MA MAJOR RESEARCH PAPER

The Security-Rights Dilemma and Communications Surveillance in Canada

Karen Moses

The Major Research Paper is submitted
in partial fulfilment of the requirements for the degree of
Master of Arts

Joint Graduate Programme in Communication & Culture
Ryerson University — York University
Toronto, Ontario, Canada

November 2009

As the understanding of political and human rights is becoming more expansive, it is clear that the movement towards an expansion of these rights is being forcibly countered by states' actions and policies developed to combat terrorism, indicating that security and rights are in competition with one another, at least according to the state. Security also now has, arguably, a more important place in the political fabric of each state since the terrorist attacks of 11 September 2001; however, it is more likely that the increased importance of security has stemmed from a constant state of insecurity or the constant fear of threats, whether these be real or imagined. Security is beginning to take on a new meaning, though at this point it is too soon to determine the long-term implications of these developments. For the time being, it is clear that the state of insecurity is impacting civil rights in Canada and is likely to affect communication rights, and privacy more specifically. These possible infringements on communication and civil rights are not well known to Canadian citizens, and both media and academia have neglected to report or study this to a sufficient degree[1]. This paper presents the main issues surrounding domestic interceptions of communications in Canada by Canadian government agencies. Not only is this a critical juncture in Canadian communications law and policy, but the lack of interest and knowledge about the topic presents a democratic deficit in Canadian politics. If this ambivalence to the possibility of illegal surveillance of domestic communications in Canada continues, Canadian democratic values and traditions, including privacy controls and civil liberties, may degrade further along the lines of American activities vis-à-vis domestic interceptions and surveillance of communications.

This paper explores the issues of balancing freedom and privacy rights with security. It also

1 The possibility of infringement of rights of Canadian citizens is related to the use of intelligence in state security. Though this is the case, the institutions, departments and agencies involved in intelligence work are not explored in depth, and a striking deficiency is that most of the literature available is concentrated on one institution in particular, the Canadian Security and Intelligence Services. Very few academic studies focus on the Communications Security Establishment Canada (CSE) in detail, with a few exceptions, most notably the research of Martin Rudner. In terms of media coverage of the CSE, a similar pattern is observed and thus the lack of public information on the CSE even led the government to produce a report in 1993 entitled *The Communications Security Establishment – Canada's Most Secretive Intelligence Agency* (Rosen, 1993).

acts as a primer for debate about related government responsibilities and explains why the security-rights dilemma—or how the threat of terrorism—may suspend the rights of Canadian citizens. Specific attention is paid to communication-related rights such as privacy and how the threat of terrorism allows due process and other checks and balances systems to be bypassed through various intelligence practices. This paper will identify why risk appears to trump rights in the current security environment and explain why security cannot be privileged over rights as rights are an integral part of public security. The state appears to view security as purely, or at least primarily, physical, however, if the state concentrates counterterrorist efforts on physical security, then this ignores the social aspects of security and therefore does not provide an adequate level of protection for its citizens but only advances the interests of the state. There are several ways in which the need for state security and desire to preserve democratic freedoms and values can be balanced without sacrificing one over the other, but this must begin with dialogue between the state and its citizens.

The purpose of this study is to explore the potential and real threats of domestic surveillance of communications in Canada and highlight the role played by the Communications Security Establishment (CSE), Canada's signals intelligence agency. This paper examines five substantial areas of the debate. First, the issue of domestic surveillance of communications is problematized within the paradigm of what one might call the security-rights dilemma. The main stakeholders are charted and analyzed within the debate. Mainly government officials, security personnel, and private interests are explored here. Next, a historical survey of the Canadian government and its intelligence and security community is briefly presented. This area of inquiry's primary focus will be to outline and analyze the structure and practice of Canadian intelligence which will be followed by a detailed analysis of the CSE and the formal and informal international agreements to which it is a party. Fourth, the technology of surveillance is presented and the main problems of interception and analysis as well as the social and political issues related to state surveillance of data and communications are itemized.

Finally, an overview of the current debate on domestic surveillance in Canada is presented before final conclusions are drawn and recommendations are made.

The security-rights dilemma is rather complex, and the rights affected by it will be carefully examined, as related to legislative and policy changes and the technologies that permit the erosion of rights. Specifically, some of these rights include the right to information, freedom of speech and association, privacy as well as basic political rights such as lawful dissent. The security-rights dilemma needs first and foremost to be defined and serves as the basis to understanding the debate and the implications of the dilemma, mainly, the erosion of rights. It is hoped that by identifying these areas this paper will serve as a primer and encourage serious and sustained debate on the topic by the general public, as well as identify the need for increased research and media attention.

The Security-rights Dilemma and Domestic Surveillance of Communications in Canada

The terrorist attacks within the United States were viewed as being without precedent. The reaction to these attacks was novel in many ways; however, the events themselves were hardly new. The United States had been the primary target of several terrorist attacks in the years leading up to 2001 when the attacks hit closer to home. Within the first few hours of this attack the rhetorical strategy to garner support was in full swing: everything was new, this war had no boundaries, and it was a war that *must* be won. On 20 September 2001, the address given by then President George W. Bush captures this rhetoric well: "All of this was brought upon us in a single day—and night fell on a different world [...] Americans should not expect one battle, but a lengthy campaign, unlike any other we have seen" (Jackson, 2005, p. 148). In effect, the events of 11 September 2001 "changed everything," and other conflicts were no longer valid as frames of reference. The United States declared war on an abstract entity or, rather, declared war on a tactic, and this has greatly confused the goals and execution of this conflict. From the very outset, the United States presented itself as a

bastion of all things good: justice, freedom, and as a state that promoted and protected human rights. Though former President Bush presented this as a "War on Terror," he was careful to say that it was not a *world* war, but instead chose to say that "what is at stake is not just America's freedom. This is the world's fight. This is civilization's fight. This is the fight of all those who believe in progress and pluralism, tolerance and freedom...Freedom and fear are at war" (U.S. Office of the Press Secretary, 2001). The War on Terror was created as a war of principles, one in which the United States, and the world, must fight to the end, and in which the first responsibility was to defend and uphold these principles. The way the war was presented, security was named as a precursor to freedom, but not an ultimate opponent of it. In practice this has not been the case, and freedom is visibly suffering. This is because the way in which the global political sphere is dealing with terrorism has changed significantly in recent years.

Before 11 September 2001, terrorism was viewed as a global problem, but did not have the same support or level of urgency. Since the attacks, security concerns now give a higher priority to terrorism and it has now been thrust to the top of the list of global priorities. 9/11 was pivotal because it was presented as an expression of crisis, an event preceding a period of emergency, and one that has continued to be used as the rationale to provide legitimacy to undemocratic counterterrorism activities carried out by governments. In assessing the response of governments, the actions and policies enacted since 9/11 suggest that most government and intelligence and security officials consider security and freedom to be in competition with one another in a "zero-sum" game. It would be wise to remember, however, that this is not a game, and while sacrificing rights in the name of freedom, terrorists still thrive[2]. Even though there are some rights that impair our security and that it might "be a safer society

2 Terrorism as news, for example, supports the terrorist cause. As Leman-Langlois and Brodeur argue, in all of its forms "terrorism thrives on media coverage" (2005, p. 131). Publicity can be brought about for many reasons and some of this can relate to government action, including the negative publicity caused by the cessation of rights and freedoms as a state response to terrorist threats. For example, media coverage by civil rights groups can increase the visibility of terrorist groups, which is an important part of terrorism, and can act as a form of propaganda.

if we allowed our police to lock up people they thought [were] likely to commit crimes in the future" this practice is simply unacceptable, and if this practice is adopted, then the state, in effect, encourages terrorism (Chrisodoulidis, 2007). It must be remembered that in forfeiting our rights or compromising our values, terrorists thrive: "What our enemies mainly hope to achieve through their terror is the destruction of the values that they hate and we cherish"; therefore, it is imperative that these rights and values be protected and defended (Chrisodoulidis, 2007).

There are many different strategies for dealing with terrorism; however, the problem with most approaches is that there is no guarantee of success. For instance, racial profiling, as one strategy often employed to deal with risk, is a controversial practice. Those who support it argue for its use on the basis of statistics. According to a study by Paul Sperry of the Hoover Institute at Harvard University in 2005, racial profiling is a legitimate and useful practice as, statistically, "[f]rom everything we know about the terrorists who may be taking aim at our transportation system, they are most likely to be young Muslim men" (Harcourt, 2007, p. 228). Those who oppose the use of racial profiling do so on the basis that it is ineffective. In reference to the London bombings, for example, New York City police commissioner Raymond Kelly made a very apt point:

> If you look at the London bombings, you have three British citizens of Pakistani descent. You have Germaine Lindsay [the fourth London suicide bomber], who is Jamaican. You have the next crew [in London], on July 21st, who are East African. You have a Chechen woman in Moscow in early 2004 who blows herself up in the subway station. So whom do you profile? (Harcourt, 2007, p. 228).

In Canada this is an especially pressing question given the diversity of the Canadian population. According to the 2006 Census, 19.8% of the population in Canada was born outside the country (Statistics Canada, 2007). There is a risk that those belonging to ethnic groups might be unreasonably implicated in terrorist activities or be suspected as associating with terrorists, thus compromising Canadian values and traditions[3]. Canada is not innocent of this kind of targeting behaviour, and there

3 Most importantly, this involves the legal principle of "innocent until proven guilty."

are no guarantees that the same might not happen in the future, or that it is not happening now.

Racial profiling is but one strategy in a complex system of various counterterrorism activities. Some scholars propose that these activities have created a state of ubiquitous surveillance, aimed to provide reasonable and accurate assessment of risk. As Webb notes,

> in the wired world of the twenty-first century, most people in the developed world and many in the developing world as well have their "wires" permanently plugged into the many surveilled networks that they must engage with in their daily lives. Thus, the information we leave behind creates an ever-accumulating, virtual picture of us, which state agents can call up to scrutinize again and again (2007, p. 137).

Through financial transactions, associative behaviour (including communications), and other types of surveillance, state agents are able to create virtual profiles of our real selves, which may or may not provide an accurate representation. Constructing virtual profiles allow for methodical categorization into two primary groups: those who are viewed as "at risk" individuals, or individuals most likely to be involved in terrorist activities, and those who are not.

Risk assessment is an essential state responsibility for several reasons. First, a state has limited resources. Second, risk assessment allows the state to identify threats, which may assist in countering or neutralizing these threats. Finally, and related to the aforementioned, governments will tend to follow the mantra of "an ounce of prevention is worth a pound of cure." Simply put, governments have limited resources, and risk assessment assists in identifying the priority for the distribution of resources: foresight and anticipatory action (pre-emption) are key (Finan & Macnamara, 2001). However, with respect to terrorism, pre-emptive action is not necessarily *preventative*. To be clear, this means that the pre-emptive counterterrorism measures cannot guarantee results. It is difficult, if not technically impossible, to prove that these measures are effective. Consider the following:

> -racial profiling could very easily subject innocent people to undue search, seizure and other intrusive and invasive acts (as has been documented by Bahdi, 2003; Choudhry & Roach, 2002; Gross & Livingston, 2002) thereby diverting precious resources while allowing non-Arab and non-Muslim extremists continue to terrorize the Western world,

-financial tracking can be elusive, particularly with the many creative means of financing and money laundering terrorists use (Homer-Dixon, 2002; Riem, 2007),

-association cannot confirm the intent or motives of individuals even when these persons do interact with known terrorists,

-and the interception and analysis of communications is a difficult endeavour due to technical limitations and because interception can provide intelligence agents with distant and sometimes discordant pieces of information that form but a small piece of the puzzle (Rosen, 1993).

This paper focuses on all of these intelligence gathering strategies more generally, and government surveillance of communications most specifically, within the security-rights dilemma. The digitization of information and the acceleration of intelligence sharing and networking between states and other actors raise concerns; however, little attention has been devoted to the surveillance of communications domestically even though the interception and analysis of personal communications *within* state boundaries is increasing. Datamining is one technique used to analyze domestic communications. Datamining involves the "use of computer models, or algorithms, to scrutinize masses of data for selected patterns or criteria" (Webb, 2007, p. 147), which allows government agencies to target certain information such as the word "explosive" or any other words, names or phrases of interest. Proponents for the expansion of datamining projects such as the United States' Total Information Awareness program argue on the basis of these successes even though counterterrorism officials working on datamining projects admit that the intelligence gathered only "led them to a few potential terrorists inside the country they did not know about from other sources and diverted agents from the counterterrorism work they viewed as more productive" (Webb, 2007, p. 49). Furthermore, datamining is proven to "generate high numbers of false positives" (Brown & Korff, 2009, p. 126). Therefore, given these reasons,

> the rationale for pre-emption, whether applied to foreign policy, security intelligence, law enforcement, or the exercise of executive power, is extremely dangerous because it justifies *almost anything* In the fields of law enforcement and security intelligence, it produced the draconian *USA PATRIOT Act*, and many other acts cast from the same mold in other countries (Webb, 2007, p. 69).

Webb raises the question: is the practice of datamining and surveillance actually appropriate, or is datamining a useful and "important policy tool" for "allocat[ing] security budgets [and] identifying vulnerable places and suspicious people" (Amoore & De Goede, 2005, p. 149) as some would argue? According to the latter authors, risk management is "emerging as the most important way in which terrorist danger is made measurable and manageable" (2005, p. 149). As has been documented with many other pre-emptive counterterrorism strategies, surveillance activities that are focused on risk management may infringe on the rights of citizens in very profound ways (Lyon, 2002).

Law enforcement agents and intelligence professionals are trying to maximize efficiency by tracking social networks through mapping associative behaviour and interactions though there are many limits to this kind of counterterrorism approach. As Steve Ressler explains, there are benefits in monitoring the relationships and transactions of individuals using the process of social network analysis (SNA) as it "can provide important information on the unique characteristics of terrorist organizations, ranging from issues of network recruitment, network evolution, and the diffusion of radical ideas" (Ressler, 2006, p. 1). However, it can also be argued that the use of SNA categorizes individuals far too much based on relationships, transactions or actions and may expose innocent individuals to excessive scrutiny and personal harm in the name of security. To be more clear, the utility of SNA is based on American social psychologist Stanley Milgram's experiments of some forty years ago in 1967. The intent of the experiment was to test "how people are connected to others by asking them to forward a package to any of their acquaintances who they thought might be able to reach the target individual" (Ressler, 2006, p. 1). Milgram discovered that people are often connected by six acquaintances or separated from one another by six degrees. What this connection has to do with counterterrorism is that an innocent person may be caught within these six degrees and deemed to be an "at risk individual." After all, disintermediation is a prominent feature of modern organizations

and networks: individuals no longer need to be connected through an intermediate but are able to "directly connect to each other, especially with the advancements of modern telecommunications and the Internet" (Ressler, 2006, p. 2). Modern information and communication technology (ICT) and the astonishingly rapid pace of digitization makes surveillance easier for government to perform on unsuspecting citizens. The revolutionary and potentially dangerous aspects of communications technologies are appreciated by government officials as government both employs this technology for surveillance purposes, but also must concern itself with cyber-attacks. Surveillance and the need to protect data and communications are now taken more seriously by government since 11 September 2001.

States are involved in many different types of surveillance, according to Professor of Law and Psychiatry Christopher Slobogin. He divides surveillance into three separate categories:

> [p]hysical surveillance is real-time observation of physical activities, using either naked eye or enhancement devices such as binoculars or video cameras. Communications surveillance is real-time interception of the content of communications relying on wiretapping, bugging, hacking, and various other methods of intercepting oral statements and wire and electronic transmissions. Transaction surveillance, in contrast, involves accessing *already-existing* records, either physically or through computer databanks. It also encompasses accessing, in real-time or otherwise, the *identifying signals* of a transaction (such as the email address of an email recipient) (Slobogin, 2005, p. 140).

Though these distinctions are helpful in understanding the nature of each strategy, these strategies often overlap. Domestic surveillance of telecommunications is a contentious issue, and reports indicate that the United States' government is able to access a plethora of information on its own citizens[4]. Analysis of domestic call traffic reveals "information about times, dates and numbers called," which can then be used to map associational networks (Strandburg, 2008, p. 741). This activity is not considered communications surveillance but is transactional in nature since it does not relate to content but is

4 Domestic wiretapping has happened before in the United States and this led to the *Foreign Intelligence Surveillance Act* (FISA) in 1978, which explicitly made this activity illegal, unless law enforcement and security and intelligence officials obtain a court warrant. Human rights lawyer Maureen Webb regards FISA as a direct response to the Watergate scandal and the U.S. Senate's Church Committee Report (2007, p. 51).

focused on the registry, call history and location of signals (Slobogin, 2005). This is not to say that governments are not interested in the content of these calls. In fact, multiple reports prove otherwise: governments are very interested in the content of domestic communications (Lewis, 2007; Risen & Lichtblau, 2005). It is possible that the Canadian signals intelligence agency, the Communications Security Establishment, may intercept domestic communications even though the agency is meant only to collect "foreign communications signals which originate and terminate abroad" (CSEC: Frequently ask questions [FAQs], 2008). As will be explored below, more recent policy moves and legislative changes in the Canadian government are blurring the lines concerning the surveillance of domestic communication. Domestic surveillance by the CSE, which was previously an illegal activity, is no longer concretely so.

Canadians, like Americans, are being asked to cooperate with the government to combat terrorism because it poses a "threat to our way of life," or, more specifically, a threat to the rights and freedoms typically cherished by liberal western democracies, Canada included (U.S. Office of the Press Secretary, 2001). States have enacted new legislation that is primarily centred around preserving this way of life; however, it is ironic that much of the legislation intended to provide greater physical security jeopardizes the security of citizens' rights and freedoms when the public interest lies in having both security *and* rights. Though many scholars have taken up the issue of asking whether Canadian laws are cast from the same mold as the American *PATRIOT Act*, few have considered the degree to which Canadians are willing to sacrifice or suspend their rights and freedoms for the impossible return of more physical security[5]. The whole issue of security is that it is based on risk, and risk is a measure

5 Assessing Canadians' willingness to forfeit rights is more complex than one might consider, according to Haggerty & Gazso (2005). Their study on *The Public Politics of Opinion Research on Surveillance and Privacy* explains that opinion polls regarding privacy are often skewed as there are many potential respondents who will not be reached by these surveys. Whether these persons are not able to be reached due to an unlisted telephone number, screening practices, or outright refusal, these are often the people who would argue for greater privacy controls. They also reveal that media outlets do not take into consideration their own positions of influence and uncritically publish studies with suspect findings due to methodological issues including non-disclosure of response rates (Haggerty & Gazso, 2005).

of threats, whether real or imagined. Rights, on the other hand, are concrete and ingrained within our political and legal systems.

Rights are given expression through statements such as the 1948 United Nations Declaration on Human Rights but are also given legal representation and affirmation of their worth in documents such as the Canadian *Charter of Rights and Freedoms*, as was signed into law in 1982. The issue at hand is that the rights of citizens have been pitted against the security of the state; however, the competition is an unfair—the response to threats becomes a top priority when threats and rights come into contact: freedom and fear are at war indeed.

International terrorism is quite obviously a transnational problem; however, it requires domestic responses. Each country needs its own plan to deal with this issue. Even so, intelligence sharing has become more important between law enforcement agencies and governments. Intelligence sharing between and among countries is not only subject to legal strictures to protect each individual country's security and national secrets, but it is also governed by international agreements of which the details remain clouded in secrecy (Aid & Weibes, 2005, p. 109).

In a democratic society, secrecy is necessary for intelligence work but soon becomes problematic. Intelligence activities are often a state secret: very little is known about them, and yet the public is asked to trust the government wholeheartedly, as though the state will always look out for the public's best interest, and any questions or criticism may be ultimately silenced with charges of being unpatriotic or be followed by accusations that an individual supports terrorism. How can the public allow the government to use undisclosed resources for programs it knows little about and with no proof that these programs actually make the country safer? The answer may be fear and intimidation[6].

6 Where charges of being unpatriotic do not work to dissuade persons or organizations of interest to discontinue their offending activities (whether this be in the form of protest, fundraising, or otherwise), more forceful action is presented as the alternative. For example, though parts of the Front de Libération du Québec (FLQ) engaged in criminal activities, on 16 October 1970 the Canadian Forces were activated and those affiliated with the movement were put in preventative custody, even though none of these arrests resulted in charges (Leman-Langois & Brodeur, 2005, p. 130). The Royal Canadian Mounted Police were also responsible historically for the "repression of terrorism and of what was perceived to be political

According to Webb "governments have been fairly successful at either selling or eluding public accountability for surveillance initiatives" (2007, p. 75). In the Standing Senate Committee on National Security Canadian Security Guidebook of 2004 report, the Canadian government openly admits there are several strategies it employs to marginalize issues. The government may marginalize any issue by one or more of the following: confusing the details; delaying debate; challenging the authority or motivation of those who raise the issue; addressing the problem superficially by promising "half measures...usually at some point in the hazy future"; or bringing other issues to the fore, arguing that they deserve higher priority (Canada, 2004, p. 7). In addition, the government may also hope that the public will soon lose interest in the issue. In the latter case, the government may take advantage of public apathy or inability to fully understand the issue, and the government may also manipulate media accounts (Kenny & Forrestall, 2004, p. 7). In democratic societies where accountability and transparency are key elements in the political system and are essential for a healthy relationship between the government and its public, this is an issue that cannot be ignored.

Domestic interception of communications, ranging from the tracking of financial and associative activities to eavesdropping or the interception of email and related communications on the Internet, is a serious issue within the security-rights dilemma and yet it has too often been neglected by scholars and media alike—or those who are allegedly charged with promoting accountability and transparency. With the rise of mass society, academics and media are continually called upon to protect the public by informing the electorate. Inspired by John Dewey's philosophy of democracy, communication and education Professor Clive Barnett explains that the "epistemological impossibility of citizens establishing rationally what is in their common interest leads on to an argument that

---

deviance" including communism, though the RCMP also played a significant part in the FLQ crisis and the abuses of citizens who were engaging solely in lawful dissent (Brodeur, 2003,p. 211). Rights & Democracy (2003) reports that recent legislation and policy changes allow governments to "crack down on political dissidents, separatists and religious groups [and] to create informal criminal justice systems and to adopt restrictive or punitive policies against refugees, asylum-seekers, and foreigners."

democracy needs to be redefined as government for the people by enlightened and responsible elites" (2003, p. 36). Both media and academics have a social responsibility to inform: media are to report, but the contribution of academics is to provide understanding and critiques of social phenomenon. In short, both have an agenda-setting function. Thus, since the public is not adequately informed to tackle issues of government, media and academics are meant to guide opinion and, consequently, action. Kellner expands on this, identifying the central problem of entrusting media and scholars to be the guardians of democracy:

> democracy requires a knowledgeable electorate that can participate in political affairs [as] participatory democracy consists of the sovereignty of the people and thus government, by, for and of, the people. In order for a free people to govern themselves, they must be adequately informed and able to participate in public debate, elections and political activity (2004, pp. 29-30).

The Canadian government has already proved to challenge the freedom of the press where one journalist obtained condemning information[7]. What is clear is that the urge to categorize citizens into two groups, those who may pose a risk and those who do not, may be overzealous and lead to civil rights infractions[8]. Others believe that government is not capable of dealing with these problems of seemingly competing interests (the security-rights dilemma) and will "uncritically accept the premises of the executive branch and police agencies" (Franco Aas, 2009, p. 318).

Citizens are expected to tolerate the deterioration of rights and freedoms without the promise of security in return. With the advent of more sophisticated personal communications systems interception is more difficult, particularly with the use of the Internet and emergent technologies

7 The Royal Canadian Mounted Police (RCMP) raided the house of Ottawa Citizen journalist Juliet O'Neill on 21 January 2004 allegedly related to the recent publication of a news piece on Maher Arar and her use of leaked documents from an unknown source within the RCMP. O'Neill challenged these acts in court and in a "landmark ruling" Judge Lynn Ratushny declared that portions of the *Security of Information Act* were invalid and promoted abuse and misuse (Canadian Journalists for Free Expression, 2006).

8 Predictions made by Paul Knox, a member of the Canadian Journalists for Free Expression [CJFE], in 2001 were confirmed by Juliet O'Neill's experience: the government's extreme categorization became out of control. When Knox opposed the anti-terrorism legislation he warned "that it could lead to the prosecution of a journalist or indeed any Canadian who receives and disseminates information whose publication is clearly in the public interest" (CJFE, 2006). His fears were not without reason.

(Canada, 2002, p. 36). Still, the state is technically able to intrude to an alarming degree into the very personal aspects of its citizens, and this should be understood as a threat to the privacy of Canadian citizens. A position paper written by the campaign for Communication Rights in an Information Society (CRIS), an association of non-governmental organizations and advocacy groups focused on media and communications issues, challenges society to consider the importance of the right for citizens to communicate. In their view, there are many ways in which citizens of democratic societies must be afforded communication rights. For CRIS, the right to communicate has been envisioned as a "general norm based on ideals of participatory democracy" in that all citizens have the "right to hear and be heard, to inform and to be informed" which originates from—but "expands and supersedes[—]the individual rights of freedom of speech, the press and assembly associated with classical liberalism" (CRIS, n.d., p. 2). The problem is, however, that these rights must be forfeited as Webb underscores, "surveillance in a world of pre-emption requires that *everyone* be evaluated as a potential suspect in order to eliminate risk to the furthest degree possible. In this paradigm, criminal law and due process protections...are viewed as intolerable risks" (Webb, 2007, pp. 72-3). What Webb is describing here is the security-rights dilemma. From a pre-emptive perspective, citizens—all citizens—must be willing to sacrifice a little bit of convenience in order to be more secure (Webb, 2007, p. 75).

Pre-emption relies heavily on actionable intelligence, or information that can be readily put to use in terms of planning or immediate action. As some contend, the "first line of defence against terrorism is intelligence" (Canada, 2002, p. 61), but this can certainly be done in a more democratic fashion. Rights and security need not be envisioned as a zero-sum game. Using methods such as racial profiling will not be effective in countering terrorists but may actually lead to more terrorist attacks as a a result of frustration from false accusations or similar situations: "extremists often frame past persecution as a justification for violent action in the present" (Chen, Thoms & Fu, 2008, p. 1). There

are many risks with unduly sacrificing the civil rights of those who are (wrongly) identified as potential terrorists, and governments must consider these risks when formulating policy related to counterterrorism. The case of Maher Arar is only one instance of the problems of increased insecurity and the pursuit of pre-emption at the expense of rule of law and democratic values (Webb, 2007). And all of this is undertaken without any measurable benefits.

Canada's Director General of the National Security Directorate Michel D'Avignon noted that "lawful surveillance of suspect communications is an essential tool in combating terrorism and organized crime" (Canada, 2002, p. 36) though his strategic use of the word "lawful" is a curious choice. Though government officials continue to profess themselves to be lawfully combating terrorism, there are many legal loopholes that allow the government to circumvent established legal safeguards in the name of "national security." In the first instance, reservations have been voiced about the use of the term "national security." Douglas Bland, the current Chair of the Defence Management Studies Program at Queen's University argues broad interpretation of the term renders it almost useless. He prefers to use the definition adopted by the now defunct National Defence College. Here the definition of national security stands as

> the preservation of a way of life acceptable to the Canadian people and compatible with the needs and legitimate aspirations of others. It includes freedom from military attack or coercion, freedom from internal subversion and freedom from the erosion of political, economic and social values that are essential to the quality of life (Canada, 2002, pp. 50-51).

This raises a very important question: where should all these freedoms and security intersect? It is the main argument of this paper that a balance can be struck between the competing needs for security and the preservation of democratic freedoms and values. Whereas the 2004 Speech from the Throne argued that the protection of Canadian citizens is the most fundamental role for government, this does not only involve collective security but must—in Martin Rudner's opinion—include "uphold[ing] the principles of democratic governance, lawfulness and civil liberty, whilst defending Canada against the avowed

enemies of those selfsame ideals" (as cited in Shore, 2006, p. 456). The government's principal duty, therefore, is to provide security while acting as a guarantor of rights (not as a granter of rights). Here it is appropriate to consider the J.S. Mill principle. In his view, governments cannot be justified in placing restrictions on the the rights and freedoms of individuals unless this will prevent harm to others[9]. Many politicians may purport to subscribe to Mill's ideal but in this does not always translate into action.

It is commonly accepted that Canada is less likely to be a primary target for terrorism than is its neighbours to the South; however, "if Canada does not provide an adequate level of security at its borders, the United States is likely to take arbitrary measures to ensure continental security" and it is possible the pressure from the United States may convince the Canadian government to adopt illegal and disproportionate counterterrorist measures (Canada, 2002, p. 37). The pressure for policy harmonization and the already substantive economic integration of Canada and the United States along with multiple signals intelligence sharing agreements between the two countries suggest that it is entirely possible that the systematic and possibly indiscriminate use of domestic communications interception is underway.

Security, the State and Intelligence Work: An Overview

The growth of communications technology over the past century has progressed at an astonishing pace so much so that many believe we are witnessing a communications and information revolution. Though scholars have competing theories about the exact nature of this revolution and argue on points about whom it privileges, most easily agree that technology is changing our lives in

9 In Mill's famous article "On Liberty" he outlines the prerequisite conditions for government intervention: "As soon as any part of a person's conduct affect prejudicially the interests of others, society had jurisdiction over it, and the question whether the interests of welfare will or will not be promoted by interfering with it becomes open to discussion. But there is not room for entertaining any such question when a person's conduct affects the interests of no person besides himself, or needs not affect them unless they like...in all such cases there should be perfect freedom, legal and social, to do the action and stand the consequences" (in Birch, 2007, p.162).

substantial ways, and the way in which the state is dealing with communications is also changing: communications intelligence is now used to a greater degree in this "new" security environment.

First it must be explained how communications is so intimately involved in the security-rights dilemma, and where the state inserts itself. Quite simply, ICT have grown tremendously over the past century, and though they are essentially neutral, they may also be used for illegal purposes. Communications technology provides a fast and affordable way to do things, but this power can be harnessed and manipulated by terrorists to advance their own agenda. This is what Thomas Homer-Dixon has called the "cruel paradox" of information and communication technology, modern high-tech society and the rise of what he calls complex terrorism (2002, p. 52). Communications are very important for networks; however, terrorists are known to exploit communications to further their own goals, and states have taken note of this fact. The Internet and other forms of communications have assisted terrorist groups in "research, planning...fundraising and creating a distributed sense of community" as well as providing outlets for propaganda and platforms for publicity (Brown & Korff, 2009, p. 120). Even the actions of terrorists are viewed as communicative in nature: for example, terrorist violence can be perceived as a costly form of signalling (Kydd & Walter, 2006, p. 50). Because terrorists lack material resources they must compensate for this deficit in other ways. Scholars disagree on the typologies of terrorist strategies. The objectives include but are not limited to "morale building, advertising, disorientation, elimination of opposing forces, provocation [as well as] weakening of the government, enforcing obedience in the population and outbidding" (Kydd & Walter, 2006, p. 56). The logic of all strategies and tactics is central to methods of fear and intimidation used to achieve various aims including "regime change, territorial change, policy change, social control, and status quo maintenance" (Kydd & Walter, 2006, p. 52). Terrorists understand well the symbolic value of violent acts and utilize information and communication technology to advance their own political aims, and this not only involves signalling activities, but very often these activities are also directed as

a psychological attack. Kydd and Walter believe that terrorism is effective "because it instills fear in target populations ...[and] causes individuals to respond in ways that aid the terrorists' cause" (2006, p. 50). The use of communications is instrumental in this process.

In order to capitalize on terrorists' use of ICT, states are relying more on intelligence. Organizations that oversee these activities are asked to "provide foreknowledge to the national leadership...by gathering intelligence information to determine its accuracy, analyzing the information from all available sources, and finally producing and disseminating an intelligence product or report to the consumer" which, in turn, is supposed to assist in making calculated and informed decisions that will maximize the benefit to the consumer or to minimize the harm that may be incurred from a specific event, campaign or political move, whether this be carried out by an individual, non-state actor (including terrorists) or other states (Christianson, 1986, p. 39). Though the function of intelligence remains much the same, the practice of intelligence has changed since the attacks the World Trade Center and the Pentagon in 2001. Before this event, in Canada at least, the main focus was to contain the Soviet threat, and after the collapse of the Soviet Union the Canadian intelligence apparatus adjusted its priorities toward the collection of economic intelligence (Rudner, 2001, p. 115; Morris, 1996).

When one speaks of the historical uses of intelligence, this should not be done without noting the historical *abuses* of intelligence[10]. Arguably the most notorious historical abuse of intelligence occurred in the United States during Richard Nixon's presidency. During Nixon's term the intelligence community abused its power and resources by carrying out an illegal domestic surveillance program. All of these abuses are documented in the U.S. Senate's Church Committee Report, The

10 Abuses can and do happen; however, there is an acute risk that Canada may engage in policy shadowing or that it might engage in the same illegal activities that is currently taking place in the United States. This is why accountability and transparency are critical, and yet in Canada these remain underdeveloped with regards to security and intelligence activities. As Martin Rudner explains, "it is inherently difficult to assess the operational performance of intelligence agencies" (2001, p. 120).

Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, and were made public during the congressional hearings related to the Watergate Scandal (Webb, 2007, p. 51). From these findings it became clear that the intelligence community needed strict boundaries so that such abuses would not happen again. To deal with the situation the *Foreign Intelligence Surveillance Act* was drafted, coming into effect in 1978. The intelligence community in the United States was targeting its own citizens; however, the main reason that these abuses were considered such a serious matter was that these efforts were targeting those who *challenged the political course of the United States*, mainly political groups and entrenched lobbyists.

Canada is not innocent of intelligence abuse either. In the 1970s the Royal Canadian Mounted Police (RCMP) embarked on a similar path, collecting files on more than 800 000 individuals and organizations (Whitaker, 2003, p. 248). The RCMP engaged in other illegal activities, which led to the establishment of the Royal Commission of Inquiry into Certain Activities of the RCMP in 1977, commonly known as the McDonald Commission. The final report, issued in 1981, documented these widespread abuses and recommended the separation of policing and intelligence[11]. Acting on this recommendation, the Canadian government established a new agency, the Canadian Security and Intelligence Service, in 1984. To avoid future abuses, the Security Intelligence Review Committee and Office of the Inspector General were also created to oversee the new agency. Even with a history of abuses with the RCMP stemming from targeting political movements (including the Front de Libération du Québec) and amounting to "secret policing," the Canadian Security and Intelligence Service opened a counter-subversion branch, which was shut down in the late 1980s by the Mulroney administration due to its controversial nature and criticisms of such activities (Whitaker, 2003, p. 248).

Since the attacks, terrorism has become a more important issue for the security and intelligence community, and Canadian scholars engaged in research on intelligence have noted that the "threat of

11 The Commission issued three reports from 1979-1981. They can all be accessed at http://epe.lac-bac.gc.ca/100/200/301/pco-bcp/commissions-ef/mcdonald1979-81-eng/mcdonald1979-81-eng.htm

well-organized and well-funded terrorist networks [requires] new Canadian responses," which Wesley Wark sums up to mean "new resources" (Canada, 2002, p. 107). Not only are terrorists being creative with financing, new technologies allow them to teach and train, research information on potential targets, recruit, publicize activities and new technologies can even allow them to play out various scenarios in virtual space, in some cases they may even use virtual worlds such as Second Life to replicate the area, complete with virtual buildings and the surrounding vicinity (see, for example, Chen et al., 2008; Gourlay & Taher, 2007). Because of these new developments, terrorism becomes a more complex problem for states to deal with. Though terrorism has always been a concern of states, it was viewed as a manageable problem until recently (Gizewski & Geddes, 2002). It appears that the reach and ambition to inflict damage has increased since the end of the Cold War, and there are worries that terrorist action will extend beyond conventional acts of terrorism and finally reaching a point where terrorist acts are "capable and willing to produce casualties and material damage on a scale so great as to weaken the societies and states which they target" through devastating economic, political and physical attacks (whether these are manifested as a physical attack or otherwise) and at which point these acts can only be understood as a kind of "catastrophic terrorism" (Gizewski & Geddes, 2002, p. 1). These challenges require not only new resources, as Wark suggests, but also new approaches to the practice of intelligence and other counterterrorism activities.

Canadian efforts to respond to this development in terrorist behaviour were seen in both instances: additional appropriations were granted to the intelligence community, and organizational changes were made in hopes that this would increase efficiency and limit duplication of work. In December 2003 the Department of Public Safety and Emergency Preparedness Canada (PSEPC) was established to create a "clear accountability for addressing public safety and security issues" (Rostek, 2006, p. 12). Though Canada attempted to separate policing and intelligence activities, the difficulty is that these are closely related activities: this can be seen during the security and intelligence

restructuring. PSEPC unites five separate agencies under one portfolio: Canada Border Services Agency, the Royal Canadian Mounted Police, the Canadian Security Intelligence Service, the Correctional Service Canada, and the National Parole Board. This arrangement suggests that the Canadian government views national security and criminality as closely related issues: PSEPC is responsible for emergency management, national security, crime prevention, and law enforcement/corrections policies. The distinction between terrorist and criminal acts is not entirely clear, even with legislative amendments in the *Anti-terrorism Act* of 2001, and for this reason the intelligence and security community has some overlap in duties and responsibilities; however, the same cannot be said about overview mechanisms. Agencies within the Department of Public Safety and Emergency Preparedness Canada are independent of the department, but function as a hub to provide "policy advice and support"; however, it is quite interesting that the Communications Security Establishment is absent from this "roundtable" on security, even though it is often called upon to assist both CSIS and the RCMP [12](Who we are, 2009).

Intelligence and security are related, but they are not exactly the same. In 2003, the Standing Committee on National Security and Defence listed the following agencies and departments involved in intelligence work: Department of the Solicitor General, Royal Canadian Mounted Police, Department of National Defence, Office of Critical Infrastructure Protection and Emergency Preparedness, Department of Foreign Affairs and International Trade, Citizenship and Immigration Canada, Customs and Revenue Agency and Privy Council Office, along with CSE and Canadian Security and Intelligence Service (Canada, 2002, p. 124). No fewer than ten agencies are involved in intelligence gathering (as differentiated from belonging to the central *security* hub of PSECP), and each

12 Since the establishment of PSEPC Canada issues the "first comprehensive statement" outlining its national security policy within which it was announced that a National Security Advisory Council would be established with a specific focus on security intelligence. The Canadian government also committed itself to creating an Integrated Threat Assessment Centre to bring together CSIS, the RCMP, the CSE, National Defence, Foreign Affairs, the Privy Council Office and PSEPC (Shore, 2006, p. 459-60). There are also additional key members including provincial authorities and several other national agencies (Integrated Threat Assessment Centre, 2008).

has its own specific cooperative agreements; however, of these ten agencies, only two are subject to external review or have formal oversight agencies (Canada, 2002, p. 124)[13]. The increased premium on sharing intelligence was promoted by the United Nations Security Council Resolution 1373 which "calls on states to intensify and accelerate the exchange of information regarding terrorist actions and movements" and most governments have embraced and aggressively advanced this resolution through their own legislation (Webb, 2007, p. 139). Furthermore, criminal and intelligence and security agencies are all implicated in this sharing arrangement.

Intelligence sharing has accelerated within Canada and most of these domestic intelligence sharing practices are guided by Memoranda of Understanding (MOUs), which relate to the structure and processes of collaboration and exchange of information[14]. The threat of terrorism has also influenced international intelligence sharing agreements. One of the most significant intelligence sharing agreements in the world is UKUSA, a five-party cooperative agreement related to signals intelligence among the United States, Britain, Australia, New Zealand and Canada, of which the specific arrangements are detailed below[15] (American Civil Liberties Union [ACLU], 1999). UKUSA is an agreement that relates to signals intelligence or SIGINT. This may also include communications intelligence (COMINT) as signals intelligence is defined by CSE as "foreign electronic emissions collected by CSEC[16]...used to produce intelligence reporting that responds to Canadian government

13 Only CSE and CSIS have formal oversight review agencies. The CSE's relationship with other agencies are often outlined in memoranda of understanding (MOUs), as is the case with the Department of Foreign Affairs, CSIS and the RCMP (Rosen, 1993, p. 9).

14 The CSE and the RCMP signed an MOU in October 1989 and have also signed two MOUs with CSIS under sections 12 and 16 of the *CSIS Act*, related to security and foreign intelligence respectively (Rosen, 1993, p. 9).

15 UKUSA provides a "virtually seamless global intelligence collection capability for various modalities of signals intelligence" (Rudner, n.d., p. 9). Due to improvements in the hardware necessary for interception and the software used for analysis, notably the Echelon system or "dictionary" to seek out specific information including "names, topics of interest, addresses, telephone numbers" or anything else that is programmed to be identified, UKUSA is a very important intelligence sharing agreement (Rudner, n.d., p. 9).

16 The Communications Security Establishment was renamed the Communications Security Establishment Canada in 2007 to bring the agency into compliance with the Federal Identity Program which requires that all federal agencies and departments include "Canada" within its title. Though its formal name is the Communications Security Establishment Canada many continue to refer to it simply as the CSE as this continues to be the agency's legal title.

requirements" (CSEC: FAQs, 2008). Collection of foreign signals are made possible "by means of sophisticated, covert interception technologies designed to intercept terrestrial, microwave, radio and satellite communications along with other electromagnetic emissions" (Rudner, 2001, p. 103). The collection of signals intelligence can be all encompassing as communications collected and analyzed by CSE—where legal restrictions do not prohibit such interception— include "any information carried on the global information infrastructure, which would include electronic emissions, communications systems, Information Technology systems and networks, and the data and technical information on or related to those systems" (CSEC: FAQs, 2008). As most communications are now digital, the CSE has a great interest in communications ranging from telephone calls, traffic data and private emails, though access to this is allegedly limited to an acceptable degree by legislation.

The type of signals intelligence engaged in during the First and Second World Wars is now very different than the type of work that the CSE is engaged in now. In a Maclean's article on the CSE, author Nomi Morris explains: "set up in 1941 to decode enemy telegraphy and radar, the service's technology has now evolved to cover cellular telephones, faxes and even emissions from computer screens or electric typewriters" and, quoting a former CSE agent, "there isn't a thing that's radiating that they can't get" (1996, p. 32).

The state seems to understand that it must keep up with emerging technologies if intelligence is to contribute to effective counterterrorism activities, and it is no surprise that "in the immediate aftermath of the terrorist attacks of September 11, the government of Canada injected funding of almost $47 million to CSIS and to the CSE to expedite improvements in their capabilities to collect foreign intelligence," and $37 million of this was granted to CSE to allow for upgrades to its interception infrastructure (Rudner, 2002, p. 25). Additional funds followed with a promise of $7.7 billion over a five-year period with these funds being granted to assist with improvements to border security, policing, emergency response, as were also to be used to provide better equipment and to employ more

personnel in the intelligence sector intelligence (Shore, 2006, p. 458).

There are many different subfields in intelligence but communications intelligence, as a more specific form of signals intelligence, is important for counterterrorism efforts as new information and communication technology assists terrorists in achieving their goals. Terrorists actively use ICT to create more cohesive networks. There is much public discussion about the possible use of the internet by terrorists to wage cyber attacks; however, as experts in conflict arising in the information age Arquilla, Ronfeldt and Zanini point out, terrorists "may often have stronger reasons for wanting to keep it up (e.g., to spread their message and communicate with one another)" (1999, p. 41).

While terrorists can attack some parts of communication networks, they can manipulate other parts to their own benefit. The attacks of 9/11 exemplify the way in which terrorists exploit communications in the information age. Images of the attacks were presented to the public in a near instantaneous fashion and repeatedly via various forms of media. Videos of the attacks were broadcast on network television stations and over the Internet, and the repeated viewing of these events had an "impact on the collective psyche of a nation...and subjective feelings of security and safety" (Homer-Dixon, 2002, p. 57). Terrorists, Homer-Dixon explains, are more tolerant of risk, which gives them leverage (2002). There is no fear of suicide, incarceration or other forms of self-sacrifice, rather the desire to attain an ultimate goal. Mark Juergensmeyer, director of the Orfalea Center for Global and International Studies and prolific author on topics related to religious violence, states that this confidence comes from the belief that terrorism is mandated by God, and that the acts themselves are simply the "public performance of violent power" (1997, p. 17). Whereas terrorists are able to bear the costs, assume greater risks and use communications technology to amplify their messages of violence, governments are less willing to take risks. Instead of risking a *possible* attack, the state is willing to impinge on its citizens' communication rights (Homer-Dixon, 2002, p. 62). This is done without consent, without notice, and without the proper administrative, legal and ethical checks and balances.

Communications technology are important: they are routine, habitual, and necessary. Most importantly, they are *politically* and *socially* important. For these reasons, surveillance is a common activity carried out by the state and other actors. Surveillance activities are also expansive: they include the simple collection of information which then constitutes surveillance once the information is analyzed and used. In terms of counterterrorist strategies, states are able to use information collected from various databases to form risk profiles of individuals, organizations and other countries; however, the legality of communications surveillance is limited by the need to protect privacy and other rights. For law enforcement, this means obtaining a warrant; however, there have been worrisome moves in Canada that suggest the state is looking toward making ubiquitous surveillance easier by removing these legal procedures that determine whether this activity is necessary or does not unduly intrude on a citizen's rights[17] (Webb, 2007, p. 123). Because of the risk of not properly identifying and dealing with terrorist threats is perceived to be great, the state is compelled to treat everyone as a potential suspect, and thus the due process protections hinder the state's ability to investigate everyone, if warrants continue to be necessary (Webb, 2007). Although citizens may appeal to legal arguments based on rights to privacy, another avenue of appeal can be made on the basis of social value. As David Lyon explains: "the debate on surveillance should begin outside the box of common assumptions about privacy as an individual matter, the zero-sum game of security and liberty and the pernicious *non sequitur* that if you have nothing to hide you have nothing to fear" (2007, p. 176). This should not and must not be an argument used to legitimize the illegal domestic interception of communications as privacy is not simply an individual value. If privacy is envisioned as an individual value, then the more significant societal benefits of privacy are negated (Solove, 2008).

Just as the value of privacy can be overlooked, the value of communications is often

17 For example, a bill was introduced in January 2006 before the defeat of the Liberal government that sought to allow police enforcement officers to access the subscriber records of telecommunications service providers without a warrant. At the same time another bill was being drafted that would lower the legal standards necessary for access to traffic and cell-phone location data (Webb, 2007, p. 123).

underestimated even though communications "enlarg[e] our understanding and the experience of the world, each other, and our own humanity by exercising us mentally, emotionally, sensually and spiritually...[and vulnerabilities through communication] release us [from] anxieties, insecurities, and paranoia that make us afraid of the world, each other, and even our own humanity" (Rodriguez, 2008, pp. 6-7). Communication is therefore transformative and liberating as an conduit of knowledge, where knowledge is a form of power. Others agree that it is "through the communicative process [that] individuals continually develop themselves and their communities" but this is also the "primary process through which humans create their collective and individual realities and identities" (Pestana & Swartz, 2008, p. 92, 100). Just as privacy has come to be accepted as a right, the same could be said of communications, at least in the normative sense, or should be envisioned as having legal protection as an extension of privacy rights. Professor of International Communication at the University of Amsterdam Cees Hamelink (in Mueller, Keurbis & Pagé, 2007) argues that "the right to communicate addresses the core of the democratic process as well as the essence of most [if not all] social and personal relations" (p. 275). Free communication between government and public is an essential part of democratic governance. In a commentary about the relationship between citizens and the state, Katja Franco Aas describes how surveillance and data collection could permanently alter this relationship as we are made to consider the level of state interference, the need for security, the right to privacy and "the centrality of privacy for maintaining a free and democratic polity" (2009 p. 317).

There are some legal orders in place that are meant to preserve the rights of citizens; however, increased cooperation among law enforcement means that SIGINT interceptions may be used for other purposes than its intended targets. There are are certain limitations placed on this integration and extension including the existence of "legal and technical prerequisites governing interceptions for law enforcement purposes," and furthermore it is expected that the distinction between law enforcement and communications intelligence interceptions "must be observed operationally and reciprocally within

multiple legal orders and jurisdictions" (Rudner, 2001, p. 123). If the distinction between law enforcement and intelligence is not observed, the resultant ambiguity risks "dangerous illegalities and human rights transgressions" that are simply not acceptable (Rudner, 2001, p. 123). Additionally, intelligence sharing blurs these lines of responsibility. The American Civil Liberties Union has commented on this development: "at the same time that the dividing line between domestic and international communications has blurred, so has the dividing line between law enforcement and foreign intelligence" (ACLU, 1999). This blurring has progressed since 9/11 though the trend was observed long before these events[18]. Even the Department of Foreign Affairs and International Trade states that global consensus and cooperation is necessary "to prevent and prosecute terrorist *crimes*" (DFAIT, 2008, emphasis added). Furthermore, the department has noted that a multifaceted approach to terrorism is necessary, and effective counterterrorism strategies will require "diplomacy, intelligence, security and law enforcement, customs and immigration, transportation, justice and finance expertise" (DFAIT, 2008).

The *Anti-terrorism Act* apparently understands that the distinction between criminal and terrorist acts continues to be a fine one, and one that is not always apparent. In a panel discussion, top RCMP officials concluded that criminal justice is an important aspect in a comprehensive and effective counterterrorism policy as "[a]ll terrorist acts are criminal," but it is still not clear as to when criminal acts become acts of terrorism[19] (Paulson, Kenny & Inkster, 2008, p. 12). In this forum it was also admitted that a significant challenge to enacting effective counterterrorism strategies is the definition of terrorism itself, citing the common mantra "one person's terrorist is another person's freedom fighter"

18 Bruce Hoffman provides several case studies to supporting the claim that the distinction between domestic and international terrorism is unclear. In his study *The Confluence of International and Domestic Trends in Terrorism* he offers several examples. Threats are commonly both domestic and international. Here he cites the "Aum sect's activities in Russia and Australia as well as Japan, the alleged links between the Oklahoma City bombers and neo-Nazis in Britain and Europe, and the network of Algerian Islamic extremists operating in France, Great Britain, Sweden, Belgium and other countries as well as in Algeria itself" (Hoffman, 1997, p. 10).

19 One respondent in the Millward Brown Goldfarb research group noted that he could have been deemed a terrorist several times in his lifetime, according to the definition provided within the *Anti-terrorism Act* (2004, p. 24).

and adding that "terrorism needs to be seen as a source of harmful criminal activity" (Paulson et al., 2008, p. 13). The government continually stresses that the *Anti-terrorism Act* is necessary and "continue[s] to be necessary"; however, most of the terrorist activities could easily be dealt with under the *Criminal Code* or other legislation in place before 11 September 2001 (Frequently asked questions [FAQs], 2009).

The government has implemented a strategy focused on pre-emption "given the issue that once a terrorist event takes place, it is too late," and so "the [*Anti-terrorism* Act] created offences that criminalize activities such as 'participation' in a terrorist group, that take place before a more dangerous terrorist event can occur" (FAQs, 2009). The new investigative activities afforded to law enforcement and security and intelligence personnel do not fall within the classic central goals of the criminal justice system of "prevention and deterrence," but are pre-emptive, though not to the extent of some other states[20] (FAQs, 2009). Furthermore, the most contentious provisions within the *Anti-terrorism Act* initially subject to a sunset clause were barely defeated in the House of Commons in 2007, even with the overwhelming number of public objections by Canadian citizens and in spite of the various Parliamentary Committees that recommended their extension[21] (FAQs, 2009). If the most contentious issues are opposed vocally, are defeated and reintroduced once public outcry has lessened, it suggests that less contentious (or wholly ignored) issues such as the interception of domestic communications might be easily and silently legislated. After all, there are provisions in the *Anti-terrorism Act* that

20 Although Canada has policy shadowed the United States in the past, there are some notable exceptions where Canadian practice diverges from that of the United States or other influential allies even when pressure to conform is exerted. For example, Canada has refused to support indefinite detention based solely on suspicion and non-Citizens are protected under the Charter after the Supreme Court ruling in the case of Singh in 1984.

21 Ultimately the resolution to extend for an additional three years was put forth and defeated with a vote of 159 to 124 and the provisions expired in March 2007. Somewhat underhandedly the Senate reviewed and passed Bill S-3, *An Act to amend the Criminal Code (investigative hearings and recognizance with conditions)* in October 2007, which reinstates these provisions "in a form substantially similar to the original 2001 provisions" (FAQs, 2009). The Canadian government appears to subscribe to the well-known saying "if at first you don't succeed, try, try again". It should also be noted that before the initial sunset of this provision section 83.28 of the *Criminal Code* relating to investigative hearings was invoked by a Provincial Attorney General; however, the hearing did not convene, which questions whether these extreme provisions are necessary, as the government continues to argue (FAQs, 2009).

"allow the minister of defence to authorize *the same kind of program* in Canada as President Bush's secret, unlegislated NSA program in the United States. In other words, the Canadian government has legislated what the Bush administration dared not legislate" (Webb, 2007, p. 124).

The tension between the state and its citizens with respect to security does not end at surveillance. Even the collection of personal data raises questions about "democratic practice, social justice and moral obligation [as] personal data pertain to human beings whose life chances and choices are affected for good or for ill" [22] (Lyon, 2007, p. 176). According to Daniel J. Solove, a Professor of Law at George Washington University and acknowledged expert on information and communication technologies, there are specific domains for privacy that must be respected and upheld including privacy for the family, body, sexual activity, home and communications (2008). State surveillance of communications relates to the social welfare of its citizens, but there are also tensions and concerns arising from intelligence sharing both within Canada and with other states, with most of these problems related to transparency and accountability, the (in)visibility of surveillance and the lack of knowledge about the potential risks and the ability and technologies that might permit illegal domestic surveillance of communications in Canada. Since the state has historically pitted dealing risk and rights against one another, and has traditionally privileged security over rule of law and the rights of citizens, the reliance on information and communication surveillance as a counterterrorism strategy must be reassessed. These issues are especially pressing for the CSE, particularly given that intelligence is regarded as a

22 If the surveillance of communications and digital data reports are known or suspected, this can affect behavioural and social patterns. For example, if an individual is a foreign-born Arab Muslim will this individual feel they are unable to contact family members within his or her country of origin? And, as a result, will familial relations suffer? Will non-Arab and non-Muslim citizens restrict their interaction with these populations in order to avoid being implicated as a terrorist? Will knowing about communications surveillance place limits on intercultural interactions and lead to an ethnocentrist alienation of "at risk" populations? How will this affect the cultural fabric of Canada? These are all questions that must be considered and questions that demand more transparency and accountability from the CSE and other agencies that may be involved in communications surveillance in Canada. If there are any lessons from the Cold War that should be remembered it's that fear can manifest itself as abuse and exclusion. The War on Terror is a more populist struggle than the Cold War and therefore "the danger of populist authoritarianism is very real to vulnerable minorities—in this case the Muslim and Arab communities—and to the fabric of liberal democracy" where ethnic victimization may be but one product of the War on Terror (Whitaker, 2003, p. 252).

flawed endeavour, and there are specific challenges and drawbacks associated with signals and communications surveillance[23].

Terrorists' use of ICT greatly assists its organizing efforts as these networks are organized horizontally, which allows for a "fully interconnected network...[with the capacity to constantly exchange] dense information flows" that is much more efficient than any other form of organizing (Arquilla et al., 1999, p. 52). It is difficult to disable or disrupt terrorist networks as the state is traditionally organized vertically, whereas terrorist networks are distributed horizontally and, according to Arquilla et al., "it takes networks to fight networks" (1999, p. 54). To respond to the challenges of terrorist networks, states need not completely reorganize themselves; however, they must be willing to conclude interagency agreements and achieve multijurisdictional cooperation (Arquilla et al., 1999, p. 55).

As reviewed in this section, given the importance ICT use by terrorists, technology is a "critical arena in the war against terrorism" (Don, Frelinger, Gerwehr, Landree & Jackson, 2007, p. iii) and governments must be able to identify the technologies used in support of terrorist operations and "understand terrorists' decisions about when and under what conditions particular technologies will be used to determine the implications of these insights for efforts to combat terrorism" (Don et al., 2007, p. iii). As communications are so essential to terrorist activities and the surveillance of these communications is a preferred strategy for counterterrorism, the main objective of this paper is to identify how the CSE functions within the security-rights dilemma and the related issues stemming from domestic surveillance activities in Canada.

---

23 Mistakes are bound to happen from time to time but intelligence officials look at these as opportunities for learning. Marrin believes that the multi-step process of intelligence involving "the acquisition and accumulation of information, its interpretation, and subsequent dissemination to policy makers is an iterative process" cannot provide the entire story (2004, p. 657). Intelligence provides imperfect information, but even this has its uses. Richard Betts, one of the first scholars who sought to develop a normative theory of intelligence failure admitted that "not only are intelligence failures inevitable, they are natural" (1978, p. 88).

The Communications Security Establishment—Canada's Best Kept Secret

The systematic use of intelligence in Canada is a relatively new phenomenon, and the history of its use does not provide a solid tradition or pattern of behaviour. This section charts the historic direction, methods and procedures of the CSE, and finds that there are three rather constant characteristics of behaviour for the CSE that may have residual influences on the future practice of signals intelligence in Canada. From accessing available public documentation on Canada's Communications Security Establishment, three trends are observed. Though it is difficult to maintain that these trends offer a formulaic projection and can predict the actions and policies of this agency in the future, these trends still provide a worthwhile reference. For this section the effort of analysis is focused on the thematics of behaviour and therefore avoids a singular chronological logic and approach[24]. The three observable trends are as follows: Canadian signals intelligence is highly underdeveloped, signals intelligence is undertaken hesitantly, and Canadian signals intelligence is highly reliant on allied powers for support and direction. Understanding the nature of Canadian intelligence is an important way to provide greater elucidation into the possibility for illegal domestic surveillance in Canada.

First "signals intelligence" must be defined. Signals intelligence involves the interception and analysis of "radio, radar and other electronic transmissions" (Rosen, 1993, p. 5). Though there have been several instances of "success" in signals intelligence for the CSE, Canadian signals intelligence is still highly underdeveloped. With respect to the successes, reports indicate that signals intelligence provided early detection of the Toronto-based Jihadist group in 2006[25] (DePalma, 2006, p. A12).

24 For a more in-depth history of the CSE readers are encouraged to see Mike Frost and Michael Gratton's *Spyworld: Inside the Canadian and American Intelligence Establishments* (1994), a government-commissioned publication by Rosen (1993) entitled *The Communications Security Establishment-Canada's Most Secretive Intelligence Agency* or Rudner (2001, 2002, 2007) also provides a more detailed history of the CSE.

25 Rudner attributes the advance knowledge of the plot with the code-name "al-Badr" to the surveillance of Internet and telecommunications traffic though he admits that "the precise role of the CSE in these investigation is classified" though it is likely that the CSE played a large role and assisted other intelligence and law enforcement agencies (Rudner, 2007, p. 483).

Signals intelligence is also said to have discovered an Algerian "Armed Islamic Group" cell in Montreal that was planning to attack the United States on New Year's Eve in 2000 (Rudner, 2001, p. 116). Canadian signals intelligence scholar Martin Rudner commends the achievements of the CSE for "becoming a substantial producer of foreign intelligence" in the 2000s and its ability to provide close to 85% of intelligence requirements for Canada (Rudner, 2007, p. 482). Whereas producing 85% of the required foreign intelligence for Canada seems like a success, I argue that this figure only highlights how underdeveloped signals intelligence in Canada really is. The inability to satisfy 100% of the intelligence requirements indicates that the programs and systems are not working for the Canadian government, and they are inefficient or ineffective.

There are several intervening factors that provide for the underdevelopment, hesitation and dependency of Canadian signals intelligence:

1) Canada does not have the required and most up-to-date technology to be a main provider of intelligence, which is an important aspect of signals and communications intelligence;
2) The organization and hyper-compartmentalization of Canadian intelligence does not promote efficient intelligence work; and,
3) Canadian intelligence as a whole suffers from a lack of personnel.

Technology is a very important part of signals intelligence. There is almost unrestricted public access to encryption and cryptography equipment, which makes intelligence and law enforcement efforts more difficult. In a government report in 2002, senior officials disclosed that publicly available programs and technology "threatens to neuter an essential source of intelligence about the activities of spies, terrorists, and criminals" (Canada, 2002, 36). Counter-measures are costly, and, although there have been heavy expenditures on new technology in policing, it is less clear as to whether this is paralleled in the CSE. Various methods of communication, and the increasing number of service providers, as well as the expanded services that are offered, make communication intelligence work more difficult. Personal communications systems that are digital are more complex to intercept, and

the Internet, Voice-over-Internet-Protocol, chat rooms, social networking and even online gaming are all different systems that may "allow violent groups to marshal resources and coordinate activities"[26](Homer-Dixon, 2002, p. 54).

As a measure of scale, technologies used by the CSE are more sophisticated than the more mobile and personal surveillance apparatus used by law enforcement agents, and technology used by the CSE can also be exorbitantly more expensive. Though the CSE is very secretive about its expenditures and technological acquisitions, it is clear from historical data that Canadian intelligence has not invested enough into technology to keep up with the massive volume of data and communications[27]. Datamining systems were introduced in order to deal with this deficiency; however, datamining is not perfect—once an anomaly or a point of interest is identified, it is imperative that a human intelligence analyst review these data sets more closely.

The introduction of human analysis is necessary; however, staffing is a persistent problem in Canadian intelligence[28]. There were vast cuts to the intelligence community after the fall of the Soviet bloc, and the governments of Jean Chrétien and Paul Martin were "preoccupied with eliminating

26 Different phone service plans (pay-as-you-go, for example) allow terrorists to use cellular phones as one-time-use and dispose of them immediately, if they so choose. There are also reports of terrorist groups using a method called stenography which involves hidden writing within other digital media. For example, a message may be written into digital media such as photographs or music clips and be posted on the Internet where it is able to be accessed by others or downloaded when necessary (Homer-Dixon, 2002, p. 54.)

27 Reports indicate that the United States gave the following technologies to the CSE: "Cray super computers, miniaturized interception and processing equipment for outplacement interceptions, high-capacity/high-speed information retrieval technologies, and high-speed traffic/topic analysis search engines." CSE has also used NSA facilities and relied on the NSA for technical consultation and training (Rudner, 2007, 478-9).

28 Employing intelligence personnel can be costly after the end of the Cold War the Canadian government neglected the intelligence community. This is evidenced by the nearly 25% reduction of CSIS between 1993 and 2002 and similar cuts were made for other intelligence agencies (Canada, 2004, p. 105). Though after 11 September 2001 more funds were allocated to better equip and staff the security and intelligence community, these funds could be seen as "too little too late" as it takes a lot of time to train new intelligence officers. In hindsight "the cuts of the 1990s were unwise" (Canada, 2004, p. 105). Related to the new allocations in the immediate aftermath of September 11th and in April 2004 an additional $137 million was granted along with up to $30 million over five years to establish a centralized intelligence agency within the Integrated Threat Assessment Centre (Canada, 2004, p. 106). These funds were also applied to recruitment and the Communications Security Establishment was said to have approximately 1000 employees in 2002, an increase of nearly 250 personnel since the attacks in 2001 (Canada, 2004, p. 206). Centralization and reorganization was meant to relieve the personnel problem in the security and intelligence community. Establishing the Integrated Threat Assessment Centre and the creation of a new "super-ministry of Public Safety and Emergency Preparedness" were meant to provide a "central threat assessment capacity to evaluate and prioritize potential threats, whether terrorist or non-terrorist, for the purpose of rationally allocating resources" (Gabor, 2004, p. 14).

budgetary deficits and reducing the national debt" but, as the 2005 Canadian Security Guidebook illustrates, "there is more to governing than frugality" [29](Kenny & Forrestall, 2004, p. 5). During these years the national priorities did not focus on intelligence, which led to Canadian intelligence, and signals intelligence in particular, relying on its allies more than it had in the past. Burden sharing is a defining feature of Canadian intelligence, but now must be accelerated as Canada lacks the personnel and equipment and the organization of Canada's intelligence community continues to promote the duplication of work, despite efforts for reform.

Where Canada lacks the technology itself, often it is given de facto access through its international intelligence sharing agreements. It is reasonably believed that the Canadian intelligence system is deeply integrated with the system of the United States, given the similar security concerns and regional proximity, although definitive statements are not possible as these arrangements remain classified. Canadian intelligence is put at a severe disadvantage because it must rely on the United States for access to certain equipment and programming and does not have anything of similar value to offer the National Security Agency (NSA)[30]. Due to this unbalanced partnership and the "limited terms of trade" for Canadian intelligence, the CSE can be seen only as a junior partner within this intelligence arrangement, and, as with almost all unbalanced relationships, there is the possibility that the NSA may convince or coerce the CSE to involve itself in more aggressive (and illegal) surveillance activities within Canada (Rudner, 2001, p. 103). Or, alternatively, if Canada refuses, the United States may take matters into its own hands.

---

29 Parallel to, and perhaps the cause of,the reduction of personnel, government appropriations for the Communications Security Establishment were 10% less than the level of funding provided in 1990/1, estimated at about $113 million in 1995/6 (Rudner, 2007, p. 478). Not only was the CSE not provided with the funding it needed, it was not a priority for government as appropriations to the CSE were much less than other intelligence and security agencies (Rudner, 2007, p. 479). Even where other agencies such as the Canadian Security and Intelligence Services (CSIS) are said to be funded better than the CSE Senator Colin Kenny remarks that CSIS is not well-equipped either: "How is it that CSIS, Canada's anti-terrorist nerve centre, has fewer employees now that it had 18 years ago?" (in Paulson, Kenny & Inkster, 2008, p. 13).

30 Canada attempted to develop its own speciality to balance the terms of trade. Attempts at developing word-spotting technology in the 1990s failed and the only niche area that Canada established some kind of independent capability is in voice/topic recognition technology and software (Rudner, 2001, p. 114).

The risk of policy laundering—one country's proclivity to transplant and adopt similar or identical policies originating from another country—is therefore great given the overwhelming power of the United States in terms of intelligence compared to its Canadian counterpart. As part of the grander scheme of surveillance activities—though not specifically in reference to communications surveillance—the United States has already proven itself to be a rather convincing ally during initial debates about the use of biometric passports. Didier Bigo believes that the " 'unanimism' of the professionals of politics after September 11th created a specific period for the enunciation of a discourse of necessity of war against terrorism and suspicion against foreigners, ethnic and religious minorities" convinced skeptics to finally agree with the measures as "a necessary act to protect the people and to reassure the task of collective survival" (2006, p. 49). This is a discourse that may not be as pronounced as it was immediately after the terrorist attacks, but it continues to thrive nonetheless, and is continually cited as the rationale to legitimize the *illegitimate* practices of democratic governments, including Canada. David Lyon argues that surveillance activities (biometrics, increased use of closed-circuit television and communications surveillance, for example) are ways in which the government is trying to make citizens into "molded subjects" (2006, p. 13). The fear is that these new forms of surveillance were instituted in a time of exception or emergency are now becoming routinized, constituting a form of governmentality which remains unacceptable within democratic states (Bigo, 2006, p. 50). Webb also recognizes this shift toward greater surveillance, but she contends that the government is promoting this movement. She notes that even though the use of biometric passports was rejected in Parliament in 2002 and the proposal was abandoned in 2003, it was later renewed after the government restructured in 2005. Debates on the matter a few years prior were not given consideration and no new debate was undertaken. The government simply "claimed that it had no choice in the matter" (Webb, 2007, p. 95). All of these various forms of surveillance have effectively amounted to ubiquitous surveillance; however, communications surveillance should be a particularly

important issue in Canada given the controversy and blatant rights violations in the United States. There are other instances where government has tried to legitimize its own illegal acts in relation to intelligence gathering, use and implementation. First it is important to understand the traditional intelligence organization, its progression and how this influences the practice of intelligence today.

States have often had intelligence sharing agreements and this holds true for Canada as well. The UKUSA agreement is considered to be the most significant intelligence arrangement in the world. Through this agreement Canada is tied to the U.S. National Security Agency, the British Government Communications Headquarters, the Defence Signals Directorate in Australia and New Zealand's Government Communications Security Bureau[31]. As noted earlier, Canada is a junior partner within these agreements; however, due to its extended relationship with the United States' and British intelligence agencies[32] Canada is often favoured over Australia and New Zealand. Regardless, this arrangement involves substantial intelligence sharing among these states including the interception of "e-mails, faxes, electronic transactions and international telephone calls carried via satellites" (Webb, 2007, p. 133). The problem is that Canada is a junior player and the exact nature of the intelligence sharing arrangement is classified. It is extremely difficult to assess what kinds of priorities Canada might have or the activities in which it participates. David Bashow argues that, "in reality, security policy in Canada, when it has existed at all, has been more ad hoc than codified in a structured manner," which suggests that Canadian security policy is reactionary in nature (as quoted in Rostek, 2006, p. 2). Canada has had a difficult time shaping the nature of its own SIGINT activities and has looked to its allies to help the design and direction of Canadian activities. The Canadian signals intelligence entity was to be a mini-Bletchley (naming Britain's Bletchley Park SIGINT complex) or a

31 More information on CSE's "peer organizations" can be accessed at http://www.cse-cst.gc.ca/home-accueil/about-apropos/peers-homologues-eng.html

32 A joint Canadian-American intelligence agreement (CANUSA) was signed in 1948 and one that also included Britain—the BRUSA agreement—was concluded in 1946. It is important that both of these agreements were forged in the initial stages of Canadian signals intelligence and may have contributed to the somewhat paternalistic relationship, particularly with the United States in the post-Cold War.

Canadian Black Chamber, the name given to the United States' secret room where decoding occurred. The desire to model these agencies, along with the assistance granted to Canada by the United States and Britain, has influenced the shape of the CSE. The Communications Security Establishment's late development and emulation of Bletchley and the Black Chamber has made it a nascent pseudo-replica on a much smaller scale. For these reasons, the CSE has "toiled in alliance obscurity [and] it very occasionally raised a cautious criticism, only to be quickly cuffed for its temerity" (Whitaker, 2003, p. 242).

With the number of staff and up-to-date equipment, it is no surprise that the United States and Britain would wield greater influence in UKUSA and other international intelligence arrangements. After all, in 1944 the CSE's predecessor of that time, the Examination Unit, had only 45 staff members[33](Rosen, 1993, p. 3). The CSE was not only obscure within alliances, but it was also obscure within Canada. The existence of a signals intelligence agency was not publicly acknowledged until 1974 when a Canadian Broadcasting Corporation broadcast an exposé of the Communications Branch of the National Research Council, the predecessor of the CSE at that time (Rosen, 1993, p. 3). Shortly after this the public was made aware of the UKUSA agreement on 24 March 1975 in a House of Commons Standing Committee when the Minister of State for Science and Technology Honourable C. M. Drury was forced to answer questions about Miscellaneous Estimates (Rosen, 1993, p. 3). Signals intelligence in Canada has not been straightforward and there have been many instances of restructuring and disagreements related to the various competing interests on how signals intelligence should "best" be done.

The first signals intelligence efforts were undertaken by the Royal Canadian Navy in 1939 but the Air Force and Army soon developed their own capabilities. Later still a civilian section was

33 The staff of the CSE grew in 1975 to about 250-300 and by 1983 was said to staff nearly 580 civilians (Rosen, 1993, p. 4). Although renewed interest has seen the staff at the CSE reach 1750 in 2009 comparatively this is a rather small contribution (Pugliese, 2009). The exact size of the NSA is classified, but to provide some measure of reference it is estimated that the NSA employs about 36 000 workers and continues to expand (Sernovitz, 2009).

established. The military and civilian interests are not always compatible with one another and this may be the impetus behind repeated efforts to restructure and rebrand signals intelligence in Canada. Signals intelligence activities have been undertaken by many different agencies and the civilian-based predecessor and first permanent signal intelligence effort within the Communications Branch of the National Research Council was an "official secret" for 28 years, from its establishment in 1946 until 1974. Furthermore, the CSE was not given an explicit public mandate until the passage of Bill C-36 as part of the *Anti-terrorism Act*.

Though this does not directly prove that the agency was not—and is not—provided with sufficient direction from government as to its mandate and operative goals, the fact that these are all contained in secret documents and considering Canada has not clearly articulated its foreign and security policies suggests that intelligence and security priorities may largely be defined by membership within these international agreements. This inclination and perceived imperative for secrecy challenges the principles of democratic governance. Secrecy does not allow for the public to participate fully and it restricts public accountability of government institutions. With regards to intelligence, the public is not allowed to be the "knowledgeable electorate" that Kellner insists is necessary for a healthy democratic governing system (2004, p. 29). With signals intelligence this need for secrecy is compounded; however, the government seems contend that its use of intelligence and secrecy are all in the best interest of the public and that if full disclosure was possible, the government would freely offer this information. As then Justice Minister Anne McLellan noted in 2001, "I wish you knew what I know" (Schneiderman, 2001, p. 64). In the case of signals intelligence very little is known about the nature of Canada's contribution within international SIGINT arrangements; however, there are a few things that are widely understood about the agency and its activities and Canada's role internationally.

It was only in 1991 that the Canadian government provided its first directive on foreign

intelligence priorities (Rudner, 2001, p. 99). Though the policy direction for Canadian signals intelligence is to come from the Privy Council Office the CSE has dual accountability, with the Department of Defence retaining administrative control (Rudner, 2007, p. 474). The Communications Security Establishment is not simply engaged in signals intelligence but it is also charged with providing Information Technology Security by "help[ing] ensure that the Canadian government's telecommunications are secure from interception, disruption, manipulation or sabotage by others" (Rudner, 2007, p. 475). The CSE also "provide[s] technical and operational assistance to federal law enforcement and security agencies" (Rudner, 2007, p. 475). The CSE is therefore not only linked to other international signals intelligence agencies but the CSE also works closely with other Canadian foreign security and law enforcement agencies.

UKUSA, the main international agreement on signals intelligence that Canada is involved in, is driven by a program called Echelon. Echelon is described as an automated global surveillance of Intelsat satellites targeting the world's satellite phone calls, internet, email, faxes and telexes [34](Wright, 1998, p. 19). The United States is considered the "senior partner in this system"; the four other UKUSA members, including Canada, act as subordinate information servicers (Wright, 1998, p. 19). Although UKUSA members claim they do not target their own citizens or share this kind of information with partner countries in UKUSA, the NSA has been proven to use this technology on its own population, and one news report reveals that British authorities used Echelon to monitor charities operating within its borders, notably Amnesty International and Christian Aid. Insiders within the British signals intelligence headquarters were compelled to make this information public as they felt they could "no longer remain silent regarding that which [they] regard to be gross malpractice and negligence within the establishment in which [they] operate" (Wright, 1998, p. 20). If Echelon is used by other states to conduct domestic surveillance, then is it really unfathomable that Canada might be

34 For comprehensive accounts of the Echelon system see Jack O'Neill's *Echelon: Somebody's Listening* (2005), *The Ties that Bind* (1985) by Jeffrey T. Richelson and Desmond Ball or refer to James Bamford's *The Puzzle Palace* (1982).

doing the same? Even though the CSE is legally mandated to collect foreign signals intelligence and is "prohibited by law from directing its activities at Canadians anywhere or at anyone in Canada" (Canada, 2007), Canadian laws related to surveillance have become progressively more far-reaching, and recently proposed legislation seeks to further extend surveillance activities[35]. This is a kind of domestic surveillance though it may not be orchestrated by the CSE itself. The reach of government is becoming very intrusive, and it is quite amazing what types of communication and information the state is able to intercept. As Reg Whitaker describes, U.S.-developed TEMPTEST technology allows authorities "to read from a distance computer communications and even files on computer drives from the electromagnetic radiation emitted" (2000, p. 94). Technology allows for the interception of domestic communications and digital data, though the laws surrounding these activities are unclear. Given that the government itself views security as the responsibility of the state and, to this end, believes it to be the "first obligation of the state," all things (including rights) are placed after this (Canada, 2002, p. 79).

International terrorist threats are not simple and therefore many agencies and departments involved in intelligence in Canada must cooperate with other international actors. UKUSA, its Echelon program as well as other programs and agreements, all seek an international solution for a transnational problem[36]; however, finding an international solution can be very complicated as each state has its own objectives and priorities, and these might not always mesh so neatly. The close relationship of Canada and the United States is therefore worrisome for Maureen Webb, who takes the United States' statement "our data should be your data" to mean "your data should be *our* data" (2007, p. 144, emphasis added).

Collective arrangements, particularly with defence has been a traditional security policy for

35 The recently proposed legislation is certainly related to Canada's signature on the Council or Europe's Convention on Cyber Crime which requires signatories to establish laws enabling "authorities to collect and record traffic data and content data on the Internet—both with and without the cooperation of service providers" (Whitaker, 2003, p. 257).
36 There are reports that Canada is also involved in a separate international agreement with Australia, Germany, the United States, and the United Kingdom since February 2003 (Webb, 2007, p. 142)

Canada, allowing it to "avoid the massive costs of wars...[with the added] benefit of containing conflict as far away from Canadian territory as possible" (Canada, 2002, p. 89). This approach has found its expression in Canada's membership within the United Nations, the North Atlantic Treaty Organization and the North American Aerospace Defence Command and is reaffirmed in more recent counterterrorism policies and agreements. Cooperation and sharing is important for collective defence and under UKUSA's reciprocity agreement Canada grants "partner SIGINT organizations virtually automatic access to Canadian interception modalities—local in country, external, HF long distance, or satellite downlinked—without Canada necessarily being aware of their targets" (Rudner, 2001, p. 112). The reliability of professionals' claims that datamining and communications surveillance will make states more secure is put in to question by overwhelming evidence to the contrary. Furthermore, Canadian government pronouncements that it does not conduct domestic surveillance to begin with are hardly reassuring. After all, Canadian reliance on the United States is rather substantial and "dependence on its American intelligence connection will likely grow even more acute apropos some of the most technically sophisticated technologies" (Rudner, 2002). Independent contributions made by the CSE are denied by British and American counterterrorism officials. Even where Canada was able to provide advance knowledge of the "London fertilizer bomb plot and the alleged Brooklyn Bridge blow-torch plot," both agencies had prior knowledge from other sources and from other methods of intelligence collection (Webb, 2007, p. 49). Canadian intelligence has little to offer to the international community, and "in the past the agency routinely broke Canadian laws in the collection of intelligence involving Canadians" (Moon, 1991, p. A1). With limited terms of trade and a demonstrated will to operate outside the laws, pressure from the United States to be more aggressive in implementing counterterrorism policies[37] and proven civil rights infractions is it so irrational to consider that Canada

37 The United States was quick to recognize the faults of Canadian intelligence. Or at least it was quick to point out the *perceived* deficiencies. For instance, many American citizens believe that the 9/11 attacks were made possible because Canadian border control is too lenient; however, "none of the nineteen hijackers who masterminded the September 11 attacks had entered from Canada [all were] issued visas by the United States" (Andreas, 2003, p. 92). Many Americans

might engage in illegal domestic communications interceptions, particularly where technology and the law are the only limitations on these actions? The government still continues to emphasize that the legal safeguards within the *Anti-Terrorism Act* sufficiently protect citizens; however, this is not the case.

Many restrictions and "safeguards" have actually been rejected by legal scholars reviewing the legislation. According to Thomas Gabor, the in-house legal team from the Department of Justice, a review process by a new CSE Commissioner as well as periodic audits conducted by the Auditor General, Privacy Commissioner or Information Commissioner are not sufficient as they are all "too narrowly focused on reviewing the legality of CSE operations and so do not approach the scope of the review body for CSIS, the Security Intelligence Review Committee" (2004, s. 37). Simply, there are many situations and circumstances in which illegal acts may be made legally permissible if one appeals to a specific authority for related permissions; however, the *Anti-terrorism Act* also promotes discretion at many levels of law enforcement and security and intelligence work. The language contained in legislation now allows for the CSE to "monitor foreign communications, wherever they may go, including points of contact in Canada, subject to certain statutory requirements," but these statutory requirements are inadequate (Rudner, 2007, p. 475)[38]. The CSE is also mandated to assist other federal security or law enforcement agencies, but here the CSE's involvement is "predicated upon the legal precepts applicable to those agencies' activities," which may allow the CSE to target Canadian citizens. The RCMP and CSIS, for example, are allowed to investigate Canadian citizens and intercept communications, subject to certain conditions that may not be as prohibitive as those applied to the CSE's independent investigations (Rudner, 2007, p. 476).

continue to view Canada as a "haven for terrorists who exploit the country's liberal refugee and immigration system" (Andreas, 2003, p. 92).

38 The *Anti-terrorism Act* now allows for ministerial authorizations where the CSE may "target foreign entities physically located outside the country which may engage in communications to or from Canada for the sole purpose of obtaining foreign intelligence" where foreign intelligence is defined as "relating to the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they affect international affairs, defence or security" (Rudner, 2007, p. 475). The language is rather all-encompassing, and may allow the government to intercept the communications of Canadian citizens with foreign persons or groups. Once this happens, it is unclear that the government may not use these communications against its own citizens, particularly where "discretion" is stressed in times of "emergency".

Because there is a greater emphasis on intelligence, and ICT limits this, the technology that enables interception is an important part of counterterrorism activities. In addition, "information is being moved globally in incredible volumes, at unprecedented speeds and on complex networks," and the technologies that allow this are continually changing (Canada, 2008, p. 12). Information and communications that will thwart terrorist efforts or assist in efforts to minimize damage is therefore of great interest to states. In the United States, the conduction of surveillance activities on its own population is highly visible, though the same cannot be said of Canada. Even so, it is important to understand the technology behind these activities so that one can appreciate such activities are technically possible in Canada, even where legally they are not. The extent of surveillance activities in the United States is quite astounding, and it would be naïve not to consider the possibility that similar activities (though possibly on a smaller scale) could be taking place in Canada as well.

In December 2005, the New York Times reported that the NSA was spying on U.S. Citizens within its borders, which is in violation of the *Foreign Intelligence Surveillance Act.* The NSA is allowed to "spy on foreign communications without warrants but warrantless domestic spying is still officially illegal in the United States" (Webb, 2007, p. 47-8). Where the law does not allow such activities, there have been special permissions and legal changes made. On 7 April 2006 the United States' Attorney General Alberto Gonzales made a statement that suggested the President was authorized to order the NSA to conduct domestic surveillance without warrants: just over a month later, it was revealed that the NSA's database was "the largest database ever assembled in the world" (Webb, 2007, pp. 55-6).

It is "widely acknowledged that intelligence cooperation and information sharing are indispensable for effectively combating a global terrorist threat" (Rudner, 2007, p. 480); however, the state's ability to collect and use information against its own citizens appears to be excessive. Although

ICT can make it easier to intercept communications and other information of interest, at the same time terrorists are using ICT to make counterintelligence activities more difficult. The state is not the only entity involved in surveillance, which makes intelligence collection easier; however, this also complicates further the legal precept of having a reasonable expectation of privacy. All kinds of surveillance efforts are focused on defining and categorizing individuals, whether this relates to an individual's background or status, preferences or intent. In terms of state surveillance it is mainly concerned with the latter, directed by the question: "is this person likely to commit a terrorist act or provide material or political support to the cause?"

The ability to engage in surveillance of domestic communications is made easy as almost all of our communications are digital. Though digital transmissions are easier and cheaper to intercept than physical interception (through the use of a wiretap, for instance), the amount of data to be assessed can be overwhelming. Consider some recent statistics: it is estimated that "each human generated an average of 250MB of digital data [in 1999], but 800MB in 2002," which amounts to about 5 million terabytes per annum overall (Müller, 2009, p. 532). With the growth in communications technology, the amount of data that is exchanged, shared and created will increase steadily, particularly with more widespread adoption of new information and communication technologies and the decreasing cost of relevant services.

Though not all of these data are communications-based, there are other figures that communicate risk or lack thereof. Due to the high volume of data traffic specific to communications, it makes more sense to take *accumulative* risk factors into consideration. Something as simple as further analysis of suspicious financial activities could indicate the possibility that an individual is providing material support to a terrorist or terrorist organization. Also reviewing an individual's travel history and associative behaviour could give further indication that this person deserves to be prioritized in terms of intercepting communications. In Canada there are concerns that these surveillance activities will be

hindered where the "relatively unrestricted public availability of sophisticated encryption/cryptology equipment and programs threatens to neuter an essential source of intelligence about the activities of spies, terrorists and criminals" (Canada, 2002, pp. 35-36). The state is not the only interested party collecting information, and this assists in creating more comprehensive virtual profiles for the purpose of risk analysis and decision making in counterterrorist policies and activities.

There have been many studies on surveillance in the workplace, for instance, where most research relates to efficiency and expediency and the ethics concerning surveillance and employee monitoring (see for example, Botan, 1996; Urgin, Peatson & Odom, 2008) or network interfaces and employee productivity (Garrett & Danziger, 2007). Surveillance in the workplace acts as a substitute for supervision. Time wasting activities are now minimal as things such as internal instant messaging obviate the need for workers to use an open system such as ICQ, MSN Messenger or AIM. Similarly, external websites deemed unnecessary to access at work are blocked, though contemporary scholars continue to debate whether "cyberslacking" affects productivity (Garrett & Danziger, 2008, p. 287).

In addition to surveillance at the workplace, information gathered on customers by corporations has grown exponentially in the past few decades and has become a sophisticated and calculated venture. Advertising and market research were the initial attempts of communicating with consumers but these have since expanded to the point where consumer information databases are considered to be one of the most valuable assets to a company (Karas, 2002, p. 36). Through the use of consumer information gathering, strategies of procuring investigative reports, selling or sharing information with other companies, pursuing and compiling information from public databases and using consumption histories for households or other units of measurement, companies are becoming well-versed in the art of "psychographics"[39] (Karas, 2002). The analysis of aggregate information is useful for precision

39 Psychographics is the reproduction of psychological profiles through the collection of data related to "opinions, attitudes, beliefs and lifestyles" and is used for the purpose of direct marketing at more specific target groups than those based on more traditional demographic measures such as age, social status or ethnicity (Karas, 2002, p. 40).

marketing and the size of corporate databases are simply astonishing: for example, in 2004, Wal-Mart had close to 460 terabytes of data (Hays, 2004). Though a small portion of this database information relates to inventory data, most of the information held by Wal-Mart is specific to consumer behaviour. In other words, customers communicate their wants/needs involuntarily thereby unknowingly contribute to the database through the tracking of purchases (Hays, 2004). More recent reports place Wal-Mart's data holdings at 600 terabytes in 2006-7 (Babcock, 2006; Foley, 2007), and industry veteran Curt Monash estimates that in 2008 Wal-Mart's database had grown to 2.5 petabytes (Monash, 2008). Only approximate figures are available, but experts predict that companies' datawarehouses will double every year (or 18 months) and that the biggest companies (referred to as Teradata's "Petabyte Power Players") are likely to triple in size every three years (Monash, 2008). The collection of information is an exercise of power, and the use of that power through knowledge is an attempt at gaining control, influencing, and benefiting those corporations that maintain records and analyze this information for their own specific purposes. Foucault's assertion that power is not only exercised by the state is correct: power is exerted—or discipline enforced—by multitudinous non-state actors. Companies may also be asked to provide these databases to government agents along with specific employee records held[40]. Furthermore, the amount of information available to government through its own interception is incredible, and all of this is made possible by technology.

From online banking, to real-time gaming, personal communications, social networking and various other activities, Canadian citizens use communication and information technologies to a great degree in everyday life. Personal information, transactions, communications and other digital "footprints"left by an individual are potentially accessible to security and intelligence officials and may

40 In the United States the government is able to access companies' employee records as well as other information holdings on their consumers under section 215 of the *PATRIOT Act*. Though Canadian legislation is not as specific on the ability of government agencies to obtain similar information from Canadian companies, there remains concern that information can be obtained by the U.S. government on a significant proportion of the Canadian population "where most credit card companies are American-based and the federal and provincial governments have contracted out medical plans, parts of the national census, and the student loan program to American companies" (Webb, 2007, p. 117).

be used to construct virtual profiles, as discussed earlier. The amount of information that can be collected on a single individual is astounding. A Statistics Canada report on Internet use from 12 June 2007 to 12 June 2008 discloses that nearly three-quarters (19.2 million) of Canadians aged 16 and older accessed the Internet for personal use, and 68% of this group accessed the Internet on a daily basis (2008). Though scholars point out that there is a digital divide—those with higher education and income, and those living in urban areas are more likely to use the Internet—statistics indicate that this gap is closing and, furthermore, online activities are becoming more diverse as users branch beyond e-mail and browsing to include online travel booking, banking, sales and shopping, blogging and participating in online communities as well as accessing various media (Statistics Canada, 2008).

More sophisticated communications technologies are gaining in popularity in Canada; however, users are less concerned about privacy or security issues than they are about the convenience and price of these technologies and appending services. Users are asked to "make a choice between privacy and convenience," but are too often not equipped to make an informed and responsible decision[41] (Fernback & Papacharissi, 2007, p. 724). As the cost of technology dramatically decreases, often these operating systems for these technologies become more user-friendly; therefore, more established forms of communication technology are relatively easy to use and reasonably affordable, leading to near-universal adoption. Communications technology is continually being developed: for example, Statistics Canada has identified that cellular phones are quickly gaining in popularity as the primary telephone service. In a survey conducted in 2006, people were asked whether they had a cell phone. At that time, there were 16.6 million mobile service subscribers (52.5% of the population) (McDonald,

41 To illustrate the ignorance of users in making a decision to privilege either convenience or privacy Papachissi and Fernback use the example of MSN's use of "cookies" and how these allow users to "fully experience the interactive features of the MSN services" by monitoring and saving your online activities. They emphasize that "the discourse about cookies is framed in terms of convenience to the user...[and] whatever privacy concerns might be raised by the notion that monitoring devices are placed on the user's computer are mollified discursively by the emphasis on convenience". Furthermore, users must review a detailed explanation of cookies on the MSN Personal Information Center's webpages, which adds to the nod toward convenience. After all, why would a user waste time reviewing the privacy policies of something that will benefit them? (Fernback & Papacharissi, 2007, p. 724).

2006, p. 12; Statistics Canada, 2006). These figures suggest that cell phones may become the primary telephone service in the next few years. Compared with 2006 statistics on cellular phone usage Crow, Sawchuck and Smith note that "at the end of March 2008, Canadian wireless phone subscribers numbered 20.1 million, representing a national wireless adoption rate of 62%" (2008, p. 351). The market for digital telephony is immense, and the adoption of new communications technologies (such as the increasing popularity of cellular phones as opposed to traditional land lines) has made this a very profitable sector[42]. Industry Canada's Office of Consumer Affairs described cellular use as "ubiquitous" and, as Warner pointed out in 2005, "the cellphone has indirectly affected many other aspects of daily life" alongside "redefining when and how people can communicate" (Industry Canada, 2006, p. 4). The various new developments in technology provide more opportunities for surveillance, if such technology exists or may be developed for that specific purpose. Wire-tapping, or one of the more traditional forms of intercepting communications, no longer requires a physical interception: surveillance is now wireless, miniaturized, and therefore more discrete.

It is also nearly impossible to avoid using communications technology as it is an essential and important aspect of everyday living and greatly influences civic and political associations. Professor of Law Katherine Strandburg describes the transformative features of digital technology and new communication technologies:

> Nearly every organization now uses email, websites and cellular phones as primary means of communications with members. Meanwhile, more and more political and civic work in society is performed not by traditionally organized, relatively long-lived, face-to-face associations with well-defined members, leaders, policies, and goals, but by decentralized, often transient networks of individuals associating only or primarily electronically and with policies and goals defined synergistically with the formation of the emergent association itself. (Strandburg, 2008, p. 745).

Communication technologies are more important in defining both personal and professional

42 One report notes that the Q4 profits of 2006 totalled more than $1 billion and this profit from the quarter represented a 64% increase from the previous year, with most of this growth coming from data usage (Use of mobile phones almost level with landline- Canada Statistics, n.d.).

relationships and therefore the effects of these technologies and the potential abuses deserve to be considered. As Saskia Sassan remarks, too often new communication technologies are understood in an overly technological way, which does not acknowledge the sociological impacts and spectrum of responses under various social orders (2002, p. 365). She identifies that digital networks have three defining properties: decentralized access, simultaneity, and interconnectivity (2002, p. 366). The increased use of digital networks makes the interconnectivity feature problematic: in most cases in order to connect with others through social networks or to enjoy online services one must provide personal information which is then stored, databased and sometimes shared or sold to third parties.

For example, the Internet allows for the "accumulation and sharing of digitized personal data on networks," and it is for this reason critics argue that the use of information and communication technologies undermines privacy rights, particularly given the perceived need for security and surveillance (Orgura, 2006, p. 278). Karas (2002) warns that the ability for remote surveillance (in both a spatial and temporal sense) has severe implications as "information gathering has effects on behaviour whether or not the data is ever analyzed" (p. 46). New technologies allow for massive amounts of data to be collected on one person and to be compiled into an elaborate dossier. These allegedly provide a representation of an individual from which intelligence analysts are able to reproduce networks of associations, and even reconstruct or predict an individual's thoughts, thereby deducing his or her intentions and motives. Due to the utility of communications intelligence, it is viewed by some as an indispensable tool in combating terrorism. In fact, communications intelligence and the collection of personal data now has a premium on it to the extent that personal information has turned into a "tradeable commodity in capitalist societies"[43](Fernback & Papacharissi, 2003, p. 1).

43 There are many examples of corporations trading and selling personal information for profit and there are some major companies willing to do business with government. For example, "ChoicePoint alone has about 17 billion public records, 250 TB of data...[and] it acquires data worldwide" (Müller, 2009, p. 535). O'Harrow notes that the company gave the U.S. government information on all South-American people and other major companies also have sharing agreements (quoted in Müller, 2009, p. 535). Interestingly enough Robert David Steel predicted that governments would approach commercial entities to build their own databases (1995).

The convergence and widespread use of ICT make communications intelligence appear fruitful, but there are too many problems associated with databasing and extreme domestic surveillance, even before one considers the illegality and immorality of such a project undertaken by government. The process of commodifying, analyzing and judging personal information, activities and associations is dehumanizing as it involves ignoring the specific identity of people and imposing a new (artificial) one based on the data collected. The most problematic area of surveillance is the use of datamining, but this remains a pervasive state activity as it allows them to pre-screen communications and information collected and to deal with massive amounts of data.

Though machines may do the initial datamining and flagging of suspicious activities and individuals, it does not end there. Security and intelligence officials must also look at the data collected by various programs and make conscious choices about how these data should be used. For example, do the data warrant the freezing the financial accounts of an individual or should this person be brought in for detention and questioning? Müller (2009) warns about confusing the right to privacy with privacy as a value. He borrows from Alan F. Westin's classic definition and takes privacy to be "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others" (2009, p. 539). From this definition along with American jurisprudence records, he concludes that datamining is a violation of privacy as artificial intelligence programs are able to make unforeseen connections through shared databases (2009, p. 540). Few argue against the fact that "current computer systems do not understand...when they find a particular pattern, they cannot know what this pattern means," and therefore datamining requires further human analysis (Müller, 2009, p. 541). Once human analysis is introduced, the process is no longer impersonal and automated and thus satisfies the parameters of a breach of privacy. Put simply, surveillance of communications through an automated system is not useful in itself though, technically, it could be argued that this does not constitute a breach of privacy; however, because the automated and

computerized systems can only identify but not understand or interpret as a human analyst can, any type of datamining surveillance, including communications surveillance, cannot be useful without violating the privacy rights of citizens (2009, p. 541)

The use of technology is instrumental in communications intelligence and other surveillance activities monitoring that is involved in the acts of risk assessment and profiling; however, it is not complete and is not reliable. As computers cannot fully understand human dynamics (psychological processes, or emotional markers such as irony or sarcasm, for instance), they are not able to "distinguish the guilty from the suspicious," which is one of the primary causes behind false positives[44](Müller, 2009, p. 542). Automated analysis and subsequent classification of individuals, along with the high number of false positives, are the reasons why in 2003 the founder and director of the Center for Advanced Studies in Science and Technology Policy, Kim Taipale, warned against using datamining techniques and being overly confident in the use of artificial intelligence as there is much room for error, therefore, "the guiding principle...should be that data mining not be used to automatically trigger law enforcement consequences" (Müller, 2009, p. 542).

Despite these limitations intelligence is a complex process that involves multiple interpretations, reassessments by others, and this work is put in to action. Most important importantly, at every step in this cycle, there is the potential for human error[45]. Although the human factor—the interpretive process in the intelligence cycle—can cause intelligence failure, it is also important as part of a checks and

44 In the United States even state officials have been caught in the web of suspicion where Senator Edward M. Kennedy and U.S. Representative John Lewis were named on the no-fly list and "federal officials make it very difficult to correct the list, thus tormenting citizens who are guilty of nothing more than having a name resembling a name suspected sometime by some government official" (Bovard, 2006). Similar events and legal records are not available in reference to the Canadian situation; however even though "Canadian jurisprudence is more protective of privacy" than other states, there are still concerns even by Canada's Privacy Commissioner that the "transborder flows of personal information...might transgress privacy rights" recommends that Canadian citizens do not uncritically accept the CSE Commissioner's assertions that the interception and analysis of a "private communication" in Canada is "circumscribed by an appropriate legal framework" (Rudner, 2007, pp. 480-1).

45 Sergeant Faragone and Captain Rivard of the Canadian Forces believe that the defining factor of intelligence is that it is use driven (2007, p. 84). Though intelligence involves analyzing various data sets, *good* intelligence "is that product that provides a far better understanding of knowledge of any issue" based on identified needs and available solutions (2007, p. 84).

balance system, particularly in communications intelligence where surveillance activities are dependent on technology and artificial intelligence is only appropriate for preliminary analyses. With communication intelligence, the use of artificial intelligence is necessary but also troublesome. It is necessary because there is too much traffic for analysts to handle on their own and, from what is known about domestic interception of communications in the United States, it seems that governments that employ this method of surveillance are more interested in blanket surveillance than in the specific surveillance of individual suspects.

Governments are already also involved in collecting mass amounts of information on its own citizens. Communications are important to governments for several reasons, and Canada has attempted to revolutionize its communications with its citizens by becoming a model country in the information age. To this end, the Canadian government has initiated an aggressive effort towards increased e-government, making it easier to create virtual profiles of Canadian citizens. The rationale behind this movement is that technology "set[s] the pace of social progress," and the availability of many government services will invite Canadian citizens to use the Internet to interface with both government and industry. To effect greater use of the Internet, the Canadian government is encouraging the private sector to provide more online content and services as a government-led effort toward greater digitization in Canada (Fraser, 2007, p. 205). What greater digitization means is that these databases of information are more readily available and accessible than is either a paper-based or a less centralized system of accessing government services.

Historically, communications between government and its public have centred around the provision of services and division of goods. Here communications were based on categorization for the purpose of identifying entitlement and debts of families or individuals. Over time, this process of categorization has accelerated and expanded. Benedict Anderson observed that the census categories have become most defined by racial background rather than by religious affiliation. Though his

observation applies primarily to the colonial state, what is clear, and appears to be nearly universal, is that citizens cannot be imagined as fractions, but are given an imaginary and "fixed" classification (2006, pp.164-65). In relation to the identities of "terrorist," "Arab," and "Muslim," we see a resurgence of religious identification but this is conflated with the other two terms so that "both Arabs and Muslims have become the target of popular suspicion," which manifests itself with the "'Arabification' of Muslims and the 'Muslimification' of Arabs" (Badhi, 2003, p. 296). The census maps populations or rather, it *marks* people within a population. Whereas identification categories in the census were mainly constructed to enumerate taxes and levy lists, processes of identification are now becoming more political and focused on identifying "at risk" populations in the global War on Terror.

Governments have had many of their own initiatives to collect information; however, this does not encompass all details of interest about a person, and therefore government databases are supplemented with corporate data sets to provide more informative risk assessments. The sheer volume of data and the vast dispersion of this information have meant that third party intermediaries obtain, store and use personal information. Not only has the government compelled companies to share the data collected so the government is able to compile mega databases but "there are continuing efforts to require Internet service providers 'ISPs' to maintain records of their customers' travels over the Internet" and, in a grand gesture of support, for example, the European Union adopted "a controversial Directive mandating telecommunications traffic data retention" (Strandburg, 2008, p. 742). Canada seems to be leaning towards more aggressive and public surveillance, especially for policing. On 18 June 2009, new legislation was tabled that will force Canadian ISPs to track the Internet traffic and to "allow law enforcement to tap into their systems to obtain information about users and their digital

conversations"[46] (Tibbetts, 2009). The proposed legislation will also allow police to use telephones as a tracking device, and essentially allows for eavesdropping without warrant or other forms of judicial authorization (Wilson, 2009).

The negation of space and time is a reflection of digital networks property of simultaneity but this is another issue Sassen identifies as the non-differentiation of the digital and real. Though the simultaneous and real-time interactive communications allow for the limits of space and time to be bridged they are not indeed dissolved entirely. She argues that through digitization the real and physical are "liquified" and de-materialized through a process of hypermobility[47] (2002, p. 369). Sassen also furthers that "the complex imbrication between the digital (as well as the global) and the non-digital brings with it a destabilizing of older hierarchies of scale and often dramatic re-scalings" (2002, p. 371). What this means for domestic surveillance and analysis is that the digital may not reflect its physical and real referent and these digital analyses can have profound, disturbing and—at times—criminal consequences[48]. Communication and information technologies are able to bridge time

46 The legislative changes proposed are in Bill C-46 and Bill C-47. There are many concerns particularly with the possibility of criminalizing an individual's ability to establish his or her own ISP, essentially making it illegal for individuals to allow proxy access through programs such as PsiPhon, a program developed to allow unrestricted Internet access to countries like Iran and China, where free access is hindered by the state (Wilson, 2009). The proposed bills can be accessed here:

Bill C-46, *An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act* (http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4008179&Language=e&Mode=1) and,

Bill C-47, *An Act regulating telecommunications facilities to support investigations* (http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4007628&Language=e&Mode=1)

47 Sassen explains that hypermobilitzation is a process whereby one is able to conceptualize something that is immobile or fixed is able to become de-materialized, therefore becoming mobile. She offers one example: capital mobility, as electronic financial markets are an enormous global venture. Though these transactions are digital they cannot be removed from the "larger social, cultural, subjective, economic, imaginary structurations of lived experience and the systems" in which it operates. In brief, electronic financial transactions are not wholly digital and one must remember the material influences: "much of the material is inflected by the digital insofar as it is a function of financial markets. And much of the digital composition of financial markets is inflected by the agendas that drive global finance" (Sassen, 2002, p. 368-9).

48 Rudner suggests that intelligence cooperation and intelligence sharing "can have profound implications for foreign policy, civil society and human rights" (2002). Webb also argues that governments should learn from the tragic experience of Maher Arar as it provides a "good example of how indiscriminately governments are sharing information and what personal and social consequences" intelligence sharing may have (2007, p. 160). The issue is identity and categorization into two groups: those who should be protected by the norms and legal apparatus of the state and those who are not. Lyon forwards that "compiling ordinary lists of persons constitutes one of the simplest kinds of surveillance, but...if that list groups together all those of who are thought of as 'citizens' or a particular nation-state" these have social consequences (2002, p. 2).

and space but when reassembled it cannot reconstruct them perfectly. Likewise, virtual profiles cannot be reconstructed perfectly; however, categorization is a natural process. "Without categorization the complexity of the human social world might not be manageable at all" because this satisfies the universal desire to achieve cognitive parsimony (Jenkins, 2000, p. 8). It is a natural process that—when emphasized—leads to extremism. Canada has a history of eliminating threats to the state, even if this has required trumping the rights of citizens to express political opinions though legal dissent[49]. Not only do these databases violate the privacy and civil rights of citizens, the mass monitoring of activities, including personal communications, can cause severe and sustained psychological repercussions for individuals and can disrupt normal processes of socialization. Furthermore, Canada's Privacy Commissioner Jennifer Stoddart has made a few cautionary statements on behalf of citizens noting that "governments appear to believe that the key to national security and public safety is collection, sorting and analyzing mountains of personal data—without demonstrating the effectiveness of doing so" (Butler, 2009). This is a very good question to put forth to government: are surveillance and datamining the key to national security? Everything remains within a "shroud of secrecy," and it is distressing that citizens do not know what the government is doing to advance national security (Rudner, 2001, p. 97). The government has compiled information on its own citizens, but as far as the illegal interception of domestic communications goes, the questions still remain. Even government officials have noted that this [post 9/11 environment] is now a "seamless world in which traditional civil liberties have been suspended to some extent" (Butler, 2009). As this is going on behind closed

49 In Whitaker's 2003 article, *Keeping up with the neighbours? Canadian responses to 9/11 in historical context*, he documents that later government inquiries have uprooted these indecencies. For example, during the Cold War he explains the government purged many civil servants solely based on suspicion and later, during the October Crisis, the government targeted political dissenters who seemed sympathetic to separatist goals. In the 1970s the interests of the NSA weighed heavily on Canadian signals intelligence and was therefore "acting at the behest of NSA" in one capacity or another (Rudner, 2001, p. 106). The government has many agents with which to conduct surveillance and to exert control over specific portions of the population and in the late 1970s it was discovered that the Royal Canadian Mounted Police had been used for one such exercise. The McDonald Commission of Inquiry reported that the RCMP had collected information on individuals and organizations. The scope of this exercise was completely surprising for Canadian citizens as the proportion of the Canadian population "watched by the secret police..would have done credit to some less savoury regimes abroad (Whitaker, 2003, p. 248).

doors it may be many years before the truth comes out. This has its place in Canadian history and therefore citizens should pre-emptively demand answers from the government[50].

The Debate on Surveillance and Privacy in Canada

When one becomes aware of the high probability of invasion of privacy and the effect on social, political and criminal arenas, one cannot help but become alarmed. For the director of the University of Ottawa's Canadian Internet Policy and Public Interest Clinic, David Fewer, the proposed legislation "looks like a grab, under the name of modernization, just a grab at our civil liberties" (Government looks to increase web surveillance, 2009). And it seems like this is a grab that no one seems to notice. As the *Ottawa Citizen* reports, "so far, there's been little public outcry about the explosive growth in private and public monitoring...because many of us are simply unaware of the extent of contemporary surveillance" (Butler, 2009). This is because the government is not really talking about it.

There has not been a significant amount of debate on the *Anti-terrorism Act* although it has, on numerous accounts, been called an "omnibus piece of legislation" and contains major enactments or amendments to a number of federal statutes (Gabor, 2004; Rudner, 2007; Shore, 2006). Changes to the *National Defence Act* resulting from the *Anti-terrorism Act* are responsible for providing the CSE with its formal mandate. It reads:

> The Communications Security Establishment Canada is Canada's national cryptologic agency. As outlined in Part v.1 of the *National Defence Act,* the mandate of CSEC is:
> a. to acquire and use information form the global information infrastructure for the purpose of providing foreign intelligence, in accordance with the Government of Canada intelligence priorities;
> b. to provide advice, guidance and services to help ensure the protection of electronic information and information infrastructures of importance to the Government of Canada; and
> c. to provide technical and operational assistance to federal law enforcement and security

50 The examples provided above (see footnote 19) show that the truth is not always known at the time in which these activities are taking place. Furthermore, much of Canadian signals activities are dependent on the United States as evidence shows the NSA urged Canada to monitor Soviet countries during the Cold War with interception equipment placed within Canadian embassies abroad. All of the data collected was then sent to the NSA for analysis and to be deciphered, as Canadian signals were unable to do this independently (Rudner, 2001, p. 107).

agencies in the performance of their lawful duties (Canada, 2007).

There are specific situations in which the illegal interception of domestic communications is made permissible and, as noted earlier, disclosure of this fact is not always required or in cases where it is, the government may disregard the fact that disclosure is mandated by law. Government has on several instances demonstrated an ability to operate outside of the law, but it is rarely confirmed or disproved until many years after the fact. Though many argue that "Canada's Communications Security Establishment has undergone a far-reaching transformation in conjunction with the expanded role in the 'global war on terror,'" it is still not known whether the CSE is engaged in illegal activities directed towards its own citizens (Rudner, 2007, p. 473).

Law enforcement must follow certain protocol and obtain judicial authorization to intercept electronic communications in criminal proceedings, as laid out in Part VI of the *Criminal Code* but even in criminal law where the laws have been tested, challenged, and established for a much longer time, it appears that authorizations are being granted without any substantial criticism or consideration (Public Safety Canada, 2004). The annual reports on the use of electronic surveillance contain all the statistics concerning electronic surveillance and these data support the claim that authorization is too easily granted[51]. There are some restrictions[52] but these can be disregarded in emergency situations, as stipulated in section 188 of the *Criminal Code*.

What is most surprising is that Canadian media have not been more curious about the government's hesitance to say much about domestic surveillance initiatives since 9/11 and, for the most

51 The terms and conditions for authorization and renewal of warrants are too easily met, and no application for electronic surveillance by peace officers has been refused for the period of 1999-2003 (Public Safety and Emergency Preparedness Canada, 2003, p. 6). The period of 2003-2007 was the same: no applications were denied (Public Safety Canada, 2007, p. 6).

52 Peace officers are not able to intercept private communications of Canadian citizens unless the offence is included in section 183 of the *Criminal Code*. Some of these offences include "facilitating terrorist activity, weapons trafficking, child pornography, child abductions, drug trafficking, and organized crime" and the like but for interceptions related to terrorism there are additional requirements (Public Safety, 2004, p. 3). In order for authorization to be granted in cases of suspected terrorist acts the judge must be "satisfied that other investigative procedures have tried and failed, that other investigative procedures are unlikely to succeed or that there is an urgency such that other investigative procedures are impractical" (Public Safety Canada, 2004, p. 3).

part, legislation governing domestic surveillance has been overlooked. Parts of the anti-terrorism legislation related to signals intelligence slipped under the radar of the Canadian public as media outlets focused on specific issues. The new legislation was controversial and drew concern from civil libertarians though few others took note of the significance of the proposed changes. In the media there were mentions about the most egregious aspects—preventative arrests and investigative hearings—but too few were aware about the changes to communications intelligence, including the first explicit public mandate from government for the Communications Security Establishment and the accompanying permissions to allow the expansion of electronic and communications surveillance (Whitaker, 2003, p. 261; Shore, 2006, p. 458). This is possibly due to the time constraint of forming debate and analyzing the legislation itself: the Bill was introduced on 15 October 2001 and was signed into law on 18 December 2001, a mere 65 days after its introduction. Canadian citizens were simply excluded from the debate. They knew little about the consequences of this piece of legislation before it was passed, and soon the legislation and it soon faded into obscurity in the public's mind [53](Millward Brown Goldfarb, 2004). The focus group study conducted by Millward Brown Goldfarb (MBG) on behalf of the Research and Statistics Division of the Justice Department in 2004 discovered that "[a]wareness of the anti-terrorism legislation was generally low, with about half of the participants in each group saying, when prompted, that they were aware of some of the aspects of legislation' (2004, p. 2). When participants were not prompted this figure was much lower and "most participants did not remember many of the details associated with the Act and admitted that when they initially heard about it, it did not strike them as something of major importance. The general consensus was that those who were aware remembered vaguely hearing something about the Act in the fall of 2001, but that was all" (MBG, 2004, p. 16).

Even with limited knowledge about the Act, participants made some critical decisions and

53 Only a few of the participants could speak about the legislation when unaided and most admitted that they had not heard much about it since it was passed into law (MBG, 2004, p. 18).

generally believed that any risks associated with this legislation were "acceptable in light of the protection the Act affords to the country and its citizens, although the level of safety they felt did not change after learning about the provisions of the Act, since they did not feel unsafe to begin with" (MBG, 2004, p. 3). Although participants did mention some of the possibilities for the government to "take away basic rights [solely] on suspicion" most were ready to hand these over to government without any consideration even though they believed the legislation provided no more protection (MBG, 2004, p. 17).

The findings from the focus group divided participants into opinion categories: there were those who felt that the legislation should be stronger if it is to be effective; those who were ready to give up some of their rights for more security; those who believed that much of this legislation would not affect them and were therefore relatively indifferent or others who believed legislation was vague and were not able to form an opinion on it for lack of information; those who voiced concern that the legislation was brought forward and enacted too quickly, which could lead to discrimination and impact privacy and other rights; and still others who opposed the laws because they viewed them as American-inspired and held the view that terrorists should not be treated differently than any other criminal as the potential for abuse was a prominent concern of theirs[54] (MBG, 2004, p. 19-20). The third group was the most prevalent opinion among participants as they asked "What investigative tools? What do they mean by ensuring Canadian values are preserved? This sounds great, but how does it work? How far does it go?" (MBG, 2004, p. 20). These are questions that still remain relevant and any answers provided to date have been unsatisfactory. In 2003 the Justice Department conducted another study with a group of Canadian academics. The final report observed that not only do "outside observers have little knowledge of how frequently and to what effect the Act's investigative tools have been used" but experts such as Reg Whitaker admits that "the effect of permitting the Communications Security

54 One respondent was quite vocal about the distinctions made in the Act: "I find it aberrant to use to word *terrorism* to qualify people as though the were different from people who commit crimes" (MBG, 2004, p. 20).

Establishment to monitor some communications in Canada is unknown" (Gabor, 2004, p. 6). Due to the limited information available to those who actively seek out information on signals and communications intelligence and the potential for illegal domestic interception of communications in Canada, namely media and academics, common citizens are not able to grasp the gravity of the situation or understand the complex technical specifics and political arrangements that determine the possibility for domestic interceptions in Canada. An uninformed public, when confronted with such a scenario, is likely to conjure up images of a "Big-Brother"-type authoritarian regime that is viewed as a fictitious dystopia rather than understand it as a practical and possible anti-terrorism policy that may be enacted, if the government so chooses[55]. Though it may seem practical for the government to assume everyone as guilty in order to increase security, in a democratic society, this is not an acceptable course of action if privacy and other freedoms must be limited or relinquished.

Since 11 September 2001 the government has been very successful in dodging public accountability (Webb, 2007, p. 75). The problem remains, however, that public debate is necessary, particularly on this matter. The government has asked Canadian citizens to simply trust them; however, author Bruce Schneier (2003) argues that one should never allow the details of a security system to remain secret. He claims that in evaluating hundreds of security systems over his lengthy career he has learned that "if someone doesn't want to disclose the details of a security system, it's usually because he's embarrassed to do so. Secrecy contributes to the 'trust us and we'll make the trade-offs for you' mentality that ensures sloppy security systems. Openness demystifies; secrecy obscures" (Schneier, 2003, p. 279). The situation is critical but remains underestimated or ignored.

Aid and Wiebes note that there are specific provisions that effectively discourages this issue from public discussion[56]. In fact, in Canada the "strictures of the *Official Secrets Act* and similar

55 The public's perception of "ubiquitous official monitoring" has promoted a case for Professor of Criminal Justice William Bloss to draw parallels with the creation of an "Orwellian" state (2007).

56 Elmer and Opel argue that since 9/11 the state has transformed into a survivor society of which the privatization of debate is a defining characteristic (2006, p. 140). They argue that debate is no longer a public and democratic function as

laws...effectively bar public discussion of this subject" (Aid & Wiebes, 2001, p. 1). Statewatch, a European civil liberties research and advocacy group, has also charged that the combination of international intelligence agreements and proposed international standardizations for interceptions "sponsored by the EU and USA...presents a truly global threat over which there are no legal or democratic controls" (Wright, 1998, p. 20). The public should be more involved and educated about domestic surveillance, particularly given the government's history of rights abuses in the name of security and more recent proposed legislation that will give the government more permissions for surveillance.

Not only is this a critical juncture in Canadian communications law and policy, but the lack of interest and knowledge about the topic presents a democratic deficit in Canadian politics. The consequences of terrorism are significant and branch far beyond the previous legislation and the possibilities of being caught within a web of suspicion are great. Even if the practice of datamining is technically illegal there are many different loopholes under which this illegal activity may become permissible. The categories of those who support the War on Terror and those who oppose are quite clear, as former U.S. President Bush proclaimed, "you are either with us or against us." In such a scenario with wide-sweeping categories it is possible—if not probable—that legal dissenters will be targeted as a threat to the state. In an interview with the Ottawa Citizen earlier this year, Professor of Criminology and Sociology Kevin Haggerty admitted that "there's an ability to connect all of this stuff across realms that is just a little unnerving," but also he also maintained that even in proffering his warnings about the consequences of monitoring data and communications, it is difficult to convey to the public the importance of these unnerving aspects of surveillance without sounding alarmist (Butler, 2009). As this is going on behind closed doors it may be many years before the truth comes out. This

---

the decision-making responsibility has transferred to intelligence and security experts and officials, often without the backing and support of the elected government. This is especially true where the judiciary is meant to balance against the executive and where new legislation has yet to be challenged in the courts.

has its place in Canadian history and therefore citizens should pre-emptively demand answers from the government[57].

Civil liberties have been tempered in certain cases where a state of emergency is declared or under other circumstances that are deemed appropriate; however, September 11th and the panic and suspicion garnered by these attacks has nothing to do with a dramatic change—in that terrorism is not a new tactic—but governments' reactions to this event are unprecedented and disproportionate. It is this supposed state of emergency that provides the rationale behind rights infractions even though governments are now trying to legislate this and make it legal, permanently placing unnecessary limits on citizens' rights[58]. The problem is that this state of emergency will no longer have spatial or temporal limits once it is signed into law and "emergency by definition is not supposed to be permanent" (Hussain, 2007, p. 738). It is a permanent state of emergency that legitimizes these infractions through the "invocation of multiple legal orders...a particular form of disciplinary rule" that constitutes not a legal blackhole but rather provides many legal loopholes under which even illegal activities may be viewed as permissible and which may only be challenged in the courts and even then become subject to the emergency powers of the executive (Hussain, 2007, p. 738-9). The steady decline of rights in favour of security should therefore be taken seriously and, given the importance of communications, the surveillance and interception of communications within Canada is an issue that must come to the fore and public debate must challenge the assumption that rights and security cannot co-exist. In fact, some believe that they cannot exist without one another. To quote Benjamin Franklin, "They who would give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety."

57 The examples provided above show that the truth is not always known at the time in which these activities are taking place. Furthermore, much of Canadian signals activities are dependent on the United States as evidence shows the NSA urged Canada to monitor Soviet countries during the Cold War with interception equipment placed within Canadian embassies abroad. All of the data collected was then sent to the NSA for analysis and to be deciphered, as Canadian signals were unable to do this independently (Rudner, 2001, p. 107).

58 Dora Kostakopoulou believes that 9/11 is the primary, if not sole reason for the development of a "strong and intrusive state" where the "categorical gap between rights based democracies and authoritarian polities" has narrowed within an "open-ended state of emergency" (2008, p. 318).

In relation to surveillance George Orwell made this comment, and it is worth quoting at length here: "it was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live—did live, from the habit that became instinct—in the assumption that every sound you made was overheard" (in Webb, 2007, p. 111). I argue that we are witnessing the beginning—albeit seemingly less perverse and intrusive than the Orwellian system—of the institution of a panoptic society where citizens are always being watched, marked and assessed within a risk society and with little debate about this new occurrence or the possible repercussions.

Governments assert engagement in counterterrorist activities is in the best interest of its citizens but history has taught us this is not always the case. Even more troubling is the fact that surveillance has become routinized, that people are becoming more accustomed to this practice, and that people tend to believe that increased surveillance directly translates to increased security. This is simply not the case: there are many ways in which surveillance actually compromises the security of society, and this can often begin with incursions on civil and political rights. Whitaker describes the similarities of the aftermath of September 11th and the crises of the Cold War and the October Crisis in Canadian history. These times of uncertainty have been used to legitimize "extraordinary state action against dissidents," which was "not only tolerated, but sanctioned by the highest authorities in the land" (2003, pp. 244-5). In his case studies of the Cold War and the Front de Libération du Québec, Whitaker was not surprised that the government favoured expediency over lawfulness but he does lament this turn of events as it has set a precedent for crisis management in Canada (2003, p. 245). Administrative methods to protect national security are used on political dissenters is tantamount to political policing, something that is entirely unacceptable in a liberal democracy such as Canada[59].

59 Honor Brabazon argues that with the *Anti-terrorism Act* a state of exception is invoked in order to make political policing acceptable. She also submits that the language of the Act is problematic as terms defined are very limited or all-encompassing and, furthermore, there is a lack of proportionality which leads her to believe that "there is an alternative purpose for the legislation" (2006, p. 2). By criminalizing political dissent governments are able to deny the legitimate aims

It is proven that communications technologies are indispensable aids to social and political movements and, therefore, the risk that domestic interception may be used to deny freedom of expression as well as freedom of assembly and association must be acknowledged. Intercepting communications, gauging intent and then naming political dissidents criminals will without a doubt affect Canadian politics and discourage citizens with legitimate political concerns from participating in democratic governance through rallies, protests and other forms of demonstration (see, for example, Brabazon, 2006; Downing, 2001; Edwards, 2001; Small, 1994). Communications technologies are important for these kinds of movements as, for example, the Internet allows for an "inexpensive and effective means of organizing" (Dimaggio, Hargittai, Neuman & Robinson, 2001, p. 319). If these avenues are compromised by the interception and trawling for evidence of political dissidence, then this may cause the collapse of a legitimate social or political movement for fear that—in a state of exception—such organizing is a criminal offence. In this case the practice of democracy will have been criminalized. Additionally, once information is gathered, it may be stored indefinitely and "retention and access to this information is not limited to terrorism offences of even activities indirectly linked to national security issues" (Ogura, 2006, p. 286). Intelligence is a very serious affair, and yet it is not taken seriously by many outside of government.

One area of the electorate that has become involved in the debate are advocacy groups; however, even this is limited. One area of interest concerns the definition of "terrorist" as many groups worry that political dissenters will be labelled as terrorists. The Canadian Centre for Policy Alternatives [CCPA], a non-profit national policy research institute, identifies the inclusion of this definition as a key provision within the Act. They are critical as the "task of trying to define terrorism is a daunting one" and efforts to provide a definition that has "enough precision to be meaningful and

---

of social movements by: 1) holding suspects in prison without charges 2) removing key activists from the movement 3) using methods of intimidation 4) or publicly labelling these activities as criminal acts—even when they are not—in order to deny future support (Brabazon, 2006, p. 7).

yet not encompass a wide array of political dissent and protect have not been successful," despite the government's assertion that political dissent is excluded within the definition as laid out in the *Anti-terrorism Act* (CCPA analysis of Bill C-36: An Act to combat terrorism [CCPA], 2001, p. 3). According to CCPA, the definition encompassed in the Act is a "generalized approach that is far reaching and unwieldy" (CCPA, 2001, p. 3). CCPA warns, "the lack of precision in the definition raises serious concerns about arbitrary and unpredictable enforcement," and these judgements unfairly impact minority groups (CCPA, 2001, p. 4). Though advocacy and research groups such as the CCPA seem to acknowledge these potential abuses, this does not extend to the greater Canadian population[60]. Some have blatantly stated that, as Caucasians with Canadian citizenship, the *Anti-terrorism Act* would not affect them personally. This kind of apathetic attitude was evident in some responses: "Look at me, I'm white, I'm Canadian and I'm not a terrorist" (MBG, 2004, p. 31). Others were confident that the provision defining terrorist acts would not affect 99.5% of the population (MBG, 2004, p. 31). Where concern was expressed, it came most often from participants from a visible minority group. The courts prove unable to find an appropriate definition for "terrorist." This inadequacy is evidenced by the 2006 challenge by an Ontario Superior Court judge who claimed the definition in the ATA violated the *Charter of Rights and Freedoms*[61] (Part of the *Anti-terrorism Act* violates Charter: Judge [Judge], 2006).

The government has provided examples of how the *Anti-terrorism Act* has been put into use[62]

60 Respondents in the Millward Brown Goldfarb focus groups were generally satisfied with the new definition; however, it must be noted that this was a limited test group (2004).

61 A CBC report covering the legal case of Mohammad Momin Khawaja, the first person to be charged under the *Anti-terrorism Act*, explains that Justice Douglas Rutherford was impelled to "sever a section in the law that defines ideological, religious or political motivations for criminal acts" as Justice Rutherford believes that motive should not something assessed in a courtroom: "motive, used as an essential element for crime, is foreign to criminal law, humanitarian law, and the law regarding crimes against humanity" (Judge, 2006).

62 As of 20 June 2008 the government made it publicly known that: "41 entities have been listed under section 83.05(1) of the *Criminal Code;* on 29 March 2004 , one individual was arrested in Ottawa and charged with participating in the activity of a terrorist group (section 83.18 of the *Criminal Code*) and facilitating a terrorist activity (s. 83.19 of the *Criminal Code;* use of explosives (s. 81(1)); the commission of offences for a terrorist group (s. 83.2); providing property for terrorist purposes (s. 83.03); and instructing another person to carry out an activity for the benefit of a terrorist group (s. 83.21); and in 2006, several suspects were charged with various terrorism related offences in the Toronto area (FAQs, 2009).

and continues to highlight the safeguards within the Act[63]; however, amendments to the *Canada Evidence Act* suppose that the government will protect information for national security reasons, as could be employed to hide the illegal domestic interception of communications, if government does engage in such activities [64](FAQs, 2009). The *Canada Evidence Act* amendments were "developed to ensure that very sensitive information, including that received from foreign services, can and will be protected" (FAQs, 2009). This is eerily similar to the situations in the October Crisis and during the Cold War where executive decisions allowed the government to target political dissenters and compile secret files on suspect persons (Whitaker, 2003; Brabazon, 2006). Recent events regarding Bill C-3, *An Act to Amend the Immigration and Refugee Protection Act (Certificate and Special Advocate) and to Make a Consequential Amendment to Another Act,* also suggest that the courts have an interest in privileging government in court proceedings[65]. The *Anti-terrorism Act* allegedly responded to the multi-dimensional character of terrorism but many of the changes brought forth by this legislation significantly alter the traditional processes of legal remedy.

Communications between democratic governments and their publics now allows the public to provide more feedback to the government through various avenues, all of which were meant to promote

---

63 The government provides assurances that the *Anti-terrorism Act* respects the rule of law and *Canadian Charter of Rights and Freedoms*. The government promotes the ATA as striking a balance between the need for security and protection of rights and freedoms. To ensure that this balance is upheld there are several safeguards included within the Act: the definition of "terrorist activities" allegedly was drafted to exclude "advocacy, protest, dissent or stoppage of work"; the Act is subject to "judicial review, appeals and judicial oversight mechanisms"; and section 145 of the Act required that a comprehensive review take place concerning the provisions and operation of the *Anti-terrorism Act* (FAQs, 2009).

64 Though it must be noted that Attorney General certificates that protect sensitive information had not been issued as of 20 June 2008 and these are "to be used only in the rarest of circumstances" and will only be issued "where there has been an order of decision demanding disclosure of sensitive information that could...compromise Canada's international relations, national defence or security" (FAQs, 2009). Along with the amendments to the *Canada Evidence Act* there were parallel amendments to the *Access to Information Act,* the *Privacy Act*, the *Personal Information Protection and Electronic Documents Act* and the *Canadian Human Rights Act* so sensitive information could not be disclosed or accessed through similar acts of Parliament (FAQs, 2009). All of these legal "safeguards" could be broadly interpreted.

65 Bill C-3, *An Act to Amend the Immigration and Refugee Protection Act (Certificate and Special Advocate) and to Make a Consequential Amendment to Another Act* attests to this. This bill was only introduced in October 2007 "after the Supreme Court of Canada ruled in February 2007 that IRPA's procedure for judicial approval or security certificated infringed the *Canadian Charter of Rights and Freedoms* and was therefore of no force or effect" (FAQs, 2009). Even though the court deemed the amended legislation illegal, the government was provided time to "clean up its act" as the court declaration was postponed for a period of one year, only to receive Royal Assent on 14 February 2008 (FAQs, 2009).

the democratic function of the state[66]. This was supposed to be paralleled by greater accountability and transparency; however, in relation to state surveillance carried out by the security and intelligence community, communication rights seem to be in jeopardy, which also draws concern for the health of democratic governance. Communication rights are related to democratic governance in two distinct ways: "one concerns the contribution of communication directly (in the sense of participation and voice); [and] the other concerns the way policies regarding communication infrastructures and systems can promote democratic ideals (CRIS, n.d., p. 1). Government provides opportunities for citizens to voice their opinions on matters, but this is limited by several factors. In the case of domestic surveillance there is too much going on in government for each citizen to be fully informed: in Canada domestic surveillance has not been given a priority standing in political discourse, receives little attention by the media as more sensationalist news tends to overshadow any reporting on the topic. In addition, scholarship on domestic surveillance of communications in Canada is made difficult in that the Communications Establishment is particularly hard to research, where even the most prolific scholar on the CSE admits it to be the "most secretive" agency in Canada (Rudner, 2002, p. 25).

Final Considerations and Recommendations

International terrorism is a real threat to Canada. Even though Canada might not be a direct target of this, the proximal nature of this country along with the integrated economy and massive flow of goods and people between Canada and the United States means that the concerns of the United States are bound to weigh heavily on Canadian policy-makers and intelligence officials. Even without these additional reasons "international terrorism figures prominently among the security concerns for Canadian foreign and security intelligence [as m]any of the world's terrorist groups have established a presence in Canada, virtually all of them relating to ethnic, religious or nationalist conflicts elsewhere

66 Universal suffrage, referendums and even town hall meetings are all functions of democracy and these all provide opportunities for citizens to take part in democratic governance.

in the world." (Rudner, 2001, p. 115). For the public, on the other hand, "Canadians do not rank national security on the public agenda" (Shore, 2006, p. 461).

As Didier Bigo explains, after 9/11 governments gave "intelligence services an incredible new role, and justified major breaches of law and democracy by arguing that these attacks were threatening the survival of their nations, that [these acts] were a different kind of undeclared war and not a criminal act" (2006, p. 51). Whether terrorism is really all that different from criminal acts has been a controversial area of debate, and will not be continued here; however, it must be realized that the distinction is unclear and is often left to the courts. The changes in legislation to define terrorism and terrorist acts clarify as much as they confuse.

New legislation is not clear. There were many changes brought with the *Anti-terrorism Act*— which have significant implications for the rights and freedoms of Canadian citizens. The practice of intelligence sharing and the structure of the Canadian intelligence community provides a smoke screen that denies fair accountability and transparency and, additionally, communications technologies allow it even where the law expressly forbids it. In terms of the *Anti-terrorist Act* that is just so: it appears to satisfy the need for accountability to the standards applied to intelligence agencies and yet on closer inspection the loopholes and potential for abuse reveal themselves quite clearly. The efforts to make the impossible possible have created an atmosphere in the United States where "the rule of law is out the window," and where the main problem lies is that the ruling elites and "the courts condone these illegal activities" (Lendman, 2007). What this means is that governments might actually target legal dissenters, and this is also a concern in Canada where much of the new legislation has yet to be tested or challenged in court. For example, in Canada the Research and Statistics Division of the Department of Justice undertook a study of focus groups in 2003 and 2004 and noted that participants were wary about the definition of "terrorist" within the *Anti-terrorism Act* as this is "dependent on the discretion of those who have the power" (Millward Brown Goldfarb [MBG], 2004, p. 24).

The law surrounding the CSE's activities is multi-layered and anything but concrete. The flexibility afforded by providing "technical and operational assistance" to other federal security and law enforcement agencies allows for far too much discretion and therefore negates the onus for "probable cause" other than trusting that law enforcement officials and intelligence and security personnel will exercise good judgement. In the past this trust was compromised and therefore more answers are needed. The illegal activities of the NSA are well known to the public; however, the potential abuses in Canada are largely ignored even though

> Canada's program may be even more intrusive than its American counterpart, because, unlike the U.S. program there is no pretence that 'probable cause' is required of that the program is restricted to an 'anti-terrorism' purpose...or what restrictions there are on the type of information the CSE can pass on to law enforcement agencies (Allmand, 2006, p. A17).

The amount of discretion provided presents a wide array of questions. Will any evidence against terrorist suspects be admissible in court if it was illegally obtained by the CSE via a proxy agency such as the RCMP? Who is authorized to act upon his or her own discretion? Will this discretion lead to unwarranted (in the legal and necessary) interception of communications by Canadians? These possibilities exist, among others, but the purpose of this paper is not to itemize these possibilities but to challenge the security-rights dilemma and government's assertions that more security (surveillance included) will make Canada any safer, or that these trade-offs are justifiable. Though the CSE is inspected by a variety of review bodies such as the Auditor General, the Canadian Human rights Commission, the Privacy Commissioner and the Department of Justice, the CSE Commissioner and others, it has not been subject to a healthy degree of public scrutiny, given the possibilities for abuse and their consequences for social and political relationships in Canada among citizens and government.

Ambiguity seems to be the rule in state security and this has and severely stymied debate. Citizens are asked to uncritically accept that Canadian signals intelligence "respect[s] the laws of privacy and do not intentionally target Canadians"; however, it is unclear "as to the extent to which

interceptions of foreign targets may incidentally capture communications" (Rudner, 2001, p. 104). Only government officials charged with the responsibility of making sure the CSE adheres to Canadian laws are in-the-know, and most have a limited understanding of signals intelligence and law enforcement activities to begin with[67]. One must ask, "*quis custodiet ipsos custodies?*" which translates as "who's guarding the guards" or "who's watching the watchers?" [68](Lyon, 2007, p. 186). As Ogura (2006, pp. 291-2) aptly put it, "the greatest obstacle to freedom is not unknown others, but the greater governance of population management by the nation state;" and, unfortunately, it appears that the "creation of risk has outpaced the creation of trust" (Buzan & Little, 1999).

Some believe that management by the nation is so far progressed that Canada and other states with legislation similar to the *Anti-terrorism Act* are described as "national security state[s]" (Gabor, 2004). The power of government cannot be underestimated, and abuses of power cannot be tolerated. An excerpt from a statement given by Senator Frank Church in a 1975 congressional hearing about abuses by the NSA and other intelligence agencies is illustrative and deserves to be quoted at length:

> [The] capability at any time could be turned around on the American people and no American would have any privacy left, such [is] the capability to monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide. [T]he technological capacity that the intelligence community has given to the government could enable it to impose total tyranny....Such is the capability of this technology...I know the capacity that is there to make tyranny total in America, and we must see to it that this agency and all agencies that possess this technology operate within the law and under proper supervision, so that we never cross over that abyss. That is the abyss from which there is no return (in Sloan, 2001, p. 1467).

---

67 Intelligence is highly compartmentalized. Though committees or assigned individuals carry the responsibility of assessing the activities of intelligence and security agencies, Parliament does not openly debate it, or when it does, it is to a very superficial degree. Ogura explains that "most wiretapping laws have no articles regarding the obligation to disclose the source codes of computer programs of wire-tapping devices. Even if source code is disclosed, most members of parliament would not be able to understand it. Parliament cannot examine whether law enforcement indeed uses wire-tapping devices lawfully" (2006, p. 286).

68 As one example, in reviewing how effective the CSE Commissioner is in providing oversight and acting as an executive accountability mechanism, Canadians are faced with the same difficulties as assessing the agency itself: "because the CSE is such a secretive government institution...it is almost impossible to evaluate the reliability of the CSE about the exercise of its functions" (Rosen, 1993, p. 11). Furthermore, the position is relatively new (1996) and recent legislation such as amendments to the *Official Secrets Act* (now the *Security of Information Act*) limit the level of access granted to the Commissioner as Cabinet confidences are excluded (Shore, 2006, p. 465).

Some measure of trust is necessary for intelligence agencies to be effective; however, in a democratic state this means that these agencies are allegedly acting on the behalf of its citizens, directed by a legitimate government. Understanding the needs of its citizens is a primary requirement and the government and its agencies. In Canada this means understanding that the short term (unquantifiable) gains in terms of increased security cannot be privileged over the long term democratic health of the state, namely in terms of free and uninhibited communications. In Canada. citizens are offered token reassurances from its own government to "just trust us" (Boyer, 2003) and too often they acquiesce.

Canadian citizens must realize the impacts of illegal domestic surveillance in other democracies post 9-11 and appreciate the fact that Canada is neither immune from terrorist threats nor is it immune from government urges to prioritize expediency over lawfulness or sacrifice freedom in the name of security. The difficulty is that national security is a contested concept; however, this seems to suit Canadian traditions and values: "National security is the preservation of a way of life acceptable to...people and compatible with the needs and legitimate aspirations of others. It includes freedom from military attack and coercion, freedom from internal subversion, and freedom from the erosion of the political, economic, and social values which are essential to the quality of life" (Macnamara & Fitz-Gerald, 2002, p.8). True security requires these rights and values and, therefore, they are not in competition with one another and must be protected.

Legal strictures do not entirely protect these freedoms and values: technology makes surveillance of communications *possible*, and yet, legal limitations do not make the possibility of surveillance *impossible*, they only make it *illegal*. Some Canadians citizens believe that "informing the public of how [the *Anti-terrorism Act*] has been used would add some legitimacy to the effectiveness of the tool and give credence to [its] existence" (MBG, 2004, p. 27). There are a few who challenge the assumption that security and rights cannot coexist but still too few to reach the critical mass required to influence how democracy is done in times of crisis: this is a critical juncture. In her review of the *Anti-*

terrorism Act in 2005, Canada's Privacy Commissioner Jennifer Stoddard stated that she had three aims: 1) contain surveillance; 2) increase oversight; and 3) promote transparency, but this cannot be done alone as "a much broader coalition of interested persons and groups is needed if transparency is really to occur in a routine way" (Lyon, 2007, p. 194). For domestic interception of communications this means that "Canadians need to know how these powers are being used, on what scale, how often and at whose request" (Allmand, 2006. p. A17). It is understood that some secrecy is necessary, but the social and political consequences of illegal communications surveillance on Canadian citizens is too important to be based on faith. Offering citizens the promise of increased security at the expense of the security of rights is an impossible task. Some suggest that "global surveillance initiatives...only create illusions of security. Illusions that do little to catch or stop terrorists and ensnare the innocent, divert resources away from better initiatives, obscure our public policy debates, and betray our real personal and collective security" (Webb, 2007, p. 235). The possibility for the illegal interception of domestic communications must be taken seriously by citizens and government must do much more to provide reassurances and earn the trust of its citizens that it prematurely claims as its own.

References

Aid, M. & Wiebes, C. (2001). Introduction on the importance of signals intelligence in the Cold War. *Intelligence and National Security, 16*(1), pp. 1-26.

Allmand, W. (2006, March 31). We need answers on domestic spying. *Toronto Star*, p. A17.

American Civil Liberties Union [ACLU] (1999). Memo on international electronic surveillance concerns. Retrieved on 27 April 2009 from http://www.aclu.org/natsec/spying/14383leg19990607.html

Amoore, L., & De Goede, M. (2005). Governance, risk and dataveillance in the war on terror. *Crime, Law and Social Change, 43*(2/3), pp. 149-173)

Anderson, B. (2006). *Imagined communities.* London: Verso Books.

Andreas, P. (2003). Redrawing the line. Borders and security in the twenty-first century. International Security, 28(2), pp. 78-111.

Arquilla, J., Ronfeldt, D., & Zanini, M. (1999). Networks, netwar and information-age terrorism. In I. O. Lesser; B. Hoffman; J. Arquilla; D. Ronfeldt & M. Zanini (Eds.), *Countering the new terrorism* (pp. 39-85). Washington, D.C.: RAND.

Babcock, C. (2006, January 9). Data, data, everywhere. *Information Week.* Retrived on 29 June, 2009 from http://www.informationweek.com/news/global-cio/showArticle.jhtml?articleID=175801775

Bahdi, R. (2003). No exit: Racial profiling and Canada's war against terrorism. *Osgoode Hall Law Journal, 41*(2&3), pp. 293-316.

Bamford, J. (1982). *The puzzle palace: Inside America's most secret intelligence organization.* Boston, MA: Houghton Mifflin.

Barnett, C. (2003). *Culture and democracy: Media, space and representation.* Tuscaloosa, AL: University of Alabama Press.

Betts, R.K. (1978). Analysis, war and decision: Why intelligence failures are inevitable. *World Politics, 32*(1), pp. 61-89.

Bigo, D. (2006). Security, exception, ban and surveillance. In D. Lyon (Ed.), *Theorizing surveillance: The Panopticon and beyond* (pp. 46-68). Portland, OR: Willan Publishing.

Bill C-46, *An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act*. Retrieved on 3 September 2009 from http://www2.parl.gc.ca/HousePublications/Publication.aspxDocId=4008179&Language=e&Mode=1

Bill C-47, *An Act regulating telecommunications facilities to support investigations*. Retrieved on 3 September 2009 from http://www2.parl.gc.ca/HousePublications/Publication.aspxDocId=4007628&Language=e&Mode=1

Birch, A. H. (2007). *The concepts and theories of modern democracy, 3rd ed.* New York: Routlege.

Bloss, W. (2007). Escalating U.S. police surveillance after 9/11: An examination of causes and effects. *Surveillance & Society, 4*(3), pp. 208-228.

Botan, C. (1996) Communication work and electronic surveillance: A model for predicting panoptic effects. *Communiction Monographs, 63*, pp. 293-313.

Bovard, J. (2006, July 21). The 'terrorist' batting average. *The Boston Globe*. Retrieved on 13 January 2009 from http://www.boston.com/news/globe/editorial_opinion/oped/articles/2006/07/21/the_terrorist_batting_average/

Boyer, J. P. (2003). *"Just trust us:" The erosion of accountability in Canada*. Toronto: Dundurn Press.

Brabazon, H. (2006). Protecting whose security?: Anti-terrorism legislation and the criminalization of dissent. *YCISS Working Paper Number 43*. Retrieved 17 June 2009 from http://www.yorku.ca/yciss/publications/documents/WP43-Brabazon.pdf

Brodeur, J-P. (2003). The globalisation of security and intelligence agencies: A report on the Canadian intelligence community. In J-P. Brodeur, P. Gill & D. Töllborg (Eds.). *Democracy, law and security: Internal security services in contemporary Europe* (pp 210-261). Burlington, VT: Ashgate Publishing Company.

Brown, I., & Korff, D. (2009). Terrorism and the proportionality of Internet surveillance. *European Journal of Criminology, 6*(2), pp. 119-134.

Butler, D. (2009). Part I: A very different world. The Ottawa Citizen. Retrieved on 25 June 2009 from http://www.ottawacitizen.com/story_print.html?id=1232203&sponsor

Buzan, B., & Little, R. (1999). Beyond Westphalia? Capitalism after the fall. *Review of International Studies, 25*(5), pp. 89-104.

Campaign for Communication Rights in the Information Society [CRIS] (2005). Communication rights in the information society: Democratization of communication as social movement? The Convergence Center. Retrieved on 13 December 2008 from http://dcc.syr.edu/ford/mim/CRIS-case-9-12-05.pdf

Canada (2002). Canadian security and military preparedness: Report of the Standing Senate Committee on National Security and Defence. Ottawa, ON: Parliament, Senate Standing Committee on National Security and Defence. Retrieved on 2 July 2008 from http://www.parl.gc.ca/37/1/parlbus/commbus/senate/com-e/defe-e/rep-e/rep05feb02-e.pdf

Canada (2004). Canadian security guide book; An update of security problems in search of solutions: A report of the Standing Senate Committee on National Security and Defence, 2005 Ed. Ottawa, ON: Parliament, Senate Standing Committee on National Security and Defence. Retrieved on 30 June 2008 from http://www.parl.gc.ca/38/1/parlbus/commbus/senate/Com-e/defe-e/rep-e/rep03nov04-e.pdf

Canadian Journalists for Free Expression (2006). CJFE salutes landmark ruling in Juliet O'Neill case. Retrieved on 5 March 2009 from http://www.cjfe.org/releases/2006/19102006oneill.html

Chen, H., Thoms, S., & Fu, T. (2008). Cyber extremism in web 2.0: An exploratory study of international Jihadist groups. Conference paper presented at the IEEE International Conference on Intelligence and Security Informatics on 17 July 2008. Retrieved on 30 August 2009 from http://www.scribd.com/doc/14339981/Cyber-Extremism-in-Web-20-an-Exploratory-Study-of-International-Jihadist-Groups

Choudhry, S., & Roach, K. (2003). Racial and ethnic profiling: statutory discretion, constitutional remedies and democratic accountability. *Osgoode Hall Law Journal, 41*, pp. 1-39. Retrieved February 8, 2009 from www.ohlj.ca/archive/articles/41_1_choudry_roach.pdf

Chrisodoulidis, E. (2007). Presentation to Ronald Dworkin. Retrieved on 5 July 2008 from http://www.holbergprisen.no/HP_prisen/en_hp_2007_christodoulidis_dworkin.html

CCPA analysis of Bill C-36: An Act to combat terrorism (2001). Canadian Cenre for Policy Alernatives. Retrieved on 23 November 2009 from http://www.policyalternatives.ca/documents/National_Office_Pubs/Terrorism_Act.pdf

Christianson, D. L. (1986). Signals intelligence. In G. W. Hopple & B. W. Watson (Eds.), The military intelligence community (pp. 39-54). Boulder, CO: Westview Press.

Crow, B., Sawchuck, K., & Smith, R. (2008). Editorial. *Canadian Journal of Communication, 3*(3), pp. 351-356.

CSEC: Frequently ask questions (2008). Communications Security Establishment Canada. Retrieved on 10 October 2009 from http://cse-cst.gc.ca/faq-eng.html#Q9

CSEC's peer organizations (2008). Communications Security Establishment Canada. Retrieved on 24 March 2009 from http://www.cse-cst.gc.ca/home-accueil/about-apropos/peers-homologues-eng.html

DePalma, A. (2006, June 8). Terror arrests reveal reach of Canada's surveillance powers. *New York Times*, p. A12.

Department of Foreign Affairs and International Trade [DFAIT] (2008). Terrorism. Retrieved on 3 January 2009 from http://www.international.gc.ca/crime/terrorism-terrorisme.aspx?menu_id=30&menu=R

DiMaggio, P., Hargittai, E., Neuman, W.R., & Robinson, J.P. (2001). Social implications of the Internet. *Annual Review of Sociology, 27*, pp. 307-336.

Downing, J. D. H. (2001). *Radical media: Rebellious communication and social movements.* Thousand Oaks, CA: Sage Publications.

Don, B. W., Frelinger, D. R., Gerwehr, S., Landree, E., & Jackson, B. A. (2007). Networked technologies for networked terrorists: Assessing the value of information and communication technologies to modern terrorist organizations. RAND Corporation. Retrieved on 31 March 2009 from http://www.rand.org/pubs/technical_reports/2007/RAND_TR454.pdf

Edwards, L. (2001). *Mediapolitik: how the mass media have transformed world politics.* Washington, D.C.: The Catholic University of America Press.

Elmer, G., & Opel, A. (2006). Pre-empting panoptic surveillance: Surviving the inevitable War on Terror. In D. Lyon (Ed.), *Theorizing surveillance: The Panopticon and beyond* (pp. 139-159). Portland, OR: Willan Publishing.

Fernback, J., & Papcharrissi, Z. (2007). Online privacy as legal safeguard: the relationship among consumer, online portal and privacy policies. *New Media & Society, 9*(5), pp. 715-734.

Finan, J. S., & Macnamara W. D. (2001). An illustrative Canadian strategic risk assessment. *Canadian Military Journal, 2*(3), pp. 29-35.

Foley, J. (2007, January 1/8). Inside HP's data warehouse gamble. *Information Week.* Retrieved on 11 January 2009 from http://h20223.www2.hp.com/NonStopComputing/downloads/iwk7198-final.pdf

Franco Aas, K. (2009). Surveillance: Citizens and the state. *Surveillance & Society, 6*(3), pp. 317-321.

Fraser, N. (2007). Creating model citizens for the Information Age: Canadian Internet policy as civilizing discourse. *Canadian Journal of Communication, 32*(2), pp. 201-218.

Frequently asked questions [FAQs]. (2009, July 31). The Department of Justice. Retrieved on 22 May 2009 from http://www.justice.gc.ca/eng/antiter/faq/index.html

Frost, M., & Gratton, M. (1994). *Spyworld: Inside the Canadian and American Intelligence Establishments*. Toronto: Doubleday.

Gabor, T. (2004). The views of Canadian scholars on the impact of the *Antiterrorism Act. Department of Justice, Research and Statistics Division.* Retrieved on 14 July 2008 from http://www.justice.gc.ca/eng/pi/rs/rep-rap/2005/rr05_1/rr05_1.pdf

Garrett, R. K., & Danzinger, J. N. (2008). On cyberslacking: workplace status and personal internet use at work. *Cyberpsychology & Behaviour, 11*(3), pp. 287-292.

Garrett, R. K., & Danziger, J. N. (2007). IM=Interruption management? Instant messaging and disruption in the workplace. *Journal of Computer-Mediated Communication, 13*(1), article 2. Retrieved on 3 May 2009 from http://jcmc.indiana.edu/voll3/issue1/garrett.html

Gizewski, P., & Geddes, A. C. (2002). Catastrophic terrorism: Challenges and responses. Foreign Affairs and International Trade Canada. Retrieved 8 October 2009 from http://www.international.gc.ca/arms-armes/assets/pdfs/gizewski_geddes2002.pdf

Gourlay, C., & Taher, A. (2007, August 5). Virtual jihad hits Second Life website. TimesOnline. Retrieved on 18 September 2009 from http://www.timesonline.co.uk/tol/news/world/middle_east/article2199193.ece

Government looks to increase web surveillance (2009, June 18). CTV.ca News. Retrieved on 21 June 2009 from http://toronto.ctv.ca/servlet/an/local/CTVNews/20090618/tories_internet_090618/200906/18?hub=TorontoNewHome

Gross, S. R,. & Livingston, D. (2002). Racial profiling under attack. *Columbia Law Review,* 102(5), pp. 1413-1438.

Haggerty, K. D., & Gazso, A. (2005). The public politics of opinion research on surveillance and privacy. *Surveillance & Society, 3*(2/3), pp. 173-180.

Harcourt, B. E. (2007). *Against prediction: Profiling, policing and punishing in an actuarial age.* Chicago, IL: The University of Chicago Press, Ltd.

Hays, C. (2004, November 14). What Wal-Mart knows about customer's habits. *The New York Times.* Retrieved on 17 April 2009 from http://www.nytimes.com/2004/11/14/business/yourmoney/14wal.html

Hoffman, B. (1997). The confluence of international and domestic trends in terrorism. *Terrorism and Political Violence, 9*(2), pp. 1-15.

Homer-Dixon, T. (2002). The rise of complex terrorism. *Foreign Policy,* 128, pp. 52-62.

Hussain, N. (2007). Beyond norm and exception: Guantanamo. *Critical Inquiry, 33*(4), pp. 734-753.

Industry Canada (2006). Trends update: The expansion of cell phone services. Canada's Office of Consumer Affairs. Retrieved on 2 August 2009 from http://www.ic.gc.ca/eic/site/ocabc.nsf/vwapj/CTUCellen.pdf/$FILE/CTUCCellen.pdf

Integrated Threat Assessment Centre (2008). Key partners. Government of Canada. Retrieved on 14 October 2009 from http://www.itac-ciem.gc.ca/prtnrs/index-eng.asp

Jackson, R. (2005). *Writing the war on terrorism: Language, politics and counterterrorism.* Manchester, UK: Manchester University Press.

Jenkins, R. (2000). Categorization: Identity, social process and epistemology. *Current Sociology 48*(3), pp. 7-25. Retrieved on 21 October 2008 from http://csi.sagepub.com/cgi/content/abstract/48/3/7

Juergensmeyer, M. (1997). Terror mandated by God. *Terrorism and Political Violence 9*(2), pp. 16-23.

Karas, S. (2002). Enhancing the privacy discourse: Consumer information gathering as surveillance. *Journal of Technology Law and Policy, 7*(1), pp. 29-64.

Kenny, C., & Forrestall, J.M. (2004). Canadian security guide book 2005 edition: An update of security problems in search of solutions. Standing Senate Committee on National Security and Defence. Retrieved on 23 March 2009 from http://www.parl.gc.ca/38/1/parlbus/commbus/senate/Com-e/defe-e/rep/rep03nov04-e.pdf

Kellner, D. (2004). The media and the crisis of democracy in the age of Bush. *Communication and Critical/Cultural Studies, 1*(1), pp. 29-58.

Kydd, A. H., & Walter, B. F. (2006). The strategies of terrorism. *International Security, 31*(1), pp. 49-79.

Kostakopoulou, D. (2008). How to do things with security post 9/11. *Oxford Journal of Legal Studies, 28*(2), pp. 317-342.

Leman-Langlois, S., & Brodeur, J-P. (2005). Terrorism old and new: Counterterrorism in Canada. *Police Practice and Research, 6*(2), pp. 121-140.

Lendman, S. (2007). Police state America—A look back and ahead. Global Research Centre for Research on Globalization Database. Retrieved on 21 November 2008 from http://www.globalresearch.ca/index.php?context=va&aid=7622

Lewis, J. (2007). Critical questions: Domestic surveillance, FISA and terrorism. *Center for Strategic International Studies. CSIS.org.* Retrieved on 10 April 2009 from http://csis.org/files/media/csis/pubcs/071107_lewis.pdf

Lyon, D. (2002). Editorial: Surveillance studies. Understanding visibility, mobility and the phenetic fix. *Surveillance & Society, 1*(1), pp. 1-7.

Lyon, D. (2006). The search for surveillance theories. In D. Lyon (Ed.), *Theorizing surveillance: The Panopticon and beyond* (pp. 3-20). Portland, OR: Willan Publishing.

Lyon, D. (2007). *Surveillance studies: An overview.* Malden, MA: Polity Press.

Marrin, S. (2004). Preventing intelligence failures by learning from the past. *International Journal of Intelligence and Counterintelligence, 17*(4), pp. 655-672.

Macnamara, W. D., & Fitz-Gerald, A. (2002). A national security framework for Canada. *Policy Matters, 10*(3), pp. 1-38. Retrieved March 23, 2009 from http://www.irpp.org/pm/index.htm

McDonald, C. (2006). Are cell phone replacing traditional home phones? Innovation and Analysis Bulletin 8(2), pp. 12-13. Retrieved on 10 July 2009 from http://www.statcan.gc.ca/pub/88-003-x/88-003-x2006002-eng.pdf

Millward Brown Goldfarb (2004). Public views on the *Anti-terrorism Act (formerly Bill C-36).* Department of Justice, Research and Statistics Division. Retrieved on 3 March 2009 from http://canada.justice.gc.ca/eng/pi/rs/rep-rap/2005/rr05_3/rr05_3.pdf

Monash, C. (2008, October 15). Teradata's petabyte power players. Retrieved on 30 June 2009 from http://www.dbm2.com/2008/10/15/teradatas-petabyte-power-players

Moon, P. (May 27, 1991). Secrecy shrouds spy agency. *Globe and Mail*, pp. A1, A4.

Morris, N. (1996). Inside Canada's most secret agency. *Maclean's, 109*(36), pp. 32-35.

Mueller, M.L., Keurbis, B.N., & Pagé, C. (2007). Democratizing global communication? Global civil society and the Campaign for Communication Rights in the Information Society. *International Journal of Communication, 1*, pp. 267-296.

Müller, V. C. (2009). Would you mind being watched by machines? Privacy concerns in data mining. *AI & Society, 23*(4), pp. 529-544.

Ogura, T. (2006). Electronic government and surveillance-oriented society. In D. Lyon (Ed.), *Theorizing surveillance: The Panopticon and beyond* (pp. 270-295). Portland, OR: Willan Publishing.

O'Neill, J. (2005). *Echelon: Somebody's listening.* Tarentum, PA: Word Association Publishers.

Part of the Anti-terrorism Act violates the Charter: Judge (2006, October 25). CBC.ca. Retrieved on 1 September 2009 from http://www.cbc.ca/canada/story/2006/10/24/khawaja-ruling.html

Paulson, B., Kenny, C., & Inkster, N. (2008). Panel discussion: Is national security overly focused on terrorism? *Gazette, 70*(3), pp. 12-13.

Pestana, C., & Swartz, O. (2008). Communication, social justice and creative democracy. In O. Swartz (Ed.), *Transformative communication studies: Culture, hierarchy and the human* condition (pp. 91-113). Leicester, UK: Troubador Publishing Ltd.

Public Safety and Emergency Preparedness Canada (2003). Annual report on the use of electronic surveillance. Retrieved on 3 May 2009 from http://dsp-psd.pwgsc.gc.ca/Collection/PS1-1-2003E.pdf

Public Safety Canada (2007). Annual report on the use of electronic surveillance—2007. Retrieved on 4 May 2009 from http://www.publicsafety.gc.ca/abt/dpr/_fl/elecsur-07-eng.pdf

Public Safety Canada (2004). Annual report on the use of electronic surveillance- 2004. Retrieved on 3 June 2009 from http://www.publicsafety.gc.ca/abt/dpr/le/elecsur-eng.aspx

Pugliese, D. (2009, May 12). East Ottawa slated to get new spy HQ. *The Ottawa Citizen.* Retrieved on 29 August 2009 from http://www.ottawacitizen.com/business/East+Ottawa+slated/1586676/story.html

Richelson, J.T., & Ball, D. (1990). *The ties that bind: Intelligence cooperation between the UKUSA countries 2nd Ed.*. Boston, MA: Unwin Hyman.

Riem, A. (2007). Second Life—The legal implications of a virtual world. *The In-House Lawyer.* Retrieved on 20 August 2008 from http://investmentfraudlitigation.com/fraud_media_center/articles/IHL153.pdf

Rights & Democracy (2003, January 29). The challenges facing the 59th session of the United Nations Commission on Human Rights: Written statement submitted by Rights & Democracy. Retrieved on 9 October 2009 from http://dd-rd.ca/site/publications/index.php?id=1332&page=2&subsection=catalogue

Risen, J., & Lichtblau, E. (2005, December 16). Bush lets U.S. Spy on callers without courts. *New York Times.* Retrieved July 16, 2009 from http://www.nytimes.com/2005/12/16/politics/16program.html?_r=1

Rivard, P. G., & Faragone, J. (2007). Privacy retention issues of defence intelligence. *Canadian Military Journal, 8*(1), pp. 83-88.

Ressler, S. (2006). Social network analysis as an approach to combat terrorism: Past, present, and future research. *Homeland Security Affairs, 2*(2), pp. 1-10. Retrieved 30 May 2009 from http://www.hsaj.org/pages/volume2/issue2/pdfs/2.2.8.pdf

Rodriguez, A. (2008). Communication and the end of hierarchy. In O. Swartz (Ed.), *Transformative communication studies: Culture, hierarchy and the human condition* (pp. 1-15). Leicester, UK: Troubador Publishing Ltd.

Rosen, P. (1993). The Communications Security Establishment: Canada's most secret intelligence agency. Ottawa, ON: Library of Parliament, Research Branch. Retrieved on 28 June 2008 from: http://dsp-psd.pwgsc.gc.ca/Collection-R/LoPBdP/BP-e/bp343-e.pdf

Rudner, M. (n.d.). Contemporary threats, future tasks: Canadian intelligence and the challenges of global security. Retrieved on 10 October 2009 from http://circ.jmellon.com/docs/pdf/canadian_intelligence_and_the_challenges_of_global_security.pdf

Rudner, M. (2001). Canada's Communications Security Establishment from Cold War to globalization. *Intelligence and National Security, 16*(1), pp. 97-128.

Rudner, M. (2002). The globalization of terrorism: Canada's intelligence responses to the post-September 11th threat environment. *Canadian Issues,* pp. 24-29.

Rudner, M. (2007). Canada's Communications Security Establishment, signals intelligence and counterterrorism. *Intelligence and National Security, 22*(4), pp. 473-490.

Sassen, S. (2002). Towards a sociology of information technology. *Current Sociology, 50*(3), pp. 365-388.

Schneiderman, D. (2001). Terrorism and the risk society. In R. J. Daniels, P. Macklem, & K. Roach (Eds.), *The security of freedom: Essays on Canada's Anti-terrorism Bill* (pp. 63-72). Toronto: U of T Press.

Schneier, B. (2003). *Thinking sensibly about security about security in an uncertain world.* New York: Copernicus Books.

Sernovitz, D. J. (2009, July 31). National Security Agency growth could add 11 000 workers at Fort Meade. *Baltimore Business Journal.* Retrieved 19 August 2009 from http://www.bizjournals.com/baltimore/stories/2009/08/03/story1.html

Shore, J. (2006). Intelligence oversight and review in Canada. *International Journal of Intelligence and CounterIntelligence*, 19:3, 456-479.

Sloan, L. D. (2001). Echelon and the legal restrains on signals intelligence: A need for reevaluation. *Duke Law Journal, 50,* pp. 1467-1510. Retrieved on 29 December 2008 from http://www.law.duke.edu/shell/cite.pl?50+Duke+L.+J.+1467

Slobogin, C. (2005). Transaction surveillance by the government. *Mississippi Law Journal, 75*, pp. 139-192.

Small, M. (1994). *Covering Dissent: The Media and the Anti-Vietnam War Movement.* New Brunswick, NJ: Rutgers University Press.

Solove, D. (2008). *Understanding privacy.* London: Harvard University Press.

Statistics Canada, (2006). 2006 Census: Portrait of the Canadian population in 2006: Highlights. 2006 Census: Analysis Series. Retrieved on 30 May 2009 from http://www12.statcan.ca/census-recensement/2006/as-sa/97-550/p1-eng.cfm

Statistics Canada (2007). Immigration in Canada: A portrait of the foreign-born population, 2006 Census. Ottawa. Statistics Canada. Retrieved on 15 May 2009 from http://www12.statcan.ca/census-recensement/2006/as-sa/97-557/p2-eng.cfm

Statistics Canada (2008). Canadian Internet use survey. *The Daily.* Retrieved on 12 June 2009 from http://www.statcan.gc.ca/daily-quotidien/080612/dq080612b-eng.htm

Strandburg, K. J. (2008). Freedom of association in a networked world: First amendment regulation of relational surveillance. *Boston College Law Review, 49*(3), pp. 741-822.

Tibbetts, J. (2009, June 17). Feds to give cops Internet-snooping powers. CanWest News Service. Retrieved on 21 June 2009 from http://www.canada.com/story_print.html?id=1706191&sponsor=

Urgin, J. C., Pearson, J. M., & Odom, M. D. (2008). Profiling cyber-slackers in the workplace: Demographic, cultural and workplace factors. *Journal of Internet Commerce, 6*(3), pp. 75-89.

U.S. Office of the Press Secretary (2001, September 20). Address to a joint session of Congress and the American people. Office of the Press Secretary. Retrieved on 11 December 2008 from http://georgewbush-whitehouse.archives.gov/news/releases/2001/01/print/20010920-8.html

Use of mobile phones almost level with landline-Canadian statistics. (n.d.). *Cell phones etc.* Retrieved on 7 January 2009 from http://www.cellphones.ca/news/post002323

Webb, M. (2007). *Illusions of security: Global surveillance and democracy in the post-9/11 world.* San Francisco: City Lights Books.

Whitaker, R. (2003). Keeping up with the neighbours? Canadian responses to 9/11 in historical context. *Osgoode Hall Law Journal, 40*(2), pp. 241-264.

Who we are (2009). Public Safety Canada. Retrieved on 10 October 2009 from http://publicsafety.gc.ca/abt/wwa/index-eng.aspx

Wilson, D. (2009). Canadian surveillance legislation dissected- Bill C-46. Zeropaid.com. Retrieved on 10 July 2009 from http://www.zeropaid.com/news/86462/canadian-surveillance-legislation-dissected-bill-c-46

Wright, S. (1998). An appraisal of technologies of political control. European Parliament, Scientific and Technological Options Assessment Unit. Directorate General for Research. Retrieved on 14 August 2008 from http://jya.com/atpc.htm