and didn't really address the issue of terrorism.[76] In the years before the implementation of the ATA, the monitoring of communications might have been able to make a difference. On June 23, 1985 Sikh terrorists killed 329 people in the bombing of the Air India Boeing 747 flight. Of those on board, 154 Canadians perished. Although CSEC had been monitoring the communications of Sikh terrorists, using an operation set up inside the Canadian embassy in New Delhi since March 1983, their inability to connect the information to Sikh terrorist activities made it impossible for them to prevent the attack.[77]

The new ATA has allowed for some successes in information collection and monitoring. In March 2004, Momin Khawaja was arrested by the RCMP and charged for terrorism under the ATA. His arrest was directly supported by the information collection activities of CSEC and its allies; his arrest was made in Canada, but he was named a co-conspirator for terrorist activities in the UK.[78] Khawaja and eight others in the UK were charged with participating in or contributing to activities of a terrorist group and with facilitating terrorist activities. Khawaja was convicted of "five charges of participating in

---

[75]United Nations, "UN Action to Counter Terrorism," available from http://www.un.org/terrorism/strategy-counter-terrorism.shtml; Internet; Accessed 10 April 2009.

[76]Department of Justice Canada, "The Anti-Terrorism Act…" Available from http://canada.justice.gc.ca/eng/antiter/act-loi/contex.html; Internet; Accessed: 14 April 2009.

[77]Dwight Hamilton, *Inside Canadian Intelligence: Exposing the New Realities of Espionage and International Terrorism* (Toronto: Dundurn Press, 2006), 128.

[78]Hamilton, *Inside Canadian Intelligence.…*, 127.

a ‘terrorist group’ and helping to build an explosive device ‘likely to cause serious bodily harm or death to persons or serious damage to property.”[79]

This overview of the history of surveillance in Canada and the US demonstrates that surveillance and information exploitation have experienced some successes such as Japanese code breaking in the Pacific, Canadian Soviet spy expulsions, and the Khawaja conviction under the ATA. Unfortunately, the intelligence community has also been hampered by failures such as Pearl Harbor, the Sikh Air India bombing in 1985, and 9/11. The Pearl Harbor and 9/11 incidents show us that intelligence agencies, at times, continue to experience information sharing problems which prevent them from connecting the dots. As modern technical developments and government wrongdoing in both countries have highlighted, and in the words of Senator Frank Church, there is a:

> “…tremendous potential for abuse. The interception of international communications signals through the air is the job of NSA [and CSEC]; and, thanks to modern technology, it does its job very well. The danger lies in the ability of the NSA [and other intelligence agencies] to turn its awesome technology against domestic communications.”[80]

If Canada wishes to continue to support her allies around the world in the fight against terrorism, it is necessary for Canadians to continue to use surveillance as a tool in the arsenal of law enforcement and military agencies. Further, we must work to ensure that the surveillance of Canadians doesn’t subvert their rights and to prevent abuses similar to those in the past from happening again.

---

[79]Richard Fidler, “Afghan resistance is ‘terrorist’ under Canadian law, Khawaja trial judge rules,” *Global Research*, 10 November 2008; Internet; www.globalresearch.ca/PrintArticle.php?articleId=10874, accessed: 3 Apr 2009.

[80]EPIC, “Legality of NSA’s Secret Eavesdropping Program Is Suspect…,” 6.

> "I really believe that we don't have to make a trade-off between security and privacy. I think technology gives us the ability to have both."[81]
>
> - John Poindexter

PRIVACY AND SECURITY

With the explosive development of the information highway, democratic nation states find their citizens interconnected in a rapidly expanding global environment. As early as 1994, the Canadian government recognized the need for a strategy for Canada's information highway.[82] This information gateway would provide an ability to gather, store, transmit and exchange vast amounts of information. This capability would have positive benefits to individuals in potentially protecting citizens from acts of violence, but it would require added personal data protections or privacy guidelines to be put in place to avoid breaching the privacy of Canadians.

What is privacy? Privacy can defined in two parts, the right to be left alone, free from intrusion or interruption, and the right to exercise control over one's personal information.[83] A leading Information Technology (IT) developer, Edward Yourdon tells us that, in our imperfect world, the balance between security and privacy/liberty is affected by events inside and outside our borders. Prior to the terrorist attack of 9/11,

---

[81]Scott Berinato, "The Short Life, Public Execution and (Secret) Resurrection of Total Information Awareness," *CSO Magazine*, August 2004, Internet; http://hanson.gmu.edu/PAM/press2/ChiefSecurityOfficer-8-04.htm; accessed: 16 Mar 2009.

[82]Industry Canada, *The Canadian Information Highway: Building Canada's Information and Communications Infrastructure* (Ottawa: Spectrum, Information Technologies and Telecommunications Sector, April 1994), Ministers message.

[83]Industry Canada, *Privacy and the Canadian Information Highway* (Ottawa: Spectrum Information Technologies and Telecommunications Sector, October 1994), 5.

individuals or corporations refused the sharing of e-mail archives or installation of monitoring technologies; following the attack those same individuals were willing to give up privacy for some added security and to track down terrorists.[84] Yourdon hypothesizes that a perfect world would allow the achievement of the level of security our society demands for its protection without sacrificing the privacy and civil liberties guaranteed by its laws. The realist takes into account the many terrorist events, such as 11 September 2001 in New York and Washington and Bali in 2002, and reflects, like Sun Microsystems' Scott McNealy, "You have zero privacy anyway. Get over it."[85]

Some have concluded that the state poses the greatest threat to personal privacy.[86] Not only does the state have a limitless appetite for information on its citizens and the citizens of other nations, it also possesses unprecedented power to obtain such information. The assaults of Governments on privacy have been characterized as the "keyhole wars." The keyhole wars are separated into three areas:

- intelligence agencies seeking built-in trap doors to our information infrastructures to enable interception of and listening in or reading personal communications,
- government access to keys to codes that seek to keep information private and secure,
- weakening of privacy and security precautions available to private citizens, including limiting the use of encryption technology.[87]

---

[84]Ed Yourdon, *Byte Wars: The Impact of September 11 on Information Technology* (Upper Saddle River, NJ: Prentice Hall PTR, 2002), 68.

[85]*Ibid.*, 67.

[86]Harry Henderson, *Privacy in the Information Age* (New York: Facts On File, 1999), 9.

[87]Charles J. Sykes, *The End of Privacy* (New York: St. Martin's Press, 1999), 155.

It is no wonder that civil rights activists have concluded that the information of private citizens is at risk. As part of their contribution to the keyhole war, the NSA has developed the "Clipper Chip",[88] a device to provide encryption for personal communications to be secured from all those who don't have the necessary "key", while providing trap door access for those with the required code. The conclusion is that this does not protect privacy, since personal communications are still subject to interception by the organization with that code; even if the public trusts that agency, there is still no privacy. The counter argument was voiced by the US government executive under President Clinton. Vice President Gore endorsed the idea that through the clipper chip's key escrow technology, private communications would be protected while also allowing government access, via court order, to information for national security purposes.[89] The average citizen knows that a device is present to provide secure point-to-point communications, but is unaware of the backdoor. The end result is a population that incorrectly believes communications are secure and private.

Is it a balancing between national security and protection of a nation's information collection and the need for government transparency and openness? In both Canada and the US, the views are varied. During the roundtable series of discussions conducted by the Public Policy Forum in March 2008, this situation was summarized by one attendee in the following statement: "One of the real frustrations is that it's politically

---

[88]Ann Cavoukian & Don Tapscott, *Who Knows: Safeguarding Your Privacy in a Networked World* (Toronto: Random House of Canada, 1995), 142.

[89]EPIC, *The Clipper Chip*, Internet; http://www.epic.org/crypto/clipper/default.html; accessed: 16 April 2009. The Q&A session of 4 Feb 1994 describe the system being "more secure than other voice encryption system[s] readily available today. The algorithm…will remain classified to protect the security of the system. An independent panel of cryptography experts…concluded that it will be 36 years until the cost of breaking the algorithm will equal the cost of breaking the current Data Encryption Standard."

incorrect to say other interests sometimes override privacy…we need to talk about that balancing act."[90] The same forum ultimately concluded that "privacy and security must not be considered at odds with one another" and that "[t]he privacy of Canadians shouldn't be sacrificed on the altar of fighting terrorism..."[91] The CATO Institute in the US recognizes the two extremes that "we should reject uncompromising views of national security" at one end of the spectrum versus "…civil liberties cannot be allowed to trump national security…" at the other.[92] Canadian and US authorities view the perceived conflict between security and privacy as no conflict at all and conclude that these two ideals aren't mutually exclusive.[93] From a legal perspective Canada does have the ability to limit the risk and/or release of national secrets while providing the Canadian people with more openness. The Personal Information and Electronic Documents Act (PIPEDA) sets ground rules for the private sector, however, it also makes stipulations for information sharing guidelines with government agencies for security purposes. This Act recognizes the ideals of security and privacy and the need to have rules in place to provide for both without circumventing one for the other. Similarly, the US Department of Homeland Security (DHS) has not adopted the idea of "balancing privacy against other values because that paradigm results in a zero-sum outcome with privacy often

---

[90]Michael Lister and Katherine Baird, "Outcome Report," *The Federal Privacy Regime Roundtable Series* (Ottawa: Public Policy Forum, March 2008), 4.

[91]Jim Bronskill, "Don't let national security trump privacy: report," *The Canadian Press* 10 November 2008. Available from http://www.metronews.ca/ArticlePrint/138965?language=en; Internet; Accessed: 19 Nov 2008.

[92]Robert A. Levy, *Ethnic Profiling: A Rational and Moral Framework*, available from http://www.cato.org/pub_display.php?pub_id=5399; Internet; Accessed 31 Mar 2009.

[93]Robert Popp and John Poindexter, "Countering Terrorism through Information and Privacy Protection Technologies," *IEEE Security & Privacy: Data Surveillance 2006*, IEEE Computer Society; available from http://www.computer.org/security; Internet; Accessed: 4 April 2009.

diminished at the expense of security."[94] The same position is taken by Dr. Ann Cavoukian, the Ontario Information Privacy Commissioner, and Dan Tapscott that "we must opt for a "positive-sum" scenario wherein privacy and security can co-exist."[95] These experts envision a way of allowing privacy and security to co-exist, but seem to rule out the idea of "balancing" the two, which might lead to a situation where our security is sacrificed for privacy. The end result would create a situation where intelligence agencies could use all possible technologies, but where their use would be based on fair information practice principles that protect privacy and safeguard personal information.

What are those fair information practices? There are variations from country to country, however, they are grounded in international guidance from the Protection of Privacy and Trans-border Flows of Personal Data developed in September 1980 by the Organization for Economic Co-operation and Development (OECD).[96] The US signed onto this document as of 1980; Canada followed suit in 1984.[97] The OECD guidelines specify the following:

- Collection Limitation - limited to data obtained by lawful and fair means and when appropriate, with the knowledge and consent of the subject;

---

[94]Hugo Teufel, "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security," *DHS Privacy Policy Guidance Memorandum 2008-01* (Washington: The Privacy Office U.S. Department of Homeland Security, 29 Dec 2008), 2.

[95]Dr. Ann Cavoukian, "Privacy, security go hand in hand," *Metro*; Available from http://metronews.ca/ArticlePrint/142425?language=en; Internet; Accessed: 19 Nov 2008.

[96]Organization For Economic Co-Operation and Development, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," Sep 1980. Available from http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html; Internet; Accessed: 3 April 2009.

[97]Cavoukian and Tapscott, *Who Knows*…, 30.

- Data Quality - relevant to the purpose for which it is used and should be accurate, complete, and up-to-date;
- Purpose Specification - purpose specified at time of data collection and only used limited to the fulfillment of that purpose;
- Use Limitation - not disclosed or made available for purposes other than those specified unless consent or law permits;
- Security Safeguards - data should be protected from such risks as loss, unauthorized access, destruction, unwanted use, modification, or unwanted disclosure;
- Openness - includes policies on developments, practices, and data control;
- Individual Participation - includes one's ability to confirm data related to him, provide for denial of access requests, challenge the said data and have it erased, rectified, completed or amended for accuracy purposes;
- Accountability - the data controller (government agency) must comply with above principles.[98]

The US DHS's Privacy Policy Memorandum dated 29 December 2008[99] is rooted in the tenets of the US Privacy Act of 1974 and the use of fair information practice principles. The DHS's Chief Privacy Officer is responsible for the creation of all privacy policy development using the fair information principles as its foundation. The DHS regulates how these rules are applied and stipulates, for every security implementation

---

[98]Cavoukian and Tapscott, *Who Knows*…, 28.

[99]The Privacy Office, *Privacy Policy Guidance Memorandum: The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (Washington: U.S. Department of Homeland Security, 29 Dec 2008), 3-4.

involving collection of personally identifiable information, that impact assessments and System of Records Notices are conducted.[100]

The same legal principles apply in Canada through our Privacy Act, the PIPEDA, and the role of the federal Privacy Commissioner which includes implementation, as in DHS, of Privacy Impact Assessments (PIA).[101] Canada's 10 principles "form the ground rules for the collection, use and disclosure of personal information. These principles give individuals control over how their personal information is handled…"[102]

The development of privacy policies for the international community allows for privacy concerns to lead systems development and for the design of new technologies both to collect information and to aid in the protection of that information. The end result should be a "win-win" for privacy protection and national security.[103]

Exploitation: Data Mining & Information Sharing

The pace of change in the telecommunications and information management worlds has moved from evolutionary to truly revolutionary.[104] The advent of the internet

---

[100]The Privacy Office, *Privacy Policy Guidance Memorandum: The Fair Information Practice Principles…*, 3.

[101]Office of the Privacy Commissioner of Canada, *Protecting Privacy in an Intrusive World* (Ottawa: Parliament, July 2006), Internet: http://www.privcom.gc.ca/parl/2006/PIPEDA_review_060718_e.asp; accessed: 17 April 2009. Canada was the 1st national government in the world to make Privacy Impact Assessments (PIA) mandatory for all government departments (see: http//www.privcom.gc.ca/fs-fi/02_05_d_33_e.asp).

[102]The Office of the Privacy Commissioner of Canada, *Your Privacy Responsibilities: Canada's Personal Information Protection and Electronic Documents Act* (Ottawa: Privacy Commissioner, September 2006), 5.

[103]Green College and Ann Cavoukian, *National Security in a Post-9/11 World: The Rise of Surveillance…the Demise of Privacy?* (Toronto: Information and Privacy Commissioner/Ontario, May 2003), 57. See pages 45-55 for a good overview of the Privacy, National Security and the New Model of a positive sum game.

protocol (IP), the use of the client/server model via the internet, and the infrastructure to support this speed-of-light superhighway has resulted in the unpredictable routing of the internet's messages. Though information flow is predicable in a closed network, the routing of information over the vast network of the World Wide Web is done on an availability basis and information may travel over the network in unexpected ways. This means that a personal e-mail may be routed to several hubs within Canada before reaching its destination. To manage this message traffic it has become necessary to create distributed storage capacity to retain this information in near real time with on-demand information updates and changes. In this environment of computer networks and connected databases, data mining and matching has grown both in the private and public domains.

Data mining is defined as the use of sophisticated data analysis tools to discover previously unknown, valid patterns and relationships in large data sets. These tools include statistical models, mathematical algorithms, and machine learning methods i.e. neural networks or decision trees that improve their performance automatically.[105] Implementation and oversight issues require further study; these issues include data quality, interoperability, mission creep, and finally privacy. Data quality relates to the accuracy and completeness of the data. In the analysis of data collected, the chances of a "false positive" based on a targeted pattern can have very disastrous consequences to the ordinary citizen. Interoperability relates to the mining of database software and databases used by different government organizations and our allies as we look to share our

---

[104]Chief CSE, "Special Senate Committee Chief CSE Appearance…" 11.

[105]Jeffrey Seifert, "Data Mining and Homeland Security: An Overview," *RL31798 CRS Report for Congress* (Washington: Congressional Research Service, 5 Jun 2007), 1.

information. Mission creep and privacy are very much related because it refers to the use of information for purposes other than those originally intended and stated for collection.[106]

In the US, data mining has been considered a very important tool for identifying terrorist threats and activities. The data involved in this mining includes tracking money transfers, communications, travel, and immigration records. Research by the Defense Advanced Research Projects Agency (DARPA), has created numerous data mining applications to assist in the US "war on terror".[107] These projects have come under close scrutiny by privacy organizations such as the CATO Institute[108] and EPIC[109] with respect to data collected via warrantless means and to the manipulation of relationships with telecommunications companies for total information access instead of specific targeted communications.

The first high profile Data Mining project was Total Information Awareness, renamed later Terrorist Information Awareness (TIA), under the leadership of Adm (ret'd) John Poindexter within the DARPA Information Awareness Office (IAO). Using connectivity to a wide array of databases, intelligence based on a particular pattern of suspicious behaviour could be mined. The data included credit card purchases, car

---

[106]Seifert, "Data Mining and Homeland Security: An Overview…," Summary.

[107]Popp, "Countering Terrorism through Information and Privacy Protection Technologies…" 19. These tools have included intelligence collaboration, text analysis and decision aides, natural language processing, pattern analysis, and predictive modeling.

[108]Jeff Jonas and Jim Harper, *Policy Analysis: Effective Counterterrorism and Limited Role of Predictive Data Mining* No. 584 (Washington: CATO Institute, 11 Dec 2006), 8. Jonas and Harper reflect on false positives as Jeffrey Rosen outlined in his book, *The Naked Crowd*, to identify the 19 hijackers from the 9/11 attacks assuming a 99% accuracy rate while searching the 300 million American population would result in 3 million identified as potential terrorists.

[109]EPIC, ~~*Total*~~ *"Terrorism" Information Awareness (TIA)*, Internet; http://epic.org/privacy/profiling/tia/default.html; updated 21 March 2005; accessed: 3 April 2009.

rentals, and travel reservations. The result was a product that an analyst could use to develop watch lists, profiles or specifically flag individuals as suspicious. The project also included a language translation capacity, data search with pattern recognition and privacy protection, and advanced collaborative and decision support tools. The project's failure was the result of many issues that included civil libertarians' concerns over mission creep (from counter-terrorism to tax collection, for example), that centralized data repositories won't stop terrorists[110], that terrorist-incident data sets would be too small to be useful as valid predictive models, and that there are "no meaningful patterns that show what behavior indicates planning or preparation for terrorism." [111] Dr. John M. Poindexter's involvement in the effort coupled with the above concerns caused the US civil liberties community to question the true motives of the project;[112] the public perception of the project logo with an "all-seeing" eye on top of a pyramid overlooking a globe and a theme of "knowledge is power" spelled its cancellation.[113] Their main concerns were that the project would work backwards; assuming all citizens were terror suspects without either a reasonable or probable cause, that though the project focused pre-emptive measures against terrorists, it would now allow targeting government dissenters, political threats, or common crimes as in the 60's and 70's, and that this type

---

[110]Jane Black, "Snooping in All the Wrong Places," *Business Week: Privacy Matters*, 18 Dec 2002; Internet; http://www.businessweek.com/print/technology/content/dec2002/tc20021218_8515.htm; accessed 2 Apr 2009.

[111]Joe W. Pitts, "Under Surveillance: The End of Illegal Domestic Spying? Don't Count on It," *The Washington Spectator* (Washington: Public Concern Foundation Inc., 15 Mar 2007), Internet; http://www.washingtonspectator.com/articles/20070315surveillance_1.cfm; accessed: 8 Mar 09.

[112]Prior to his work in TIA, Dr. Poindexter was involved in the Iran-Contra Afffair as part of his duties as the National Security Advisor to President Ronald Regan. Poindexter had become familiar to the public as a result of this activity. Many in the civil liberties movement distrusted Dr. Poindexter.

[113]Jeffery Seifert. "Data Mining and Homeland Security: An Overview…" 7.

of technology would lead to dragnet surveillance, thereby overwhelming an already overworked security community and would be the next step in a totalitarian society.[114] Following the failure of TIA and faced with an American public's ever increasing use of electronic tools, the US government implemented policy under the E-Government Act of April 2003 that required privacy impact assessments (PIA) to be conducted on all future projects of this nature.[115] The PIA's would ensure that each agency's information handling conformed to legal, regulatory, and policy requirements based on privacy, risks to privacy, and handling protections and processes to mitigate those risks.

US Congressional oversight of information collection projects was assigned to the US' Government Accountability Office (GAO), formally known as the General Accounting Office (GAO). The GAO is responsible for investigating how the US federal government spends taxpayer dollars,[116] but does make suggestions on how government departments can best serve the public. In direct response to the 11 September 2001 attacks other projects were developed to improve national security including the Computer-Assisted Passenger Prescreening System (CAPPS and CAPPS II) which then transitioned to the Secure Flight program under the Transportation Security Agency

---

[114]Timothy B. Lee, "Electronic Surveillance," *CATO Handbook For Policymakers* 28 (Washington: CATO Institute, 2009), 305-306.

[115]Sayaka Kawakami and Sarah C. McCarty, "Privacy Year in Review: Privacy Impact Assessments, Airline Passenger Pre-Screening, and Government Data Mining," *A Journal of Law and Policy For The Information Society* Vol. 1, Issue 2-3 Spring/Summer 2005 (Columbus: Moritz College of Law, 2005), 222. The Act outlined that each government agency "conduct privacy impact assessments before developing or producing information technology that collects, maintains, or disseminates information that is in an identifiable form."

[116]Government Accountability Office, "About GAO," Internet; www.gao.gov/about/index.html, accessed: 18 April 2009. The Budget and Accounting Act of 1921 requires the "GAO investigate at the seat of government or elsewhere all matter relating to the receipt, disbursement, and application of public funds and shall make to the President…and to Congress…reports [and] recommendations looking to greater economy or efficiency in public expenditures." Legal and ethical oversight remains with the US Congress.

(TSA) for passenger screening. Though similar to TIA, the GAO found TSA's interoperability linkages and data capture mechanisms were in compliance with the US Privacy Act; however, some data integrity and security issues were uncovered.[117] The TSA was found to have attempted to "balance privacy with…national security, and that policymakers would have the final determination as to whether TSA's balance was appropriate."[118] NASCIO concluded, in keeping with fair information practice principles, that:

> "transparency as to data mining program's purpose, the reason why information is collected, how it will be used, who will have access to the information, how it will be secured, and whether individuals can access and correct their personal information is key [to accepting introduction of this technology]."[119]

As a result of early intelligence communities' efforts to compartmentalize their information, a culture developed around the philosophy of "need-to-know" and much of the information was over-classified and kept back from information sharing efforts. In its 9/11 commission report, the US National Commission on Terrorist Attacks Upon the United States recognized that the "US government cannot meet its own obligations to the American people to prevent entry of terrorists without a major effort to collaborate with other governments."[120] The 9/11 commission concluded that more exchange of

---

[117]Gregory D. Kutz, *Data Mining: Results and Challenges for Government Program Audits and Investigations* GAO-03-591T (Washington: GAO, 25 March 2003); Internet; http://usacm.acu.org/usacm/testimony/GAODatamining.pdf; accessed: 18 April 2009. The GAO reported on a security breach at a Phoenix office of the Tri-West Healthcare Alliance that resulted in healthcare information and social security numbers of 500,000 military, retirees, and family members being stolen in Dec 2002.

[118]NASCIO, "Think Before You Dig: Privacy Implications of Data Mining & Aggregation," (Lexington, KY: NASCIO, Sept 2004), 9.

[119]*Ibid*., 4.

suspected terrorist information with trusted allies is required and that global security standards for travel and border crossing can only be increased through international cooperation. The "need-to-know" culture, with its perceived security procedures outweighing the benefits from information sharing, must change to a "need-to-share" culture and be built on a trusted information network.[121]

There are three data types that the 9/11 Commission saw as information that would potentially be within the scope of being shared. These are raw data, knowledge and intelligence. Raw data has little to no assessment with respect to the accuracy or implications of that information when collected, knowledge would include that information deemed to have a high degree of reliability or validity and intelligence would have been carefully evaluated concerning accuracy and significance and would sometimes be credited in terms of its source. It was determined that intelligence, homeland security, law enforcement, and critical infrastructure information in a combination of the above forms would facilitate better collaboration and information analysis. In order to do this, improved Information Technology (IT) and common information standards would be required.[122]

Following the 9/11 attacks and the 9/11 Commission's recommendations there have been focused information systems and network developments to better enable this information sharing. Examples of these systems include the Joint Regional Information Exchange System (JRIES), Homeland Security Information Network (HSIN), Automated

---

[120]Harold C. Relyea and Jeffrey W. Seifert, "Information Sharing for Homeland Security: A Brief Overview," *CRS Report for Congress RL32597* (Washington: Congressional Research Service, 10 Jan 2005), 5.

[121]Relyea and Seifert, "Information Sharing for Homeland Security…" 6.

[122]*Ibid., 8.*

Targeting System (ATS), Regional Information Sharing System (RISS) and its associated Anti-Terrorism Information Exchange module, and the Multi-State Anti-Terrorism Information Exchange (MATRIX).[123] Though several systems have again been extended to the point that their information collection threatens privacy considerations, because of the large amount of information collected, systems such as the RISS, with its interconnectivity with the law and intelligence organizations from Australia, Canada and the UK, have used secure intranet technology with digital rights management functionality to allow database owners the ability to regulate access and data manipulation. The new IT tools allow for mitigation of intentional abuse, security breaches, mission creep, and concerns about data aggregation. Technology alone cannot address all the concerns surrounding the complex issue of privacy, however, working within the existing legal frameworks, these new tools will allow for the scrambling of data for one-way exchange, building permission rules into the data and search engines to regulate access, and provide audit trails that can identify abuse. As Dempsey and Rosenzweig tell us, the total solution in countering terrorism will require a combination of policy, legal and technological advances.[124]

As a case-in-point of policy and legal requirements that were not met, the RCMP threw aside normal protocols to share information with their US counterparts with respect

---

[123]Relyea and Seifert, "Information Sharing for Homeland Security…" 9.

[124]James X. Dempsey and Paul Rosensweig, *Technologies That Can Protect Privacy as Information Is Shared To Combat Terrorism* (Washington: Center For Democracy and Technology, 26 May 2004), 3-4. Canada's "Flight Guardian" software, though still hampered by some data issues (See: Faisal Kutty, "Canada's No-Fly List: a False Sense of National Security," *Global Research*, 13 Jun 2007, Internet; www.globalresearch.ca/PrintArticle.php?articleId=5952, accessed: 3 Apr 2009) looks to implement some of these protections.

to Project A-O Canada and the activities of Maher Arar's possible terrorist ties.[125] Maher Arar's deportation to and detention in a Syrian jail and subsequent interrogations must flag a caution to total information sharing without proper controls in place such as signed authorizations and limits on the dissemination of information they shared with foreign agencies. Maher Arar was subsequently returned to Canada and found to be innocent of the charges.

Rapidly emerging technologies will continue to force law enforcement agencies and military organizations to work toward maintaining an "edge" on criminals and terrorists. As The Markle Foundation indicates, agencies at all levels of government are now interested in collecting and mining large amounts of data from commercial sources to combat the continuing threat of terrorism around the world, but also to perform large scale data analysis and pattern discovery in order to discern potential activity by unknown individuals, some of those with the potential of using weapons of mass destruction.[126] The use of data mining and other new computer models will assist our governments' efforts to protect citizens. The Markle Foundation envisions the creation of a "Systemwide Homeland Analysis and Response Exchange Network (SHARE) that will empower all participants in protecting our security, and which would be governed by guidelines designed to protect our liberties."[127] This information collection serves no purpose if the information cannot be shared between agencies and with our allies within

---

[125]Maureen Webb, *Illusions of security: Global Surveillance and Democracy in the Post-9/11 World* (San Francisco: City Lights Books, 2007), 10. Though not part of this paper, the topic of Arar's dual citizenship was not widely publicized. This begs the question: was his deportation to Syria by American authorities even wrong?

[126]The Markle Foundation, *Creating a Trusted Information Network for Homeland Security* (New York City: The Markle Foundation, Dec. 2003), 5.

[127]*Ibid.*, 2.

reasonable timeframes. Considerable discussion with various allied nations is essential as we move forward with increased surveillance and information exploitation. As Dempsey and Rosensweig and The Heritage Foundation conclude: "IT properly designed and implemented with appropriate legal controls and oversight, offer potential for enabling government to act in support of vital national security concerns while also serving privacy and liberty interest."[128]

[128]Dempsey and Rosensweig, *Technologies That Can Protect Privacy…*, 15. James Jay Carafono, Todd Gagiano, and Alone Kochems, *Domestic Surveillance: Dual Priorities & Civil Liberties, Must be Met* (Washinton: The Heritage Foundation); Available from www.heritage.org/Research/HomelandSecurity/wm1950.cfm; Internet; Accessed: 18 April 2009.

> "Those who would give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety."[129]
>
> - Benjamin Franklin

THE ETHICAL DILEMMA – IS SURVEILLANCE A MORAL ACT?

In addition to the debate about privacy versus security, there are ethical and moral questions about surveillance, information collection and information exploitation as nations counter the domestic and international terrorist threat. A brief study of today's ethical theories, as they apply to national security and privacy, is helpful to better understand our governments' increasing reliance on information and intelligence in the war on terror. The use of these theories will help us determine the ethical merits of our actions and our expanding reliance on information collection and information exploitation technologies.

To assist in comparing and contrasting the ethical and moral theories, four principles of information gathering activities must be considered as we go through this analysis. The first principle is that a government must take steps to understand foreign or terrorist threats to its citizens as well as the nation as a whole.[130] The second principle is that the state should use the least intrusive means of information collection, for instance not "spy" when information can be gathered in an open way. The historical adage that "Gentlemen do not read other's mail" is dangerous when a nation's security is in

---

[129]Jennings, *Benjamin Franklin…*, 117.

[130]Arthur S. Hulnick and Daniel W. Mattausch, "Ethics and Morality in U.S. Secret Intelligence," *Ethics of Spying: A Reader for the Intelligence Professional* (Toronto: The Scarecrow Press, 2006), 40.

question.[131] The third principle is that information collection and analysis must not be affected by bias or political manipulation and lastly, our forth principle is the requirement to use counterintelligence mechanisms to protect our own national security information from theft.[132]

Surveillance and information exploitation could be considered to be correct and morally justifiable as long as they are conducted on the basis that they are needed to allow the state to protect its citizens. From the tenets of western democracy the primary responsibility of a sovereign state is to secure the welfare of its people. John Smith wrote that "the sole end for which mankind are warranted, individually or collectively in interfering with the liberty of action of any of their number, is self-protection."[133] Within a state then, certain rights and privileges are conferred on citizens to ensure human dignity. The state has a duty or obligation to protect and respect these rights and freedoms even when its citizens are unable to do so themselves. Basic human rights as encapsulated in the 10 Dec 1948 United Nations Universal Declaration of Human Rights include things like the right to life, liberty and security of person (Article 3), no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation (Article 12), and in the exercise of rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements or morality, public order and the general

---

[131]Hulnick and Mattausch, "Ethics and Morality in U.S. Secret Intelligence…", 41.

[132]*Ibid.*, 42.

[133]John Stuart Mill, *On* Liberty (New York: Dover Publications, 2002), 8.

welfare in a democratic society (Article 29 (2)).[134] Modern philosophers have extended some of the rights on this list, such as privacy, due in large part to new technological advances that transcend those barriers that historically protected personal information.[135]

Kantianism

Kantianism is the ethical theory developed by the German philosopher Immanuel Kant, to explain how actions ought to be guided by moral laws and that these moral laws are universal.[136] Kant "believed that an act has specifically moral worth only if it is done with a right intention or motive."[137] In outlining his theory, Immanuel Kant described categorical imperatives that provide for moral absolutes or obligations to be tested. The first formulation suggests that we should "act only from moral rules that you can at the same time will to be universal moral laws."[138] Kant's second formulation specifies that you "act so that you always treat both yourself and other people as ends in themselves, and never only as means to an end."[139] These imperatives are further broken down into decision rules as follows:

---

[134]Iain Atack, *The Ethics of Peace and War: From State Security to World Community* (New York: Palgrave MacMillan, 2005), 45. United Nations, *Universal Declaration of Human Rights*; Internet; http://www.un.org/Overview/rights.html; accessed: 4 Apr. 2009.

[135]Michael J. Quinn, *Ethics for the Information Age - 3rd Ed*. (Boston: Pearson Education, 2009), 84 and Marx, *The World and I, Privacy and Technology*, 1.

[136]*Ibid.*, 69.

[137]Barbara MacKinnon, *Ethics: Theory and Contemporary Issues, 2nd Ed.* (Belmont, CA: Wadsworth Publishing, 1998), 53.

[138]Quinn, *Ethics for the Information Age…*, 70.

[139]*Ibid.*, 71.

- Categorical Imperative (CI); act in a way that your behavior would stand as a universal law,
- Principle of Ends (PE); that every human being has intrinsic dignity and worth and that all should act to treat everyone as an end and not as a means to an end, and finally,
- Principle of Autonomy (PA); any rational being will, through reason, come to the same moral principles to be acted on.

All three of Kant's decision rules conclude that information collection and exploitation is not justified. Firstly, the collection of information and its use cannot be seen as a universal law. The Categorical Imperative would require that information collection is binding on all persons at all times and that this principle could be universally applied to everyone for the overall good of society. With respect to surveillance and information collection this is just not true. Secondly, individuals are treated as a "means" to attain the "end", that being the security of the state. Monitoring the private communications of individuals, treats those individuals as tools in the fight against terror. Thirdly, not all rational beings will come to the conclusion that intelligence gathering is justified. By definition, information collection and exploitation depends on secrecy, deception and manipulation. Under Kant, it is clear that no state can violate the rights of the citizens of any state, such as the right to privacy, without violating the universal moral law. Additionally, no state can declare its ends superior to those of any other state.[140]

---

[140]James M. Olson, *Fair Play: The Moral Dilemmas of Spying* (Washington: Potomac Books, 2006), 25.

As Valerie Steeves, University of Ottawa criminologist indicates, in our post 9/11 society we are obsessed with the need to eliminate risk and as a result we have lost trust in the governments formed to protect our society; everyone is treated as a suspect.[141] In part, this trust has been destroyed by today's extremists and their direct attacks on western values. This lack of trust now extends to our treatment of individuals and has forced the state to rob our citizens of this trust.[142] The use of surveillance and information collection methods have been justified in the name of national security; however, overt surveillance, according to Jane Bailey of the University of Ottawa, "…feeds the whole notion of societies of suspicion…[and] the notion of the risk society and engenders more mistrust between members of society."[143] Once again, this situation fails the test of Categorical Imperative; our behaviour has resulted in negative consequences to trusting our fellow man and therefore, can't be seen as a universal law.

Utilitarianism

The Utilitarianism theory was first proposed by English philosophers Jeremy Bentham, generally regarded as the father of utilitarianism, and John Stuart Mill.[144] The

---

[141]Don Butler, "Exposing our lives to pervasive, prying electronic eyes," *Ottawa Citizen* 7 Feb 2009; Internet; http://www.edmontonjournal.com/story_print.html?id=1264103&sponsor=; accessed 9 Feb 2009.

[142]Tony Pfaff, "Bungee Jumping off the Moral High Ground: Ethics of Espionage in the Modern Age," *Ethics of Spying: A Reader for the Intelligence Professional* (Toronto: The Scarecrow Press, 2006), 77.

[143]Butler, "Exposing our lives to pervasive, prying electronic eyes…" Ulrich Beck, *Risk Society: Towards a New Modernity* (Munich, Germany: Sage Publications, 1992), 34. "In the risk society, the past loses the power to determine the present. Its place is taken by the future, thus, something non-existent, invented, fictive as the 'cause' of current experience and action. We become active today in order to prevent, alleviate or take precautions against the problems and crises of tomorrow and the day after tomorrow – or not to do so."

consequentialist principle, also called act utilitarianism, considers that an "action is good if it benefits someone; an action is bad if it harms someone."[145] This equates to the ends and not the means that count. In contrast, as Michael Quinn writes, the principle of utility can be used as a "yardstick" to judge all actions in the moral realm. This involves determining likely outcomes, good or bad, for each action, calculating the net good for each act, and then selecting the action that will provide for the greatest good for the greatest number. This utility principle, also known as rule utilitarianism, holds that "we ought to adopt those moral rules which, if followed by everyone, will lead to the greatest increase in total happiness."[146]

Prior to the twenty-first century states had no inherent right of privacy against other states. In the international environment, state to state surveillance and information exploitation looked at "whether it [was] good or bad for international society…[if] it promotes…responsible government behavior, good inter-state relationships, the minimization of tension, co-operation …, and the avoidance of war."[147] 9/11 saw a renewed emphasis on counter-terrorism and the associated information collection activities that had been in existence for at least 30 years. As reported in January 2003, since the 11 September 2001 terrorist attacks, 100 terrorists had been thwarted world-wide and a total of 3,000 suspects detained throughout 100 countries.[148] Eavesdropping

---

[144]Olson, *Fair Play*…, 27.

[145]Commander G.A. Hannah, "Seizing and Holding the Moral High Ground An Introduction to Ethical Theories" (Toronto: Canadian Forces College, 2006), 12.

[146]*Quinn, Ethics for the Information Age…*, 79.

[147]Michael Herman, "Ethics and Intelligence after September 2001," *Intelligence and National Security* 19, No. 2 (London: Frank Cass & Company, Summer 2004), 344.

on national and international communications made these discoveries possible. Western societies have always had "an aversion to Big Brother watching, however, there is now an understanding that there is a justifiable need…[for surveillance] under law and public opinion."[149] From a utilitarian perspective this surveillance and information exploitation or intelligence sharing has "reduced irresponsible and ignorant behavior and [on] balance made the world better; but some of the activities producing [and collecting] it made the world marginally worse."[150] In light of the new threat, those non-state targets, the use of new methods such as increased surveillance and information exploitation cause us no qualms with respect to the possible effects on society when considering international security and humanitarianism as the motives. The end justified the means.

When information collection is targeted at specific terrorist threats, from a utility perspective, increased information collection is justified. When data mining efforts and projects such as TIA or MATRIX collect targeted personal information, the cases of abuse of individual citizen's privacy will be isolated incidents and incidences of ethnic profiling will be rare. As James Olson indicated, Bentham and Mill both elevated security to a special status in their hierarchy of happiness. It is not surprising that considering the use of TIA and MATRIX, with their focus on defence and national security, the end justifies the means because these systems contribute to the greatest happiness of the greatest number of Americans.[151]

---

[148]Herman, "Ethics and Intelligence after September 2001…", 348.

[149]Stephanie Sanborn, Owen Linderholm, and Cathleen Moore, "Privacy concerns raised," *INFOWORLD* 23, Issue 38, 19 Sep 2001; Internet; www.infoworld.com; accessed: 13 Mar 2009.

[150]Herman, "Ethics and Intelligence after September 2001…", 346.

[151]Olson, *Fair Play.*.., 28-29.

Let's now switch our study to those carrying out the surveillance or data collection from those being watched. Gary Marx tells us that the principle of proportionality[152] in which the means and ends stand in appropriate balance is a possible ethical approach in the uses of surveillance data. This principle enables us to think comparatively about means and whether there are "less costly means available?" The measures can involve significant risks and costs and in the end, given the goal of a particular surveillance technique, steps are taken to minimize costs and risks. The problem that we need to be cognizant of is the possibility that publicly stated goals may mask other less desirable goals. In determining the ethical use of surveillance, the following factors need to be considered: appropriate vs. inappropriate goals, goodness of fit between the means and the goal, if information is used for original vs. other unrelated purposes, how to share gains from the information, and if unfair harm or disadvantage may occur to those being watched. As Gary Marx concludes, in the case of the watcher, the more the above factors are applied the more ethical the situation is likely to be; the less the factors are applied, the less ethical the surveillance.[153]

In keeping with the utilitarian theory, it can be concluded that if one can monitor people's communications or obtain added information to isolate extremism, then it should be done. From a utility point of view, what is important is that things turn out for the best. Gary Marx would have us utilize a measure of the means to the way in which we focus our approach to the end goal. Though it is important to consider risks, costs, and

---

[152]Gary T. Marx, "An Ethics For The New Surveillance," *The Information Society* 14, no. 3, 1998. available from http://web.mit.edu/gtmarx/www/ncolin5.html; Internet; Accessed: 22 April 2009. 14-16.

[153]*Ibid.*, 17.

long term consequences, surveillance and information exploitation, even if they are somewhat harmful, are justified.

Social Contract Theory

Philosopher Thomas Hobbes argued in his book "Leviathan" that without rules and the means of enforcing them, people would not bother to create anything of value, because nobody could be sure of keeping what they created. This position is a result of his direct observation of the terrible consequences of the English civil war in the 1600s and his observations of anarchy in social society. Hobbes called the anarchistic state the "state of nature"; his view was that the only way to bring society out of this state was through its people working in cooperation based on specific guidelines. Hobbs concluded that civilized societies have agreed to live by two things: "the establishment of a set of moral rules to govern relations among citizens and [supporting] a government capable of enforcing these moral rules."[154] This is the beginning of the enactment of a "social contract". Philosopher Jean-Jacques Rousseau continued Hobbes' work by concluding that authority among men must be based on covenants. Because Rousseau determined that society's critical problem was finding a way to guarantee everyone's safety and property while enabling everyone to remain free, he concluded that everyone must give themselves and their rights to the whole community. The community would determine those moral rules and each member would then be obliged to follow them. Rousseau and Hobbes, therefore, see the Social Contract giving a person's actions a moral quality due their membership in the civil society and that the "voice of duty" has

---

[154]Quinn, *Ethics for the Information Age…*, 83.

replaced the "state of nature." In summary, Social Contract Theory concludes that "morality consists in the set of rules, governing how people are to treat one another, that rational people will agree to accept, for their mutual benefit, on the conditions that others follow those rules as well."[155] John Rawls, revived the Social Contract in the twentieth century and expanded it to include the Theory of Justice and to allow for the unequal distribution of wealth and power. Rawls added the idea of rights and liberties for all versus moral rules and the difference principle that recognizes the possibility that inequalities can be associated with positions in society as long as everyone has the fair and equal opportunity to assume these positions. In his theory, those inequalities must be justifiable.[156] The Social Contract theory and additions such as the Rawls Theory of Justice helps us look at ethical and moral dilemmas from a logical and analytical point of view and will be used as a valid ethical theory.

In using the Social Contract theory, the question of rules becomes the central focus. Everyone benefits when everyone bears the burden of following certain rules. The rules include protection of a citizen's right to safety, liberty and privacy. Let's review a few examples where these rules were not followed. In the Richard Helms perjury case, Helms lied to the Senate Defence Committee with respect to CIA involvement in a coup in Chile, placing the organization for which he worked above the interests of his government and, hence, his society. This example demonstrates a government official contravening American liberties of trust and justice. In another example, General Lemnitzer, former US Department of Defense Joint Chief of Staff, was

---

[155]Quinn, *Ethics for the Information Age…*, 84.

[156]*Ibid*., 85.

involved in the planning of the Bay of Pigs fiasco that resulted in loss of American lives; this is a breach of the right to safety. The NSA Minaret domestic surveillance program has been shown to be counter to US laws and has faced severe public scrutiny over privacy issues; it is a fundamental breach of the right to privacy. This 1960's program was a domestic watch list shared by the FBI, Secret Service, military and the CIA to track threats to national security. As Lieutenant-General Lew Allen Jr., former NSA Director, testified to the US Senate Select Committee to Study Governmental Operations With Respect to Intelligence Activities (commonly known as the Church committee) in 1975, the list contained information on over 1,200 American citizens with respect to phone conversations collected over a six year period. The list included civil rights leaders such Dr. Martin Luther King, Jr and those involved in anti-war activities.[157] Even today, David Fewer, acting director of the Canadian Internet Policy and Public Interest Clinic (CIPPIC) indicates that "Canada has a recent history of abuse of process in both criminal and national security settings…"[158] These examples lead us to conclude that the temptation to break the social contract in the face of what some individuals would deem to be higher order duties and responsibilities is immense.

Based on Social Contract theory, a valid argument for increased surveillance and information exploitation can be made when the society is made aware of the surveillance and the tacit permission of citizens is gained. Since each individual has a responsibility to share in the contract, the citizens would feel they had a stake in complying with the need for increased surveillance and that they would benefit from the increased safety

---

[157]EPIC, "Legality of NSA's Secret Eavesdropping Program Is Suspect…" 2.

[158]Nestor E. Arellano, "Feds to push Web eavesdropping bill," *NetworkWorld* 19, no. 6, 20 Mar 2009, 9.

provided by that surveillance. Before any surveillance program can be considered acceptable, the checks and balances have to be in place to combat people acting out of self-interest and immoral ideals. The second part of the social contract theory provides for society to punish those who commit crimes against those rules or laws which are in place to protect the citizens' rights. This is a safeguard for society against the abuse of the power conferred by allowing government to use internal surveillance i.e. to spy on its own citizens.

The study of the frameworks of Utilitarianism and Social Contract Theory as they apply to information collection and data exploitation have supported the morality of increased surveillance and information sharing. Certain balances, as purported by Gary Marx would be necessary to further support the use of surveillance. Kantian philosophy concludes that any surveillance and information exploitation is difficult to defend; however, any moral dilemma will inevitably leave some issues unresolved and some conflict of values and needs is unavoidable. The government must attempt to provide the best possible end result. Canadians expect that governments will endeavour to apply moral and ethical standards to all situations and with all technologies, in this case surveillance and information exploitation to counter the terrorist threat and provide for national security, especially when our liberties are threatened.

Looking back to the history section of this paper, we are left with the question, were the Security Service Mounties in the 1970's, those involved in the rise of illegal wire-tapping activity, ethically correct? They would say that their

"acts were morally right and view impeding legal statutes only as technical barriers, not ethical ones."[159]

[159]John Sawatsky, *Men in the Shadows: The RCMP Security Service* (Toronto: Doubleday Canada Limited, 1980), 252.

"To stop terrorists before they strike, we must do three things: deny them entry into the country, curtail their freedom of action inside the country, and deprive them material and moral support from within the country."[160]

- Richard Perle

THE LEGAL ASPECTS

Canada's national security policy stipulates that there is no greater role or obligation of the government than the protection and safety of its citizens.[161] Canadians are well aware of the new threat(s) to our liberty and quality of life as a result of the al-Qaeda attacks on 9/11. Our national security policy clearly outlines the need for all threat related information to be brought together and acknowledges that Canada needs an enhanced intelligence collection capacity to counter the criminal nature of international terrorism.[162] Despite the need for these powers to be augmented, Canadians still insist on the right to privacy; the right to freedom from intrusion and the right to control personal information are important to Canadians. Even if Canadians agree to a reduced level of privacy to help secure the country, they insist that they must have the right to voice their concerns.

So what does the law have to say on this issue? Canadian democratic values, as outlined in the Canadian Constitution, include peace, order and good government. In his speech "We have to rethink privacy protection," during the Organization for Security and Cooperation in Europe (OSCE) Human Rights and Terrorism seminar, Professor Viet Dinh of Georgetown University concludes that true liberty exists only in an ordered

---

[160]David Frum and Richard Perle, *An end to evil: How to win the war on terror* (New York: Ballantine Books, 2004), 120.

[161]Privy Council. *Securing an Open Society…*, 5.

[162]*Ibid*., 6.

society with rules and laws that govern its people.[163] A review of the legal aspects of personal information collection, information exploitation, and national security versus terrorism is required to better comprehend our legal rights and security in this revolutionary and chaotic information age. This review will include an overview of US and Canadian Privacy laws and a detailed look at the USA PATRIOT Act and the Canadian Anti-Terrorism Act (ATA).

Privacy Laws

Although it will surprise many Canadians, neither the Canadian Charter of Rights and Freedoms, known as the Charter, nor the American Bill of Rights make mention of privacy, however, as Justice Brandeis correctly indicates, privacy is the "right most valued by civilized men."[164] The problem with the concept of privacy is it is a vulnerable legal construct in that it is not considered to be a basic human right in every society. Because of privacy's plural and diffuse nature, privacy laws have been developed by judges without a clear grounding in legal text or traditions; privacy has always been in jeopardy.[165] Limited legal privacy protection measures have not allowed for the resolution of issues that placed privacy in competition with other needs. This negative situation is summarized in the Peter Galison and Martha Minow conclusion that "…the idea that by sacrificing personal privacy we will achieve security at best reflects faulty

---

[163]OSCE, *Human Rights and Terrorism, Hall of Knights 18 Sep 2003* (The Hague: Netherlands Helsinki Committee, November, 2003), 75.

[164]Cohen, *Privacy, Crime and Terror*…, 9.

[165]Peter Galison and Martha Minow, "Our Privacy, Ourselves in the Age of Technological Intrusions," *Human Rights in the 'War on Terror,'* (New York: Cambridge University Press, 2005), 268.

analysis or magical thinking and at worst seeks to excuse failures to attend to immediate and difficult security dangers that require no sacrifice of privacy."[166]

US Privacy Laws

The US Privacy Act of 1974 was enacted to counter privacy concerns that evolved out of the Watergate era. The Act's fundamental intention is to make government agencies disclose their information-gathering and distribution activities and allow US citizens to learn what information has been collected about them and correct any errors. Law enforcement or intelligence activities could be blocked from disclosure for national security reasons. FISA, 1978, placed legal limits on government's ability to spy on citizens and stipulated that warrantless domestic wiretapping would be considered a criminal act. Nevertheless, FISA holds the government to a lower standard in gathering foreign intelligence; the requirement is to have "reasonable belief' that a terrorist act was to be committed rather than the "probable cause" required for domestic surveillance.[167]

Canadian Privacy Laws

In contrast to the privacy laws of other countries, Don Butler concludes that Canada has "more robust privacy laws."[168] For example, Canadian privacy laws would prohibit the establishment of a database of public officials like the one compiled in France and it is unlikely that Canadian intelligence agencies would be permitted to access

---

[166]Galison and Minow, "Our Privacy, Ourselves in the Age of Technological Intrusions…" 285.

[167]Joe W. Pitts, "Under Surveillance: The End of Illegal Domestic Spying…, 1

[168]Don Butler, "Part 1: A very different world," *Ottawa Citizen* 5 Feb 2009; http://www.ottawacitizen.com/story_print.html?id=1232203&sponsor=; Internet; Accessed 9 Feb 2009.

telecom records without judicial authority as police in the UK can.[169] The Charter, the Privacy Act of 1974, and the Personal Information Protection and Electronic Documents Act (PIPEDA) of 2001 reinforce this position. Further, PIPEDA establishes a Privacy Commissioner of Canada as the ombudsman for complaints under this new law.[170] Still, some Canadians share the views of Ms Philippa Lawson, the former director of the Canadian Internet Policy and Public Interest Clinic (CIPPIC), that "behavioral targeting violates the PIPEDA, Canada's private-sector privacy law".[171] In contrast to Ms. Lawson, Canadian scholars agree that the focus of the Privacy Commissioner who oversees the federal Privacy Act has lead to "pressure for stronger security measures" with a better privacy framework.[172] There are many stresses on maintaining vigilance to protect privacy. The digital information revolution that has included the internet, global positioning systems, and wireless technology has outpaced the legal community; however, scholars continue to see privacy and security "mutually reinforcing" our new surveillance society.[173]

---

[169]Butler, "Part 1: A very different world…" *Ottawa Citizen* 5 Feb 2009.

[170]Office of the Privacy Commissioner of Canada, *Protecting Privacy in an Intrusive World…*, available from http://www.privcom.gc.ca/parl/2006/PIPEDA_review_060718_e.asp; Internet; Accessed: 17 April 2009.

[171]Don Butler, "Part V: You've been targeted," *Ottawa Citizen* 5 Feb 2009; http://www.ottawacitizen.com/story_print.html?id=1249220&sponsor=; Internet; Accessed 9 Feb 2009.

[172]Thomas Gabor, *Views of Canadian Scholars on the Impact of the Anti-Terrorism Act* (Ottawa: Department of Justice, 31 Mar 2004), 6.1.

[173]*Ibid*., 6.2.

Anti-Terrorism Acts

A significant theme following the 9/11 attacks in the US was an effort to clearly define what constitutes an act of terrorism. The US and Canadian governments have been unable to reach the "holy grail" of defining what a terrorist is. Nevertheless, there is agreement on some of the features of terrorism; it is generally held that terrorist acts "…intentionally intimidate the public or compel a government to do or refrain from acting in a certain way, and are intended to kill, seriously harm or endanger people, or substantially damage property or disrupt essential services."[174] With this in mind, both Canada and the US have created legislation to aid in anti-terrorism activities. What follows is a review of the US and Canadian legislations following 9/11 to counter the terrorist threat.

USA PATRIOT Act

The United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act was passed on October 2001, in the shadow of the September 11, 2001 attacks on the World Trade Centre and Pentagon, under the direction of the George W. Bush administration. The language of the act largely augments and amends previous US federal legislation such as the Radio Communications Act (1934) and the Foreign Intelligence Surveillance Act (1978). Some changes resulting from the act were to be permanent changes while others were designed with sunset clauses requiring renewal after a four year period. One of the areas requiring renewal was surveillance and data collection measures. The act's main target areas are:

---

[174]Cohen, *Privacy, Crime and Terror*…, 201.

- Enhancing domestic security against terrorism
- Enhancing surveillance procedures
- International money laundering abatement and anti-terrorism financing
- Protecting the border
- Removing obstacles to investigating terrorism
- Providing for victims of terrorism, public safety officers, and their families
- Increased information sharing and critical infrastructure protection
- Strengthening the criminal laws against terrorism
- Improved intelligence[175]

US civil liberty groups are concerned that provisions of the act go too far in allowing government to spy on its citizens and in fact obstruct the rights of law-abiding citizens. The argument is that the Act has decreased the ability of American citizens to obtain information about their government while, at the same time, giving the government the means to pry into the personal lives its citizens.[176] However, Francis Fukuyama argues in his book *America at the Crossroads: Democracy, Power, and the Neoconservative Legacy* "[it is] hard to imagine that the nation would have continued in its lackadaisical approach to homeland security after the World Trade Center and Pentagon attack."[177] One civil liberty issue is that US law enforcement officials are permitted to seek a court order to access the personal records of any person for the

---

[175]United States Government, USA PATRIOT ACT HR 3162, 24 Oct 2001. 2-6.

[176]Gustavo Diaz Matey, "Intelligence Studies at the Dawn of the 21st Century: New Possibilities and Resources For a Recent Topic in International Relations," *UNISCI Discussion Papers* May 2005, available from http://revistas.ucm.es/cps/16962206/articulos/UNIS0505230003A.PDF; Internet; Accessed: 3 April 2009. 12.

[177]Francis Fukuyama, *America at the Crossroads*: *Democracy, Power, and the Neoconservative Legacy* (New Haven: Yale University Press, 2006), 2.

purposes of an anti-terrorism investigation without that person's knowledge. Intelligence and law enforcement officials maintain that the act does not go far enough to help prevent future acts of terrorism. Gustavo Matey supports this position, noting that the PATRIOT Act lead to the development of the Homeland Security Interagency and Inter-jurisdictional Information Sharing Act of 2004 and the National Intelligence Reform and Terrorism Prevention Act (Dec 2004). He states, "[the American Administration] has only stepped back to the correct understanding of the requirements of secrecy in a democratic society to protect the National Security, and not to increase the power of the state."[178] Where does the PATRIOT Act find the balance between being too invasive and being ineffective? The balance is found in fair information practice principles and is reflected in the International Covenants on Civil and Political Rights legislation. As Michael Freeman summarizes in *Order, Rights and Threats: Terrorism and Global Justice,* when governments are looking at enacting "fair balanced" legislation to counter terrorism while maintaining human rights and values, the tests of consistency, importance, and cost-efficiency are required.[179] Clearly, 9/11 forced governments to strike a balance between liberty and security because the costs of liberty that they enjoyed on 9/10 were "too high."[180] The recommendations of Michael Ignatieff have been implemented in US and Canadian anti-terrorism laws to strike a legal balance. In combating the terror emergency his principles guide the choice of the "lesser evils" of:

- Protect human dignity…not countenance torture,

---

[178]Matey, "Intelligence Studies at the Dawn of the 21st Century…", 13.

[179]Michael Freeman, "Order, Rights and Threats: Terrorism and Global Justice," *Human Rights in the 'War on Terror,'* (New York: Cambridge University Press, 2005), 46.

[180]*Ibid.*, 46.

- Protect due process, make detention subject to judicial review and ensure that those detained have access to lawyers,
- Insist that exceptional measures will make the people more secure,
- Exceptional measures should be a last resort,
- Exceptional measures should be subject to open adversarial review by legislative and judicial bodies,
- The state should respect its international obligations, and
- Exceptional measures should have "sunset clauses" that subject them to time limits.[181]

As part of the re-authorization hearings for the USA PATRIOT Act, the US Chief Privacy Officer Dan Collins concluded that the Act protects the rights to privacy while helping law enforcement tasks. In his statement to the Senate Committee on the Judiciary in 2004, he said "...privacy is not always the most important value." He further comments on the idea that transactions protected or conducted by using technologies should not result in a loss of privacy.[182]

Prior to the PATRIOT act, federal agencies could obtain phone and internet company customer internet records via the issuing of "National Security Letters (NSLs)" only on suspected terrorists and spies. Following the PATRIOT Act, NSLs can be used to obtain information about anyone at all.[183] The act now allows Internet Service

---

[181]Freeman, "Order, Rights and Threats: Terrorism and Global Justice…", 47.

[182]Grant Christensen, "Federal Data Collection, Secure Flight, the Intelligence Reform and Terrorism Prevention Act, and the Reauthorization of the USA PATRIOT Act," *2005-2006 Privacy Year in Review, A Journal of Law and Policy for the Information Society* 2, Issue 3, (Columbus: Moritz College of Law, Fall 2006), 503.

[183]Cohen, *Privacy, Crime and Terror…*, 525.

Providers (ISPs) to hand over all "traffic" data to law enforcement without the need for a court order or subpoena. From a surveillance perspective, agencies such as the NSA do not require the FISC order prior to tracking suspected computer network trespassers.[184] This change modified the Electronics Communications Privacy Act to include routing and addressing information and provided government agencies with the tools to trace e-mails, monitor web sites, and other on-line communications. The end result was to allow monitoring of entire cells of suspected terrorists and was an aid in targeting terrorist watch lists.[185] The FISA was also amended to allow for intercepts on any phone or computer that may be have been used by a suspected terrorist and to allow government agencies to compel common carriers, landlords, or any person to assist in performing these intercept tasks.[186]

What legal concerns should Canadians have with respect to the USA PATRIOT Act? The Treasury Board of Canada has developed a federal strategy to address concerns about the USA PATRIOT Act and Transborder Data Flows. The main issue is that US officials have the ability to access information about Canadians, if that information was physically within the US or accessible electronically, without proper Canadian authority. The Canadian federal strategy includes the following factors: shared responsibility, balanced approach, and building on existing measures such as the PIPEDA.[187]

---

[184]Cohen, *Privacy, Crime and Terror...*, 485.

[185]Christensen, "Federal Data Collection, Secure Flight, the Intelligence Reform…, 496.

[186]*Ibid.*, 497.

[187]Office of the Privacy Commissioner of Canada, *Protecting Privacy in an Intrusive World…*, available from http://www.privcom.gc.ca/parl/2006/PIPEDA_review_060718_e.asp; Internet; Accessed: 17 April 2009.

Canadian Anti-Terrorism Act (ATA)

The Anti-terrorism Act has three main purposes: suppressing the existence of terrorist groups, providing new investigative tools, and providing a tougher sentencing regime to include terrorists and terrorist groups. Like the US PATRIOT Act, the ATA includes the following measures:

- Proceeds of Crime/Money Laundering Act amendment to extend coverage of terrorist activities and reinforced the Financial Transactions Reports and Analysis Center mandate,
- Amendments to the National Defence Act to include the CSEC mandate, scope and accountability,
- Criminal code was amended to remove the "last resort" to surveillance in the investigation of terrorist offences,
- The Official Secrets Act was amended to address national security concerns such as threats of espionage by foreign powers and terrorist groups and the intimidation or coercion of communities in Canada,
- The Canada Evidence Act was amended to protect classified information during courtroom and other proceedings, and
- Clear definitions of what constituted a terrorist activity (did not define "terrorism") and laid out a process for listing suspected terrorist.[188]

In addition, the government hoped the legislation would:

- Strengthen capacity to prevent terrorist activity before it can occur
- Disrupt, disable, and dismantle terrorist groups before they can act

---

[188]Cohen, *Privacy, Crime and Terror*…, 195.

- Meet Canada's international obligations
- Ensure respect for human rights and constitutional principles while enhancing public safety and national security
- Affirm vales of tolerance, equality and diversity[189]

Did the Canadian government go far enough? The B'nai Brith Canada organization's comments to the Senate Special Committee on the Anti-Terrorism Act in September 2005 indicated that the "ATA was indeed a step forward, but in our view, far to timid a step…[and] aspects of the legislation do not go far enough."[190] B'nai Brith Canada recommended changes including: removing the addition of a non-discrimination clause to include all groups targeting civilians, expanded hate-crime provisions, removal of motivation as a required element of proof from the definition of a terrorist act and addition of an incitement of terror clause.[191] The CSEC Chief, during parliamentary review of the Anti-Terrorism Act, compared the ability of the CSEC to perform its legislated mandate to engage in the war on terror under the new ATA, with the situation that had existed prior to this legislation. The CSEC Chief made it clear that the Criminal Code's prohibition on intercepting private communications made it impossible for the CSEC to perform its basic mission of collecting foreign communications information. Additionally, because of the introduction of evolutionary technologies such as fibre-optics, CSEC was unable to access valuable intelligence sources once previously available. With the implementation of the ATA, mechanisms are now in place to allow

---

[189]Cohen, Privacy, Crime and Terror…, 199.

[190]B'nai Brith Canada, *A Review of Canada's Anti-Terrorism Act*, Sep 2005 (Ottawa: B'Nai Brith Canada), 2.

[191]*Ibid.*, 2.

CSEC to intercept private communications when directing its activities against foreign entities located abroad. The activities require the Minister of National Defence's authorization and, with the ATA, are under constant review by the non-partisan CSEC Commissioner.[192] The CSEC Chief concluded that "authorities granted CSEC under the Anti-Terrorism Act provide the right foundation for the organization's activities while protecting the privacy of Canadians."[193]

Information Sharing Legislation

The OSCE seminar on human rights and terrorism on 18 September 2003 concluded in plenary session that international or human-rights laws must address a coordinated action against terrorism in order to be more effective.[194] Canadian and US legal measures have fallen short of the mark set at that seminar and continue to be marred by legal disconnects. The 2004 Canadian Auditor General's report outlined the following problems with respect to interoperability and information sharing:

- Watch lists require timely sharing and transfer of information between the collector and trans-border customs officers
- Information on lost and stolen passports needs to be available to officials
- Increased reliance on intelligence requires a more effective and efficient means of sharing information among intelligence agencies

---

[192]CSEC Chief, "Speaking Notes…," 5.

[193]*Ibid.*, 10.

[194]OSCE, "Human Rights and Terrorism, Towards a Multilateral, coordinated approach for the struggle against terrorism," *Seminar in the Hall of Knights: Human Rights & Terrorism, The Hague, The Netherlands* (The Hague: Netherlands Helsinski Committee, 18 September 2003), 32.

- Screening of people working in secure areas of airports requires more complete information from intelligence and law enforcement agencies.[195]

More specifically, the report indicated that the government failed to achieve improvements in the ability of security information systems to communicate with each other. The way intelligence is managed and co-ordinated has led to gaps in intelligence coverage as well as duplication, and lessons learned in improvement programs such as Canada's involvement with the MATRIX project did not adequately address September 11 threats.[196] The Public Policy Forum concluded in their report *Don't let national security trump privacy* that cross-border information sharing rules should be written into law."[197]

Data Mining Legislation

Data Mining or the automated sifting of data is a new and evolving technology that stretches the boundaries of current legislation. Judge Richard Posner has argued that the "automated sifting of data cannot, by definition, invade liberty, since it means that most data is not read by an intelligence officer."[198] In the US, President Bush signed the Homeland Security law that directed the DHS to "establish and utilize…a secure communications and information technology infrastructure, including data mining and

---

[195]Cohen, *Privacy, Crime and Terror*…, 475.

[196]Office of the Auditor General of Canada, National Security in Canada – The 2001 Anti-Terrorism Initiative, 1.

[197]The Canadian Press, "Don't let national security trump privacy…", 1.

[198]Joe W. Pitts, The Washington Spectator. Under Surveillance: The End of Illegal Domestic Spying? Don't Count on it, 15 Mar 2007.p. 3. http://www.washingtonspectator.com/articles/20070315surveillance_1.cfm accessed: 8 Mar 09.

other advanced analytical tools, in order to access, receive, and analyze data and information…"[199]

Though Canadian laws have not kept in step with technology, our allies have determined that data mining is perhaps an inevitable development in surveillance. The United Kingdom has amended their Serious Crime Act of 2007 to include data mining as a statutory process and have concluded that "data matching and mining are set to be [sic a] central part of the brave new world…".[200] Canada will have to come to terms with this new technology in the very near future, since it is clearly going to be used by our allies.

The fact that national security is a fundamental concern for all Canadians is reflected in the laws enacted by our government. Our legal provisions for the collection and exploitation of personal information juggle the needs of the state and the rights of the individual. While we have not gone as far as the US or the UK in our use of surveillance technologies, the ATA will allow Canada to move toward greater use of these capabilities as the need arises.

---

[199]K.A. Taipale, Data Mining and Domestic Security: Connecting The Dots To Make Sense of Data, The Columbia Science and Technology Law Review, Vol V, 2003. p.4.

[200]Gareth Crossman, "Nothing to hide, nothing to fear?" *International Review of Law Computers & Technology* 22,1-2, March-July 2008, 118.

> "By "intelligence" we mean every sort of information about the enemy and his country – the basis, in short, of our own plans and operations."[201]
>
> - Carl Von Clauswitz.

WHAT DOES THE FUTURE HOLD?

As Privacy Commissioner Jennifer Stoddart tells us "we are in an age of surveillance" and "the issue is not whether we are in a surveillance society but how well do we control the surveillance and ensure there are stringent rules about who gets what information and for what purposes." Dr. Ann Cavoukian theorizes that we can eliminate the "zero-sum" game of sacrificing privacy in favour of security to the option of a "positive-sum" scenario that she terms: transformative technologies. She envisions privacy built directly into the architecture of technology at the development stage.[202]

K.A Taipale, Executive Director at the Center for Advanced Studies in Science and Technology Policy, agrees with Dr. Cavoukian's argument, "that security with privacy can be achieved by employing value-sensitive development, in particular, by building in rule-based processing, selective revelation, and strong credential and audit features."[203] The future will see systems such as TIA and MATRIX with their initially flawed approaches replaced with systems such as the Automated Targeting System (ATS) that has been credited with stopping suspected terrorists from entering the US.[204] The ATS has built in policies, including information disclosure requests like those in

---

[201]Carl Von Clausewitz, *On War* (Princeton, New Jersey: Prince University Press, 1984), 117.

[202]Don Butler, "Privacy and surveillance: An interview with Canada's privacy commissioner," *The Ottawa Citizen* 29 Jan 2009, available from http://www.ottawacitizen.com/story_print.html?id=1232461&sponsor=; Internet; Accessed: 9 Feb 2009.

[203]K.A. Taipale, Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data, 15 Dec 2003, 3.

[204]*Ibid.,* 5.

place for airlines, which inform a purchaser up front that the information may be shared with intelligence agencies and can be used for data mining. Disclosure of the fact that information can be collected and utilized allows citizens to choose whether they will purchase the ticket under those conditions, or reject the option of travelling by this method. Disclosure of the fact of data collection is an important check on the power of intelligence agencies and fundamentally protects individuals. The other important check is controlling who gets information on citizens and ensuring the validity of that information before handing it on to international agencies. The future will never be without civil libertarians who question government activites, however, as Russ Knocke, assistant secretary for media relation from the DHS has indicates: "[you] would be hard-pressed to find a more transparent government program than ATS." The DHS has spent a great deal of time and effort on explaining to the public through media events such as congressional testimony, hearings, and speeches that ATS includes "rules and assessment techniques."[205]

According to Professor Martin Rudner, of Carleton University, "…[Canada] must deploy all the instruments of an asymmetric warfare effort, including an effectual legislative armoury, proactive intelligence collection, vigilant law enforcement, critical infrastructure protection, and government policies designed to promote the values and interests of [Canadians]…"[206] Canada has come some way toward providing these instruments; but, as CSEC Commissioner Charles Gonthier indicated in his 2007/2008 annual report, "enhanced accountability regarding linkages between CSEC reporting and

---

[205]Marc Perelman, "Connecting the Dots," *National Journal* 39 no. 37, 29 Sep 2007, 61-62.

[206]Thomas Gador, The views of Canadian Scholars…" 6.1.

the intelligence priorities of the government of Canada" and "enhanced accountability for the use and retention of private communications and information about Canadians" is required.[207] As Professor Steve Mann of the University of Toronto says, "Balancing surveillance with sousveillance, [literally, to watch from below] might even result in a purer form of democracy, one in which respect, power and participation are well distributed and shared." Ultimately, it will be essential for Canadians to be sure that someone is watching the watchers.[208]

---

[207]CSEC, Annual Report 2007-2008…" 17.

[208]Don Butler, "Part 6 Everyone's Watching," *The Ottawa Citizen*, 5 Feb 2009, available from http://www.ottawacitizen.com/story_print.html?id=1253557&sponsor=; Internet: Accessed: 9 Feb 2009.

CONCLUSION

The post 9/11 world poses many interesting questions for jurists, law enforcement agencies and military organizations. How do governments best protect their citizens while providing for the right to privacy? How far can we go with data collection and exploitation before the state becomes too invasive? Are we morally justified in collecting personal information on private citizens?

The new threat of terrorism is a reality that Canada cannot escape. The terrorist is working to challenge our values and beliefs and utilizes the most modern tools available. Terrorists are no longer identifiably different from the average individual; they live among us, adopt our lifestyle (while plotting to destroy it) and have become expert at adapting developing technologies to their own ends. That being the case, the state is compelled to use any means available to counter those goals even if that means impinging on dearly held values and rights.

Historically, governments have struggled with the need to protect privacy while defending citizens against domestic and international threats; but the threat used to be clear and the methods and were generally held in common. The new threat to western nations comes from a faceless enemy, not backed by the government of a specific country, and whose methods are unexpected. The most troubling issue for governments to deal with is the issue of privacy. From defining what it is, to engaging to protect it, privacy is one of the major challenges for agencies charged with national security. As history shows, some government abuse is possible when faced with an overwhelming need to protect its citizenry. The best and most effective way to defend against terrorism

is to prevent it before it happens; information collection and exploitation is an enabler in winning the war on terror.

Both ethically and legally, the collection and use of personal information can be justified in the war on terror. In fact, it is clear that the Canadian government can go further, while still remaining within the law as it currently stands, by increasing surveillance capabilities at all likely terrorist targets including transportation and government facilities. Use of data mining tools will allow for the exploitation of information target sets and analysis will determine terrorist patterns and ultimately pre-empt attacks. In the US, the PATRIOT Act extends the surveillance and information exploitation on private individuals to a much greater extent than is allowed under Canadian law. While the US government seeks to push out the boundaries of the law with respect to privacy protection, the Canadian government has protected privacy and works to find a way for privacy and security to coexist and mutually support the values of our society. The US can collect information on its citizens without the need for a warrant based on probable cause; Canada requires that those who would collect personal information must direct their collection to those outside of Canada. Canadian law enforcement and security agencies must have a court order/warrant to collect information on Canadians. Unfortunately, the threat remains and requiring probable cause to collect information on Canadians means that data mining is controversial and the risk is that those charged with protecting Canadian citizens will fail to detect terror plots until after the fact. Canada cannot continue to rely on information collected by our allies, since some of the threat comes from within. As the technologies continue to evolve, Canada should work to be at the forefront of data collection and exploitation to protect both

herself and her allies. Establishing privacy laws that can coexist with security needs can help set an example for other nations in the war on terror.

BIBLIOGRAPHY

ABC-CLIO. "USA Patriot Act (2001)." *United States at War: Understanding Conflict and Society* (2009); available from http://www.usatwar.abc-clio.com; Internet; accessed: 13 March 2009.

Aid, Matthew M. "The Time of Trouble: The U.S. National Security Agency in the Twenty-First Century." *Strategic Intelligence: Windows Into a Secret World: An Anthology*. Los Angeles: Roxbury Publishing, 2004.

Andrejevic, Mark. *iSpy: Surveillance and Power in the Interactive Era*. Lawrence, Kansas: University Press of Kansas, 2007.

Anonymous. *Through Our Enemies' Eyes: Osama bin Laden, Radical Islam, and the Future of America*. Dulles, Virginia: Brassey's, 2003.

Arellano, Nestor E. "Feds to push Web eavesdropping bill." *NetworkWorld* 19, no. 6, 20 Mar 2009. 9.

Arquilla, John. "Can Information Warfare Ever Be Just?" *Ethics and Information Technology* 1, 1999. 203-212.

Atack, Iaim. *The Ethics of Peace and War*. New York: Palgrave MacMillan, 2005.

Bamford, James. *A Pretext For War: 9/11, Iraq, and the Abuse of America's Intelligence Agencies*. New York: Doubleday, 2004.

Bamford, James. *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*. New York: Anchor Books, 2002.

Bamford, James. *The Puzzle Palace: A Report on America's Most Secret Agency*. Boston: Houghton Mifflin Company, 1982.

Bamford, James. *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*. New York: Doubleday, 2008.

Beck, Ulrich. *Risk Society: Towards a New Modernity*. Munich, Germany: Sage Publications, 1992.

Berinato, Scott. "The Short Life, Public Execution and (Secret) Resurrection of Total Information Awareness." *CSO Magazine*. August 2004. Internet; http://hanson.gmu.edu/PAM/press2/ChiefSecurityOfficer-8-04.htm; accessed: 16 Mar 2009.

Black, Jane. "Snooping in All the Wrong Places." *Business Week: Privacy Matters*, 18 Dec 2002; available from http://www.businessweek.com/print/technology/content/dec2002/tc20021218_8515.htm; Internet; Accessed: 2 Apr 2009.

B'nai Brith Canada. *A Review of Canada's Anti-Terrorism Act.* Sep 2005. Ottawa: B'Nai Brith Canada, Sep 2005.

Borovoy, Alan A. *The Fundamentals of Our Fundamental Freedoms.* Toronto: The Canadian Civil Liberties Eduction Trust, 2001.

Bothwell, Robert and J.L. Granatstein. *The Gouzenko Transcripts: The Evidence Presented to the Kellock-Taschereau Royal Commission of 1946*. Ottawa: Deneau Publishers, 1969.

Boufford, John. *CIPS's Position on E-mail & Internet Surveillance*. Available from http://www.cips.ca/position?q=surveillance; Internet; Accessed: 4 Apr 09.

Brigety, Reuben E. II. *Ethics, Technology, and the American Way of War: Cruise Missiles and US Security Policy*. New York: Routledge, 2007.

Bronskill, Jim. "Don't let national security trump privacy: report," *The Canadian Press* 10 November 2008. Available from http://www.metronews.ca/ArticlePrint/138965?language=en; Internet; Accessed: 19 Nov 2008.

Butler, Don. "Exposing our lives to pervasive, prying electronic eyes," The *Ottawa Citizen* 7 Feb 2009; available from http://www.edmontonjournal.com/story_print.html?id=1264103&sponsor=; Internet; Accessed 9 Feb 2009.

Butler, Don. "Part 1: A very different world." *Ottawa Citizen* 5 Feb 2009; http://www.ottawacitizen.com/story_print.html?id=1232203&sponsor=; Internet; Accessed 9 Feb 2009.

Butler, Don. "Part 5: You've been targeted." *Ottawa Citizen* 5 Feb 2009; http://www.ottawacitizen.com/story_print.html?id=1249220&sponsor=; Internet; Accessed 9 Feb 2009.

Butler, Don. "Part 6 Everyone's Watching," *The Ottawa Citizen* 5 Feb 2009; available from http://www.ottawacitizen.com/story_print.html?id=1253557&sponsor=; Internet: Accessed: 9 Feb 2009.

Butler, Don. "Privacy and surveillance: An interview with Canada's privacy commissioner." *The Ottawa Citizen* 29 Jan 2009; available from

http://www.ottawacitizen.com/story_print.html?id=1232461&sponsor=; Internet; Accessed: 9 Feb 2009.

Campbell, Karl E. *Senator Sam Ervin and the Army Spy Scandal of 1970-71: Balancing National Security and Civil Liberties in a Free Society, 10;* Internet; http://www.cmhpf.org/senator%20sam%sam%20ervin.hym; accessed: 2 April 2009.

Canada. Canadian Security Intelligence Service. *Backgrounder No. 8 – Counter-Terrorism*. Available from www.csis-scrs.gc.ca/nwsrm/bckgrndrs/bckgrndr08-end.asp; Internet; Accessed: 10 April 09.

Canada. Department of Justice Canada. "The Anti-Terrorism Act." Available from http://canada.justice.gc.ca/eng/antiter/act-loi/contex.html; Internet; Accessed: 14 April 2009.

Canada. Department of National Defence. B-GG-005-004/AF-010 *CF Information Operations*. Ottawa: DND Canada, 15 April 1998.

Canada. Department of National Defence. B-GG-005-027/AF-021 *The Law of Armed Conflict at the Operational and Tactical Level – annotated-*. Ottawa: DND Canada, 2001.

Canada. Department of National Defence. B-GJ-005-200/FP-000 *CF Joint Intelligence Doctrine*. Ottawa: DND Canada, 21 May 2003.

Canada. Department of National Defence. *Canada's International Policy Statement: A Role of Pride and Influence in the World – Defence.* Ottawa: Department of National Defence, 2005.

Canada. Department of National Defence. *Strategic Assessment 2006/07*. Ottawa: Directorate of Strategic Analysis Policy Planning Division Policy Group, December 2006.

Canada. Industry Canada. *Privacy and the Canadian Information Highway*. Ottawa: Communications Development and Planning Branch – Spectrum, Information Technologies and Telecommunications Sector,1994.

Canada. Industry Canada. *The Canadian Information Highway: Building Canada's Information and Communications Infrastructure*. Ottawa: Spectrum, Information Technologies and Telecommunications Sector, April 1994.

Canada. Library and Archives Canada. *The Gouzenko Affair and the Cold War*. Internet; www.collectionscanada.gc.ca/index-e.html, accessed: 4 April 2009.

Canada. McDonald Royal Commission. "Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police." Internet; http://epe.lac-bac.gc.ca/100/200/301/commissions-ef/mcdonald1979-81-eng/mcdonald1979-81-eng.htm; accessed: 14 April 2009.

Canada. Office of the Communications Security Establishment Commissioner. *Annual Report: 2007-2008.* Ottawa: Minister of Public Works and Government Services, May 2008.

Canada. Office of the Judge Advocate General. *Collection of Documents on the Law of Armed Conflict,* 2005 ed. Edited by Directorate of Law Training. Ottawa: DND, 2005.

Canada. Office of the Judge Advocate General. *Collection of Documents on the Law of Armed Conflict,* 2005 ed. Edited by Directorate of Law Training. Ottawa: DND, 2005.

Canada. Office of the Privacy Commissioner of Canada. *Protecting Privacy in an Intrusive World.* Ottawa: Parliament, July 2006; available from http://www.privcom.gc.ca/parl/2006/PIPEDA_review_060718_e.asp; Internet; Accessed: 17 April 2009.

Canada. Privy Coucil. *Securing an Open Society: Canada's National Security Policy.* Ottawa: Privy Council Office, April 2004.

Canada. Security Intelligence Review Committee. *Reflections.* Ottawa: Government of Canada, 2005; available from www.sirc-csars.gc.ca; Internet; Accessed: 14 April 2009.

Canada. The Office of the Privacy Commissioner of Canada. *Your Privacy Responsibilities: Canada's Personal Information Protection and Electronic Documents Act.* Ottawa: Privacy Commissioner, September 2006.

Canli, Turnhan et al. "Neuroethics and National Security." *The American Journal of Bioethics* 7, no. 5, 2007. 3-13.

Carafono, James Jay, Todd Gagiano, and Alone Kochems. *Domestic Surveillance: Dual Priorities & Civil Liberties, Must be Met.* Washinton: The Heritage Foundation; available from www.heritage.org/Research/HomelandSecurity/wm1950.cfm; Internet; Accessed: 18 April 2009.

Cate, Fred H. "Government Data Mining: The Need for a Legal Framework." *Harvard Civil Rights – Civil Liberties Law Review* 43, 2008. 435-489.

Cavoukian, Ann Dr. "Privacy, security go hand in hand." *Metro News* (18 November 2008). Journal on-line; available from

http://www.metronews.ca/ArticlePrint/142425?language=en; Internet; Accessed 19 November 2008.

Cavoukian, Ann Ph.D. and Don Tapscott. *Who Knows: Safeguarding Your Privacy in a Networked World*. Toronto: Random House of Canada, 1995.

CBS News. "Yemen Frees USS Cole Bomb Plotter." *The Associated Press.* Available from http://www.cbsnews.com/stories/2007/10/26/terror/main3414029.shtml; Internet; Accessed 3 April 2009.

Chief CSE. "Special Senate Committee Chief CSE Appearance – 11 April 2005 Speaking Notes." *Parliamentary Review of the Anti-Terrorism Act.* Available from www.cse-cst.gc.ca/home-accueil/nat-sec/review-ata-examen-lat-eng.html; Internet; Accessed: 3 April 2009.

Christensen, Grant. "Federal Data Collection, Secure Flight, the Intelligence Reform and Terrorism Prevention Act, and the Reauthorization of the USA PATRIOT Act." *2005-2006 Privacy Year in Review, A Journal of Law and Policy for the Information Society* 2, Issue 3. Spring/Summer 2005. Columbus: Moritz College of Law, Fall 2006.

Church Committee Reports. *Book 1: Foreign and Military Intelligence.* Washington: Assassination Archives and Research Center, 1976. Available from http://aarclibrary.org/publib/contents/church/contents_church_reports_book1.htm; Internet; Accessed: 3 April 2009.

Church Committee Reports. *Book 2: Intelligence Activities and the Rights of Americans.* Washington: Assassination Archives and Research Center, 1976. Available from http://aarclibrary.org/publib/contents/church/contents_church_reports_book2.htm; Internet; Accessed: 3 April 2009.

Church Committee Reports. *Book 3: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans.* Washington: Assassination Archives and Research Center, 1976. Available from http://aarclibrary.org/publib/contents/church/contents_church_reports_book3.htm; Internet; Accessed: 2 April 2009.

Church Committee Reports. *Book 6: Supplementary Reports on Intelligence.* Washington: Assassination Archives and Research Center, 1976. Available from http://aarclibrary.org/publib/contents/church/contents_church_reports_book6.htm; Internet; Accessed: 2 April 2009.

Church Committee Reports. *Volume 5 Intelligence Activities – The National Security Agency and Fourth Amendment Rights*. Washington: Assassination Archives and Research Center, 1976. Available from

http://aarclibrary.org/publib/contents/church/contents_church_reports_vol5.htm; Internet; Accessed: 2 April 2009.

Clausewitz, Carl Von. *On War*. Princeton, New Jersey: Prince University Press, 1984.

Cloutier, Pierre. "1948-1958 – The hunt for communists is open." *Rene Levesque: 38 Years of Federal Police Surveillance*, 15 Feb 2008. available from http://www.vigile.net/IMG/doc_Rene_Levesque_-_episode_no_1.doc; Internet; Accessed: 4 April 2009.

Cloutier, Pierre. "The magnitude of the federal police surveillance on the movement sovereignist Quebec (10960-1985)." Available from http://www.vigile.net/L-ampleur-de-la-surveillance; Internet; Accessed: 4 April 2009.

Cohen, Stanley A. *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril*. Markham, Ontario: LexisNexis Canada, 2005.

College, Green and Ann Cavoukian, *National Security in a Post-9/11 World: The Rise of Surveillance…the Demise of Privacy?* Toronto: Information and Privacy Commissioner/Ontario, May 2003.

Crossman, Gareth. "Nothing to hide, nothing to fear?" *International Review of Law Computers & Technology* 22, nos. 1-2, March-July 2008. 115-118.

Dempsey, James X. and Paul Rosensweig. *Technologies That Can Protect Privacy as Information Is Shared To Combat Terrorism* (Washington: Center For Democracy and Technology, 26 May 2004).

Electronic Privacy Information Centre (EPIC). "Legality of NSA's Secret Eavesdropping Program Is Suspect and Cost is Unknown." *Spotlight on Surveillance* Jan 2006; Internet; http://epic.org/privacy/surveillance/spotlight/0106/default.html; accessed 30 Oct 2008.

EPIC. *The Clipper Chip*. Internet; http://www.epic.org/crypto/clipper/default.html; accessed: 16 April 2009.

EPIC. ~~*Total*~~ *"Terrorism" Information Awareness (TIA).* Available from http://epic.org/privacy/profiling/tia/default.html; Internet; updated 21 March 2005; accessed: 3 April 2009.

Freeman, Michael. "Order, Rights and Threats: Terrorism and Global Justice." *Human Rights in the 'War on Terror,'*. New York: Cambridge University Press, 2005).

Fidler, Richard. "Afghan resistance is 'terrorist' under Canadian law, Khawaja trial judge rules." *Global Research.* 10 November 2008; Internet; www.globalresearch.ca/PrintArticle.php?articleId=10874; accessed: 3 Apr 2009.

Frost, Mike. *Spyworld: Inside the Canadian and American Intelligence Establishments*. Toronto: Doubleday Canada Limited, 1994.

Frum, David and Richard Perle. *An End to Evil: How to win the war on terror.* New York: Ballantine Books, 2004.

Fukuyama, Francis. *America at the Crossroads: Democracy, Power, and the Neoconservative Legacy*. New Haven: Yale University Press, 2006.

Galison, Peter and Martha Minow. "Our Privacy, Ourselves in the Age of Technological Intrusions." *Human Rights in the 'War on Terror.'* New York: Cambridge University Press, 2005.

Gaston, James C. and Janis Bren Hietala. *Ethics and National Defense: The Timeless Issues*. Washington: National University Press, 1993.

Gleditsch, Nils Petter. Review of "Signals Intelligence in the Post-Cold War Era. Developments in the Asia-Pacific Region by Desmond Ball." *Journal of Peace Research* 31, no. 2 (May, 1994).

Granatstein, J.L. *Whose War is it? How Canada Can Survive in the Post-9/11 World*. Toronto: HarperCollins Publishers, 2007.

Goldman, Jan. *Ethics of Spying: A Reader For The Intelligence Professional*. Lanham, Maryland: Scarecrow Press, 2006.

Gup, Ted. *Nation of Secrets: The Threat to Democracy and the American Way of Life*. New York: Doubleday, 2007.

Guthrie, Charles, and Michael Quinlan. *Just War: The Just War Tradition: Ethics in Modern Warfare*. London: Bloomsbury Publishing, 2007.

Haggerty, Kevin D. and Amber Gazso. "Seeing beyond the Ruins: Surveillance as a Response to Terrorist Threats." *Canadian Journal of Sociology* 30, no. 2 (Spring, 2005). 169-187.

Hambling, David. *Weapons Grade: How Modern Warfare Gave Birth to Our High-Tech World*. New York: Carroll & Graf Publishers, 2005.

Hamilton, Dwight. *Inside Canadian Intelligence: Exposing the New Realities of Espionage and International Terrorism*. Toronto: Dundurn Press, 2006.

Hannah, Commander G.A. "Seizing and Holding the Moral High Ground An Introduction to Ethical Theories." Toronto: Canadian Forces College, 2006.

Henderson, Harry. *Privacy in the Information Age.* New York: Facts on File, 1999.

Herman, Michael. "Ethics and Intelligence after September 2001." *Intelligence and National Security* 19, No. 2. London: Frank Cass & Company, Summer 2004.

Heymann, Philip B. *Terrorism, Freedom, and Security: Winning Without War*. Cambridge, MA: MIT Press, 2003.

Hulnick, Arthur S. and Daniel W. Mattausch. "Ethics and Morality in U.S. Secret Intelligence." *Ethics of Spying: A Reader for the Intelligence Professional.* Toronto: The Scarecrow Press, 2006.

Ignatieff, Michael, Dr. "Ethics and the New War." *Canadian Military Journal* 2, no. 4 (Winter 2001-2002): 5-10.

Jennings, Francis. *Benjamin Franklin: Politician.* New York: W.W Norton & Company, 1996.

Jonas, Jeff and Jim Harper, *Policy Analysis: Effective Counterterrorism and Limited Role of Predictive Data Mining* No. 584. Washington: CATO Institute, 11 Dec 2006.

Kawakami, Sayaka and Sarah C. McCarty. "Privacy Year in Review: Privacy Impact Assessments, Airline Passenger Pre-Screening, and Government Data Mining." *A Journal of Law and Policy For The Information Society* Vol. 1, Issue 2-3 Spring/Summer 2005. Columbus: Moritz College of Law, 2005.

Kutz, Gregory D. *Data Mining: Results and Challenges for Government Program Audits and Investigations* GAO-03-591T. Washington: GAO, 25 March 2003; available from http://usacm.acu.org/usacm/testimony/GAODatamining.pdf; Internet; Accessed: 18 April 2009.

Lee, Timothy B. "Electronic Surveillance." *CATO Handbook For Policymakers* 28. Washington: CATO Institute, 2009.

Levy, Robert A. *Ethnic Profiling: A Rational and Moral Framework.* Internet; http://www.cato.org/pub_display.php?pub_id=5399; accessed: 31 Mar 2009.

Lister, Michael and Katherine Baird. "Outcome Report." *The Federal Privacy Regime Roundtable Series*. Ottawa: Public Policy Forum, March 2008.

MacDonald, Spencer R. "Rational Profiling in America's Airports." *B.Y.U. Journal of Public Law* XVII, 2003, 113-139.

MacKinnon, Barabara. *Ethics: Theory and Contemporary Issues*. Belmont, CA: Wadsworth Publishing Company, 1998.

Marx, Gary T. "An Ethics For The New Surveillance," *The Information Society* 14, no. 3, 1998. available from http://web.mit.edu/gtmarx/www/ncolin5.html; Internet; Accessed: 22 April 2009.

Marx, Gary T. "Privacy and Technology." *The World and I*. September 1990; Internet; http://web.mit.edu/gtmarx/www/privantt.html; accessed 3 April 2009.

Matey, Gustavo Diaz. "Intelligence Studies at the Dawn of the 21st Century: New Possibilities and Resources For a Recent Topic in International Relations." *UNISCI Discussion Papers* May 2005. Available from http://revistas.ucm.es/cps/16962206/articulos/UNIS0505230003A.PDF; Internet; Accessed: 3 April 2009.

McLaughlin, Abraham. "It will gather intelligence at home to curb terrorism. Critics see era of Big Trench coat." *The Christian Science Monitor*. 17 December 2001. Available from http://www.csmonitor.com/2001/1217/p2s1-usgn.html; Internet: Accessed: 2 April 2009.

Melanson, Rhilip H. *Secrecy Wars: National Security, Privacy, and the Public's Right to Know*. Washington: Brassey's Inc., 2001.

Mill, John Stuart. *On* Liberty. New York: Dover Publications, 2002.

NASCIO. "Think Before You Dig: Privacy Implications of Data Mining & Aggregation." (Lexington, KY: NASCIO, Sept 2004).

Nef, Jorge and J. Vanderkop. *Technology – Moral and Ethical Aspects*. Guelph: University of Guelph, 1989.

Olson, James M. *Fair Play: The Moral Dilemmas of Spying*. Washington: Potomac Books, 2006.

O'Neill, Bard E. *Insurgency & Terrorism: From Revolution to Apocalypse*. Washington: Potomac Books, 2005.

Organization For Economic Co-Operation and Development. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." Sep 1980. Available from http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html; Internet; Accessed: 3 April 2009.

Orr, Robert. "Review of Legislating Privacy by Priscilla Regan." *Policy 8803*. Georgia: Georgia Tech, Fall 2000.

Orwell, George. *Nineteen Eighty-Four*. New York: Penguin Books, 1976.

OSCE, the Netherlands. *Seminar in the Hall of Knights: Human Rights & Terrorism, The Hague, The Netherlands*. The Hague: Netherlands Helsinski Committee, 18 September 2003.

PBS Frontline, "Trail of a Terrorist: The Millennium Plot: Ahmed Ressam's Millennium Plot."; available from http://www.pbs.org/wgbh/pages/frontline/shows/trail/inside/cron.html; Internet; accessed: 16 March 2009.

Perelman, Marc. "Connecting the Dots." *National Journal* 39 no. 37. New York: National Journal, 29 Sep 2007.

Pfaff, Tony. "Bungee Jumping off the Moral High Ground: Ethics of Espionage in the Modern Age." *Ethics of Spying: A Reader for the Intelligence Professional.* Toronto: The Scarecrow Press, 2006.

Pitts, Joe W. "Under Surveillance: The End of Illegal Domestic Spying? Don't Count on It." *The Washington Spectator* 15 Mar 2007. Washington: Public Concern Foundation Inc. available from http://www.washingtonspectator.com/articles/20070315surveillance_1.cfm; Internet; Accessed: 8 Mar 09.

Popp, Robert and John Poindexter. "Countering Terrorism through Information and Privacy Protection Technologies." *IEEE Security & Privacy: Data Surveillance 2006*, IEEE Computer Society; Internet; http://www.computer.org/security; accessed: 4 April 2009.

Quinn, Michael J. *Ethics for the Information Age 3rd Ed.* Boston: Pearson Education, 2009.

Reed, Charles and David Ryall. *The Price of Peace: Just War in the Twenty-First Century*. Cambridge: Cambridge University Press, 2007.

Relyea, Harold C. and Jeffrey W. Seifert. "Information Sharing for Homeland Security: A Brief Overview." *CRS Report for Congress RL32597.* Washington: Congressional Research Service, 10 Jan 2005.

Richelson, Jeffrey T. *The US Intelligence Community 5th Ed.* Boulder, Colorado: Westview Press, 2008.

Roberts, Alasdair. *Blacked Out: Government Secrecy in the Information Age*. New York: Cambridge University Press, 2006.

Rohwer, Jurgen. "Signal Intelligence and World War II: The Unfolding Story." *The Journal of Military History* 63, no. 4 (Oct., 1999).

Sanborn, Stephanie, Owen Linderholm, and Cathleen Moore. "Privacy concerns raised." *INFOWORLD* 23, Issue 38, 19 Sep 2001 available from www.infoworld.com; Internet; Accessed: 13 Mar 2009.

Sawatsky, John. *For Services Rendered: Leslie James Bennett and the RCMP Security Service.* Toronto: Doubleday Canada Limited, 1982.

Sawatsky, John. *Men in the Shadows: The RCMP Security Service*. Toronto: Doubleday Canada Limited, 1980.

Seifert, Jeffery. "Data Mining and Homeland Security: An Overview." *RL31798 CRS Report for Congress.* Washington: Congressional Research Service, 5 Jun 2007.

Stein, Janice Gross and Eugene Lang. *The Unexpected War: Canada in Kandahar*. Toronto: Penguin Canada, 2007.

Sloan, Lawrence D. "ECHELON and the Legal Restraints on Signal Intelligence: A Need for Reevaluation." *Duke Law Journal* 50, no. 5 Special Symposium Issue: Congress and the Constitution (Mar., 2001).

Sykes, Charles J. *The End of Privacy*. New York: St. Martin's Press, 1999.

Taipale, K. A. "Data Mining and Domestic Security: Connecting The Dots To Make Sense of Data." *The Columbia Science and Technology Law Review* 5, 2003.1-82.

Teufel, Hugo. "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security." *DHS Privacy Policy Guidance Memorandum 2008-01*. Washington: The Privacy Office U.S. Department of Homeland Security, 29 Dec 2008.

The Markle Foundation. *Creating a Trusted Information Network for Homeland Security.* New York City: The Markle Foundation, Dec. 2003.

The Markle Foundation. *Mobilizing Information to Prevent Terrorism.* New York City: The Markle Foundation, 2006

The Markle Foundation. *Protecting America's Freedom in the Information Age.* New York City: The Markle Foundation, Oct. 2002.

.

Treverton, Gregory F. "Intelligence: Welcome to the American Government." *Strategic Intelligence: Windows Into a Secret World: An Anthology.* Los Angeles: Roxbury Publishing, 2004.

United Kingdom. HM Government. *Countering International Terrorism: The United Kingdom's Strategy July 2006.* Norwich, England: TSO (The Stationary Office), 2006.

United Nations. "UN Action to Counter Terrorism." Available from http://www.un.org/terrorism/strategy-counter-terrorism.shtml; Internet; Accessed 10 April 2009.

United States. Communications Act of 1934, Public Law No. 416, June 19, 1934, 73rd Congress. Available from http://criminalgovernment.com/docs/61StatL101/ComAct34.html; Internet; Accessed: 11 April 2009.

United States. Government Accountability Office. *About GAO*. Available from www.gao.gov/about/index.html; Internet; Accessed: 18 April 2009.

United States. The Privacy Office. *Privacy Policy Guidance Memorandum: The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*. Washington: U.S. Department of Homeland Security, 29 Dec 2008.

United States. US Congress. USA PATRIOT ACT HR 3162, 24 Oct 2001.

Wark, Wesley K. "Cryptographic Innocence: The Origins of Signals Intelligence in Canada in the Second World War." *Journal of Contemporary History* 22, No. 4 Intelligence Services during the Second World War: Part 2 (Oct. 1987).

Webb, Maureen Webb. *Illusions of security: Global Surveillance and Democracy in the Post-9/11 World.* San Francisco: City Lights Books, 2007.

Whitaker, Reg. *The End of Privacy: How Total Surveillance Is Becoming A Reality*. New York: The New Press, 1999.

Wohlstetter, Roberta. *Pearl Harbor: Warning and Decision.* Stanford: Stanford University Press, 1962.

Woodward, John D. *Privacy vs. Security: Electronic Surveillance in the Nation's Capital*. Santa Monica, CA: RAND, March 2002.

Yourdon, Edward. *Byte Wars: The Impact of September 11 on Information Technology*. Upper Saddle River, NJ: Prentice Hall PTR, 2002.