Volume 5 – Spring 2009
djim.management.dal.ca

Protecting Personal Information
Nova Scotia's Personal Information International Disclosure Protection Act and the USA Patriot Act

Abstract: This paper looks at Nova Scotia's Personal Information International Disclosure Protection Act (PIIDPA), a piece of legislation that was specifically designed to protect Nova Scotia's citizens from having their personal information accessed by foreign governments. This is a direct reaction to new powers the United States government has given itself, through the *USA Patriot Act*, in collecting information to protect Americans from terrorism.

The main thesis of my paper will be to determine whether this piece of legislation is an effective piece of public policy, asking the question: Does Nova Scotia, through PIIDPA, have the ability to protect Nova Scotians from having their personal information accessed by foreign governments? Using a policy framework designed by political scientists Paul Sabatier and Daniel Mazmanian (1980) to analyse policy effectiveness I will determine whether PIIDPA is an act that will effectively do what it was created to do, or whether it will face problems in achieving those goals.

About the Author: Nathaniel Smith is a native of Halifax, Nova Scotia. He holds a B.A (Hons.) in History from Saint Mary's University (2006) and a Certificate of Municipal Government Administration from Dalhousie University (2004). He is currently enrolled in the joint Master of Public Administration (MPA) and Master of Library and Information Studies (MLIS) program at Dalhousie University and expects to graduate in 2010. Nathaniel has a love for history. He is the owner of the award winning Prospect Genealogical Website (www.prospectvillage.ca). He is a member of a number of local historical groups.

Protecting Personal Information
Nova Scotia's Personal Information International Disclosure Protection Act and the USA Patriot Act

Introduction

The use of information for the purpose of intelligence gathering has become more important to governments since the events of 11 September 2001. This is particularly the case in the United States where the government has made it its mission to identify and combat terrorism before incidents happen. With the passage of the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*, more commonly referred to as the *USA Patriot Act* or *The Patriot Act*, from October 2001, the United States government has given itself and the various agencies that gather intelligence certain powers to achieve the objectives of combating terrorism and those who could potentially commit terrorist acts (Ibbitson, 2001). These new powers under the *Patriot Act* have changed the way the U.S. government collects information and whom they can ask to disclose information. These privileges under the *Patriot Act* have come under heavy criticism as large amounts of private personal information have been collected since 2001 on not only American citizens but citizens throughout the world in an effort to "combat and obstruct' terrorism (MacGregor, 2001; Shenon, 2003).

In the fall of 2006, the provincial government of Nova Scotia, following that of British Columbia, enacted a piece of legislation which prevents foreign governments, particularly that of the United States, from accessing the personal information of the citizens of Nova Scotia. The *Personal Information International Disclosure Protection Act* (PIIDPA) was passed unanimously by provincial legislators and requires foreign governments and businesses to consult not only with the Government of Nova Scotia but also with the individual whose information they are requesting and the failure to do so will result in penalty. This is an action that is in complete conflict with the current political and legal situation in the United States where the government, under the *Patriot Act*, has access to personal information under secret request and the bodies that are asked to disclose this information are required by law not to disclose that the information has been requested.

This paper will look at how Nova Scotia's PIIDPA legislation came to be conceived and then will attempt to evaluate its effectiveness as a piece of public policy by running the legislation through a policy framework created by political scientists Paul Sabatier and Daniel Mazmanian (1980). This framework is specifically designed to examine and analyse what Sabatier and Mazmanian refer to as "traditional regulatory policies in which governments seek to alter the behaviour of private target groups", with a caveat that with a small bit of modification it can be

applied to examine the changes in the behaviour of field-level bureaucrats, local and (state) officials, and private actors through the disbursement of funds (Sabatier and Mazmanian, 1980). Finally, Sabatier and Mazmanian's (1980) framework for policy implementation is extremely useful in showcasing the various factors that help to ensure that Nova Scotia's law will meet its designed policy implementation objectives.

SECTION I: Setting the Scene

1.1 The Patriot Act and Section 215

Immediately after the 11 September 2001 terrorists attacks on the World Trade Center twin-towers in New York City, the Pentagon in Washington, D.C., and American Airlines Flight 77 which crashed in Pennsylvania, the United States government took quick action to introduce and pass the *Patriot Act*, giving its law enforcement agencies expanded power to seek out, combat and neutralize terrorists before they could commit acts of terror again on American soil. The Act was rushed through the United States Congress and Senate in forty-five days and President George W. Bush heralded this new law as an necessary new tool to fight immediate dangers (Ibbitson, 2001). One of the most potent and highly criticised parts of the law is Section 215.

Section 215 strikes out and amends particular sections in the *Foreign Intelligence Surveillance Act* (FISA) of 1978, particularly sections 501 through 503 and inserts a new section 501 entitled "Access to Certain Business Records for Foreign Intelligence and International Terrorism Investigations." This particular section extends the ability of the Federal Bureau of Investigation (FBI) to subpoena records in the care of private corporations and businesses for the purposes of terrorism investigations. Some of these extended powers give the government the ability to require organizations to turn over personal information without warrant, without cause and without reason. A particular issue with this power is that the organization being asked to provide information is compelled to comply and also to not speak about or disclose that the search was requested and whether or not information was obtained (United States Senate, 2001).

The American Civil Liberties Union (ACLU), in particular, is a significant critic of Section 215 on the grounds that the section directly violates American's Fourth Amendment rights to unlawful searches (American Civil Liberties Union, 2007). In an updated report on what it terms "the emerging surveillance society," the ACLU blasts The *Patriot Act* and the United States government – Congress, the Senate and in particular the Bush Administration – for what it perceives as a "weakening of checks and balances on the government's surveillance powers." It goes further to suggest that the "current government has chosen mass surveillance as its principal approach to preventing another terrorist attack," rather than take steps to strengthen

infrastructure and secure ports of entry throughout the country (Stanley and Steinhardt, 2007, p. 4, 8). The U.S. Department of Justice makes every effort to dispel these accusations. The Justice Department stated in October 2002 that "the House Judiciary Committee issued a press release indicating it is satisfied with the Department's use of section 215: 'The Committee's review of classified information related to FISA orders for tangible records, such as library records, has not given rise to any concern that the authority is being misused or abused'" (U.S. Department of Justice, 2007).

The ACLU is not the only organization in the U.S critical of the Bush Administration for the powers it has granted the FBI and other intelligence agencies under Section 215 of the *Patriot Act*. One group of particular interest is Patriots to Restore Checks and Balances, a bi-partisan alliance of individuals and organizations chaired by former Republican Congressman Bob Barr. This organization's sole purpose is to ensure that Congress makes an effort to verify and scrutinize the *Patriot Act* in a way it did not do when it originally passed the law in 2001. The group's mission statement states that it agrees that "it is necessary to provide law enforcement with the resources it needs to defeat terrorism, but it is that they are being allowed – by law – to go beyond that mission and infringe on the rights of law-abiding Americans in ways that raise serious constitutional and practical concerns" (Patriots to Restore Checks and Balances, 2007).

Even though there is widespread opposition towards the powers given to American law enforcement agencies in order to protect Americans from terrorist threats, the United States Congress reauthorized much of the *Patriot Act* when the legislation came up for renewal in March 2005. Those who oppose the Act will have to wait till 2009 when the current legislation comes up for renewal again. In 2009 there is a new President and a new Congress and they will have to determine whether or not these powers represent an adequate way to combat present threats.

1.2 Canadian Response to the Patriot Act

The Canadian Parliament, like the U.S. Congress, passed legislation in response to the attacks of 11 September 2001. Canada's new legislation, entitled the *Anti-Terrorism Act*, was similar in intent but different in scope from that of the United States. The *Anti-Terrorism Act* has been divided into three specific areas in the effort to combat terrorism. These parts include: new abilities for the government to identify, prosecute, convict and punish terrorists; new and stronger investigative tools which allow law enforcement and security agencies the ability to carry out the above; and, finally, stronger laws dealing directly with hate crimes and propaganda. The following discussion focuses on the first two points as they directly relate to the topic being discussed (Government of Canada, 2001).

The first section of the new Act covers the abilities of law enforcement officials and national security agencies to investigate, prosecute, and convict or punish terrorists. The Canadian government took steps to do this by ratifying two United Nations Conventions and Protocols related to terrorism and terrorist activities. Having already signed all twelve agreements, the ratification of the remaining two helped the *Anti-Terrorism Act* go a step further to defining terrorist activity, something not previously defined in the *Canadian Criminal Code* (Wispinski, 2006, p. 2). The new definition of "terrorist activity" is that it is "an action that takes places either within or outside of Canada that is an offence under one of the 10 UN anti-terrorism conventions and protocols; or is taken or threatened for political, religious or ideological purposes and threatens public or national security" (Wispinski, 2006, p. 2; Government of Canada, 1985, s. 83.01(1)). The latter part of this definition deviates from the American definition of terrorist activities and terrorist groups, which does not includes political, religious and ideological purposes (Wispinski, 2006, p. 2).

The second section works with the first and is centered on the government's ability to investigate and establish terrorist activity. This includes the use of electronic surveillance and amendments to the *Official Secrets Act*, the *Canada Evidence Act* and parts of the *National Defence Act* dealing with the *Communications Security Establishment (CSE)*. The Actchanges very little with regards to how electronic surveillance is conducted in Canada; however, it does extend the period in which a wiretap can be used, from sixty days to up to one year. This once again differs from U.S. law which Wispinski suggests had various levels of privacy protection and access via surveillance techniques prior to the enactment of the *Patriot Act* (2006, p. 8-9). Since 2001 the breakdown of privacy protection on the part of the American government, specifically surrounding wiretapping, has led to a number of very public controversies exposing the government's willingness to spy on its own citizens and their contacts internationally (The Associated Press, 2006).

The Anti-Terrorism Act also differs from the *Patriot Act* in the authority it gives government to gather and share information, making little change to previous laws that deal with this type of surveillance. According to Wispinski (2006), the *Patriot Act* is "less concerned with information secrecy and more concerned with giving government officials more power to gather foreign intelligence information from a variety of sources and share it with other government officials and agencies" (p. 15). In the Canadian context there are a number of checks and balances in place to ensure that abuse of these clauses does not take place. For example, the Canadian legislation establishes the need for a Superior Court justice to authorize and approve of any type of surveillance and includes the need of law enforcement to inform the target of the surveillance that they are being investigated, though newer legislation has amended this particular point to withhold disclosure of the investigation from the surveillance suspect.

Unlike its American counterpart the Canadian act has significant checks and balances built into the legislation itself. First and above all, the *Anti-Terrorism Act* must adhere throughout to all sections of the *Charter of Rights and Freedom*. The main checks and balances deal with any potential abuse of the various clauses under the Act; also, the Act has specific provisions that require both the Solicitor General of Canada and provincial counterparts to report annually on how the various provisions of the Act have been used (Jenkins, 2003, pp. 548-551). This differs from The *Patriot Act* as there are no provisions in the latter for the reporting of arrests, warrantless access to information and so on. Wispinski (2006) argues that though the two pieces of legislation are similar in their intent, their focus and their ability to achieve their objective, there are significant differences. She argues that this is reflective of

> [T]he fact that while Canada and the United States both have legal systems rooted in the British common law tradition, they, as sovereign nations, have developed different constitutional legislative and bureaucratic structures, as well as somewhat different approaches to legislative problem solving. (p. 27)

1.2.1 Canadian and Provincial Privacy Laws

Canada has two federal laws dealing with privacy. *The Privacy Act*, which was enacted in 1983, places limits on the collection, use and disclosure of personal information held by the Federal Government as well as providing individuals the right to access and request personal information being held by the government pertaining to them. The second piece of legislation that covers information privacy is the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, enacted in 2000, which covers private sector collection, use, and disclosure of personal information and which also gives individuals the right to access and request information being held by these organizations that pertains to them (Office of the Privacy Commissioner of Canada, 2007a).

All provincial jurisdictions have laws for the protection of privacy and personal information; however, only Alberta, British Columbia and Ontario have laws that are similar in intent to that of PIPEDA and are thus considered exempt with regard to certain sections of that law (Office of the Privacy Commissioner of Canada, 2007b).

1.2.2 British Columbia

British Columbia was one of the first provinces to actively question the validity of the *Patriot Act* in terms of the access it grants authorities to Canadians' private personal information. The whole thing came to light when BC's Information and Privacy Commissioner, David Loukidelis, was asked to comment on the legality of the Province's decision to contract out the administration of the province's public health insurance program to a U.S. owned company's

subsidiary in the province and to determine whether this decision violated the province's protection of privacy legislation, *Freedom of Information and Protection of Privacy Act (FOIPPA)*, in relation to the *Patriot Act*. Mr. Loukidelis concludes in his report, *Privacy and the USA Patriot Act: Implications for British Columbia and Public Sector Outsourcing*, that there is a significant degree of concern with regard to how deeply the *Patriot Act* could reach into a foreign jurisdiction. He makes sixteen recommendations for amendments to the province's FOIPPA to ensure that any foreign subpoena for access to information be made public by the contracted service provider. He also recommends that the province create and publish a litigation policy whereby it outlines how it will deal with a "subpoena, warrant, order, demand or request made by a foreign court or other foreign authority for disclosure of personal information in British Columbia" (Office of the Privacy Commissioner of Canada, 2007b, p. 19). The Commissioner's final recommendation urges the Federal government to consult with the provinces and territories on the potential to enter into talks with the U.S. and Mexico for "comprehensive transnational data protection standards and for multilateral agreements respecting continental control and oversight of transnational information sharing for government purposes, including national security and public safety purpose" (Office of the Privacy Commissioner of Canada, 2007b, p. 22).

Though the Commissioner's report was received in October 2004 and the government did move quickly to amend FOIPPA legislation to meet his recommendations, BC's Ministry of Health Services nonetheless entered into an agreement with Maximus BC Health Inc., a subsidiary of Maximus Inc., the U.S. owned parent company, in November 2004 to oversee the province's public health insurance program (BC Government and Service Employees' Union v. British Columbia Minister of Health Services, 2005).

In 2005 a lawsuit was filed in the B.C. Supreme Court by the British Columbia Government and Services Employee's Union (BCGEU) citing this contract as a direct violation of the province's privacy laws. The BCGEU (2004) stated that, "under ss. 32 and 33 of FOIPPA, British Columbians have a statutory right to expect that their personal information will only be used for the purposes for which it was obtained, or for other purposes, such as Canadian law enforcement, where reasonable grounds exist" (p. ii). They argue, however, that due to the move to outsource services dealing with health records the government is directly compromising the security and privacy of this information (BCGEU, 2004, p. i-iii). The BCGEU also argued that the contract went further in violating Canadians rights under the *Charter*, specifically ss. 7 which deals with life, liberty and security of person and ss. 8 which deals with the right to be secure against unreasonable search and seizure. They cite the precedent of the Supreme Court of Canada's recognition of three kinds of privacy protection within the Constitution, that of privacy in places, privacy of the person, and privacy of information (BCGEU, 2004, p. 35). The Hon. Mr. Justice F. A. Melvin presided over this case and concluded that he was, "satisfied that there has not been a breach of either ss. 7 or 8 of the

Charter or of *The Freedom of Information and Protection of Privacy Act*. Consequently, the petition fails on that basis as well" (BCGSE vs. BC Minister of Health Services, 2005). The BCGEU subsequently appealed the judgment but it was upheld in BC Court of Appeals (BCGEU vs. BC Minister of Health Services, 2007).

1.3 Nova Scotia and PIIDPA

Following the British Columbia court decisions and the report of that province's Information and Privacy Commissioner, the Nova Scotia government took steps to deal with the issue of foreign disclosure of its citizens' personal information. The issue was first raised by Nova Scotia's Auditor General in his 2005 Annual Report in a discussion on Electronic Information Security and Privacy Protection. The Auditor General stressed that, "the Government of Nova Scotia should continue to assess the implications of the changes enacted by the U.S. Government through the *Patriot Act* which could pose a risk to the security of the personal information of Nova Scotians" (Office of the Auditor General of Nova Scotia, 2005, p.33).

In July 2006 Nova Scotia's government re-introduced *Bill No. 19*, *Personal Information International Disclosure Protection Act*, a bill that died on the order paper in the previous legislature when the Premier called an election. This bill takes steps to "strengthen against the disclosure of Nova Scotians' personal information, under the U.S. Patriot Act" (Nova Scotia Legislature, 2006, p. 314). The act was passed unanimously by all political parties and heralded by privacy watchdogs as a productive move to ensure the security of private personal information. David Fraser, a privacy lawyer for McInnis Cooper, a Halifax law firm, suggests the act might also have the ability to "encourage more companies to set up their operations in Nova Scotia rather than the U.S.," that the province is showing that there is a "good regulatory climate," in Nova Scotia and that this "allows technology companies in particular to flourish" (Furlong, 2007: E7). However, it is commonly agreed that there is still some vagueness on how this new law will be implemented and implemented effectively.

The PIIDPA was designed specifically to ensure the security and privacy of Nova Scotians' personal information, and the act describes an offence as "the improper storage, collection, use or disclosure, failure to notify the Minister of Justice of foreign disclosure demands, and the improper discipline or termination of employees" (NS Department of Justice, 2006). The act ensures that the Government of Nova Scotia and specifically the Minister of Justice are properly informed of any foreign demand for disclosure of the personal information of Nova Scotians. The act goes further in requiring that "service providers storing information only collect and use personal information necessary for their work for a public body or municipality" (Government of Nova Scotia, 2006). PIIDPA includes whistleblower protection for employees who work for service providers and this particularly protects them should they report an offence. The act also includes a financial penalty should there be an offence of the act, up to

$2,000 per government employee who discloses personal information. The penalties extend into the private sector with fines up to $2,000 for employees and $500,000 for companies who fail to adhere to the act (Government of Nova Scotia, 2006).

The following discussion uses Sabatier and Mazmanian's (1980) framework for policy implementation to assess whether Nova Scotia's PIIDPA can be implemented effectively to ensure the security and privacy of information.

SECTION 2: A Framework for Policy Analysis

2.1: Sabatier and Mazmanian's Framework

Paul Sabatier and Daniel Mazmanian (1980) developed a framework for public policy implementation that looks at how the implementation of public policy relates to variables in the implementation process, specifically statutory and non-statutory variables. They suggest that their framework, "attempts to capture the dynamic nature of implementation by focusing on the manner in which changes in socio-economic conditions, public opinion, and other factors affect the implementation process" (1980, p. 538). The implementation of public policy is the practical application of "basic policy decisions," which according to Sabatier and Mazmanian (1980) usually take the form of a statute. These decisions identify a problem, suggest ways to deal with the problem and then go further to "structure" the implementation process so as to solve the problem. Their framework is designed to identify the factors that directly affect whether a decision can be implemented effectively. Or, put another, way external factors promote or prevent a statute's objectives from being reached through the implementation process.

Sabatier and Mazmanian have designed their framework around three broad categories (1) the tractability of the problem(s) being addressed by the statute; (2) the ability of the statute to favourably structure the implementation process or the statutory variables and (3) the net effect of a variety of "political" variables on the balance of support for statutory objectives, or, the non-statutory variables (1980, p. 541). They suggest that although each of these three categories or variables is independent of each other they can work to influence and affect the results of one another. In a study of Environment Canada's effectiveness as an organization within the Canadian bureaucracy, Paul Brown uses the Sabatier and Mazmanian model and suggests that the relationship between these variables, though casual, is important due to a number of factors. Brown (1992) describes these factors by suggesting that "for example, the perceived tractability of a problem could well influence the degree of support for proposed solutions," or that "the degree of public support clearly has an impact on the level of support accorded a problem" (p. 35). Brown supports the idea behind the framework in his description of how each of these pillars of implementation, statutory and non-statutory, can directly influence the results of each objective (1992, p. 35). A brief discussion of each of these

variables is needed before this model can be applied to Nova Scotia's PIIDPA legislation.

The first category in the framework is described as the tractability of the problem(s) addressed by the statute. Sabatier and Mazmanian (1980) make it quite clear that some problems are easier to deal with than others based solely on their tractability. This variable has a number of equally independent factors or variables that Sabatier and Mazmanian have combined to help them determine the tractability of the problem(s). The first variable attempts to establish the difficulties a decision will have measuring the changes in the seriousness of a problem, in relating these changes back to the behaviour of the target group, and in developing the technology to enable the target group to achieve the changes prescribed. This can be described in the ability of a statutory objective that requires a certain type of technology to be used by the target group in order to achieve its objectives. Sabatier and Mazmanian (1980) use sulphur dioxide reduction as an example of this. They argue that the availability of cheap technologies to achieve the goal of reduction either at the point where coal burning takes place or before, in the refining process will encourage those with the task of reducing emissions to do so with greater success than they would if the technology was unavailable and/or relatively expensive. The second sub-variable is the diversity of behaviour being regulated; suggesting that the larger the diversity of the behaviour a statute is attempting to regulate the more difficult it will be to meet the objectives. The third sub-variable looks at the percentage of the population within a political jurisdiction whose behaviour that needs to be changed, arguing that the smaller the target group, the easier the ability to get them to change their behaviour to reach the statutory objectives. Finally, the fourth sub-variables looks at the extent of behavioural change required of the target group suggesting that the larger the amount of change in behaviour that must take place the less likely successful implementation will occur. Sabatier and Mazmanian (1980) stress that though all of these variables help move successful implementation forward not all need to be in play. They use the U.S. Voting Rights Act of 1965 to stress this point, suggesting that this act showed strong characteristics of variables one and three but showed signs of considerable behavioural change on the part of Southern voting officials in accepting the change in law. They also stress the importance of caution in placing too much emphasis on the tractability of the problem because they believe that their framework can show how even extremely difficult problems can be solved by properly understanding the other statutory and non-statutory variables at play (Sabatier and Mazmanian, 1980, p. 541-544).

The second category is a look at the how statute structures the implementation process. Sabatier and Mazmanian (1980) suggest that a statute has "the capacity to "structure" the entire implementation process through its selection of the implementing institutions; through providing legal and financial recourse to those institutions; through biasing the probable policy orientations of agency officials; and through regulating opportunities for participation of non-agency actors" in the process (p. 544). If a statute is designed or constructed carefully it can

lend itself very efficiently to reaching the objectives it sets out to achieve. Sabatier and Mazmanian support this by suggesting that all statues explicitly and implicitly have an underlying causal theory which promotes the objectives and helps the agencies or institutions that are charged with implementation deal with the target group's behavioural change. They posit this theory as having two components, "technical validity,' and "implementation effectiveness.' The first component describes the relationships between the behaviour of the target group and the ability to reach the statute's objectives and the second component deals with how institutions charged with implementation help foster behavioural change within the target group. Sabatier and Mazmanian (1980) stress the importance of both components being valid if statutory objectives are to be attained. The other six sub-variables all deal with implementing institutions and thus the second component of the causal theory.

The third category attempts to describe the non-statutory variables affecting the implementation process. Sabatier and Mazmanian (1980) suggest that this particular variable category describes the

> [E]xogenous variables, e.g., changes in socio-economic conditions; moves through essentially intervening variables, e.g., attitudes of sovereigns and constituency groups, and deals finally with the variable most directly affecting the policy outputs of implementing agencies, namely the commitment and leadership skill of agency officials. (p. 549)

To summarize all of the above, Sabatier and Mazmanian (1980) suggest that a statute or other policy decision seeking a substantial departure from the status quo is most likely to achieve its desired goals under the following set of conditions:

- The enabling legislation or other legal directive mandates policy has objectives which are clear and consistent (or at least provides substantive criteria for resolving goal conflicts)
- The enabling legislation incorporates a sound theory identifying the principal factors and causal linkages affecting policy objectives, as well as the changes in the behaviour of target groups (the regulated) and other conditions necessary to attain the desired goals
- The enabling legislation not only gives implementing agencies sufficient jurisdiction over the target groups and other critical areas of intervention but also structures the implementation process so as to maximize the probability that target groups will perform as desired (p. 549)

2.2 Implementation of PIIDPA

Using the framework developed by Sabatier and Mazmanian (1980) and described above, we will test Nova Scotia's *Personal Information International Disclosure Protection Act* to determine whether the act can be implemented effectively to meet the statute's objectives of protecting personal information of Nova Scotians from being disclosed to foreign governments.

The PIIDPAis designed specifically as a piece of legislation and public policy to support and protect the personal information of Nova Scotians at a time when "Canadians are increasingly concerned with the protection of personal information" (EKOS Research Associates, 2006). This statement is supported by the fact that in a pair of studies, conducted in 2005 and 2006, 71% of Canadians agreed that they feel there is less protection of their personal information than there was ten years ago (EKOS Research Associates, 2006). This result supports a dichotomy that exists around the issue of privacy laws because though 71% of Canadians feel less secure in how their personal information is protected, 74% support the need to have strong laws around the protection of their personal information. These studies conducted by EKOS Research Associates go further to determine the level of concern on the part of Canadians with regard to cross border information transfers and the *Patriot Act*. The study in 2006 suggested that information sharing across borders was of high concern to 65% of Canadians, and that Canadians highly valued the right to be notified of the transfer of their personal information, especially should the transfer take place under the guise of national security. The study also showed that though Canadians value the right to be notified, four in five respondents (84%) placed a "high importance" on the requirement that their consent be obtained should their information be disclosed. These results are supported by what the study calls an "impressive awareness of the *USA Patriot Act* and the privacy issues it raises" (EKOS Research Associates, 2006). The majority of those that claimed awareness of the Act and how it pertains to privacy said they were personally concerned about how that relates to the protection of their personal information, some 58% in this case (2006).

As far as the tractability of the problem is concerned, PIIDPA speaks directly to the current political culture in Canada surrounding the need for stronger laws for the protection of personal information, especially when there is potential for it to be disclosed to foreign governments. The causal theory behind the statute is very valid. Also, the statute speaks to a very small target group and attempts to change the behaviour of a relatively small group of public and private sector institutions, merely supporting laws that already exist and that are very effective. It could be argued, and rightly so, that the target groups are the foreign governments that could potentially demand disclosure of the personal information; the law, however, is not designed to deal with foreign governments but rather specifically with what it refers to as public bodies and private sector service providers. Within the context of current privacy legislation that already applies to both public bodies and private sector service providers, the behavioural change required for implementation to succeed is very minimal since they already operate under strong privacy laws. However, if you follow the argument that foreign governments are the

target group then there is potential for difficulties in effecting change outside of the statute's jurisdiction.

The extent to which PIIDPA as a statute coherently structures the implementation process is evident in the fact that its implementation institution is the Nova Scotia Department of Justice. The Department of Justice is a strong central agency within the provincial government. The Department of Justice holds prestige and power at the cabinet table, thus putting a strong ministry behind this statute. Placing the statute under the control of the Department of Justice, like all other privacy legislation, ensures that it will be administered by a competent group of public servants who have a long history in the administration of these types of laws. The placement of the statute within the Department of Justice also ensures that the central tenets of the Act – specifically the *protection* of personal information – are adhered to because they speak directly to the mission statement of that department, primarily that the department "is committed to the fair and effective administration of justice," and that they are, "accountable to the citizens of Nova Scotia," and will, "strive to inform the public of their activities through a policy of openness and accessibility" (Nova Scotia Department of Justice, 2006a). Also, within the Department of Justice the statute is given strong support through a very informative website that provides valuable information regarding what the scope and intent of the legislation is. The Department also provides training on legislation for those who are involved in the collection, use and/or disclosure of personal information within government departments, offices, agencies, boards and commissions. Though as of December 2007 there is no evidence that any information sessions have taken place this could change as the Act came into full effect for all municipalities in Nova Scotia as of 15 December 2007. Training might be necessary to meet a potential increase in demand (Nova Scotia Department of Justice, 2007b). The statute meets all of Sabatier and Mazmanian's sub-variables under the broader statutory variable in its ability to structure the implementation process from within the implementing institution (1980, p. 542). The statute has been assigned a dedicated staff member, namely the FOIPOP Commissioner, who is legally responsible to the minister to ensure that the act is being enforced. Finally, the statute allows for outside consultation in the form of the FOIPOP review board, which oversees all privacy laws in Nova Scotia.

The non-statutory variables affecting the implementation of PIIDPA go further to supporting strong implementation of the statute within the provincial jurisdiction. Sabatier and Mazmanian (1980) stress the importance of a statute "receiving a constant and/or periodic infusion of political support" if it is to be successful in the implementation of its statutory objectives (pp. 549-550). They also stress that there needs to be a "reservoir" of support for the statutory objectives from the "general public, interest groups, and sovereigns" (pp. 549-550). These particular points are clearly present with regard to Nova Scotia's PIIDPA particularly the support from the general public, interest groups and the state. An EKOS Research Associates poll taken in 2006 clearly states that there is a huge sense of importance placed on the

protection of personal information throughout Canada, particularly with regard to how that relates to the personal information being transferred across borders. As long as there continues to be a general concern for the protection of personal information, governments will have a reason to continue to enact and enforce legislation to provide it. The political culture supports the need to protect personal information which in turn means that politicians will continue to support laws such as Nova Scotia's PIIDPA. Following this line of argument, as long as the political culture continues to debate issues around protection of personal information, politicians will continue to support these types of laws and in turn there will be "continued support for statutory objectives among sovereigns of implementing institutions" (Sabatier and Mazmanian, 1980, p. 551).

Though the non-statutory variables are positive in relation to PIIDPA, there is definitely conflict in relation to how it will directly interact with privacy legislation at the federal and international level. There is no evidence, however, that the federal government would take steps to infringe on this provincial responsibility, especially when the objectives of the statute are supported at the federal level through existing privacy laws. However, it is possible that the objectives of the statute could be successfully implemented at the provincial level, yet at the same time be completely undermined by the statutes of foreign governments, especially those of the United States. Though as stated above, there are sizable penalties for public bodies and business that violate PIIDPA in Nova Scotia, the statute is not enforceable outside of the province.

The final stage of Sabatier and Mazmanian's framework is referred to as Dependent Variables stage in the Implementation process, commonly referred to as the "feedback loop," where the independent variables are applied to the various stages statutes must go through in order to complete the implementation process. They describe the various stages in this process as being (1) the policy outputs (decision) of the implementing agencies; (2) the compliance of target groups with those decisions; (3) the actual impacts of agency groups; (4) the perceived impacts of those decisions; and finally, (5) the political system's evaluation of a statute in terms of major revisions (Sabatier and Mazmanian, 1980, p. 553). PIIDPA has managed to advance through four of the five stages and currently the outputs or decisions of the implementing agency have not warranted any results or actions on the part of the Nova Scotia government. Since the enactment of PIIDPA in December 2006 the Minister of Justice has had no foreign disclosure requests made for access to the personal information of Nova Scotians (Personal communication, 2007). What this suggests is that at the fourth stage of Sabatier and Mazmanian's model the statute has stalled with regard to the impact of the statutes objectives. It raises the question as to whether the public concern for the protection of information, government's reactions to a potential security threat with regard to this information from foreign governments, and finally the need to protect private personal information from foreign disclosure, is a non-issue.

This goes further to raise the question as to whether foreign governments, in this case primarily the United States, are actually taking steps to respect the law of Nova Scotia and go through the process outlined in PIIDPA. These are all questions which will have to be answered when legislators review the statute and decide whether its intent was warranted and whether the statutes objectives were successfully achieved. This process will take place when the legislation comes up for review at a future date.

Conclusion

The events of 11 September 2001 set into motion a series of changes to the common law of all major countries, specifically the United States and Canada, with regards to empowering governments with the ability to investigate, prosecute and convict terrorists and terrorist groups that could be operating within their borders. In doing so these events and the laws that grew from them have caused serious implications with regards to the protection of personal information. This is especially the case with regard to the protection of personal information from foreign disclosure. Public opinion on the issue suggests a strong need for governments to deal with this issue in a serious and productive manner to ensure their citizens that their private personal information is being protected.

Nova Scotia, like British Columbia, Alberta, Ontario and Quebec, took steps to deal with what appears to be a serious issue. At the moment, governments find it extremely advantageous politically to invest resources into dealing with this issue, thus reassuring their citizens that something is being done to deal with the perceived problem.

As stated in the above Sabatier and Mazmanian's (1980) framework for policy, implementation is extremely useful in showcasing the various factors that help to ensure that Nova Scotia's law will meet its designed policy implementation objectives. The *Personal Information International Disclosure Protection Act* of Nova Scotia takes a number of constructive steps towards meeting Sabatier and Mazmanian's "minimum list of crucial conditions" that allow statutes to achieve their desired goals:

- PIIDPA functions within a legal framework of provincial and federal privacy laws that are considered by most outside observers to be strong and effective, if not the best in the world (Privacy International, 2006). It outlines clear and substantive goals and objectives for those given the task of implementing it, re-enforced by a strong and effective set of penalties.
- PIIDPA is based on a sound theory that reflects a current political culture concerned about privacy issues, particularly those dealing with foreign countries. The statute reaches a defined and manageable target group whose behaviour needs minimal changing due to their function within an already established system of laws and

regulations. The statute has support that is broad and inclusive of the general public, stake holders, politicians and the implementation agency itself.

- PIIDPA is designed to ensure that the Department of Justice can adequately enforce its objectives and also structures the implementation so that there is maximum cooperation by target groups to achieve the statutes objectives. However, by way of caveat, PIIDPA is very much limited in its effectiveness due to its inability to influence jurisdictions outside of Nova Scotia and public bodies and private sector service deliverers in those jurisdictions.

PIIDPA's success continues to rely on the ability of the government to control access to the personal information of its citizens by businesses that are subsidiaries of foreign owned parent companies. This is especially the case if those parent companies reside in countries that have deep investigative and surveillance gathering laws that conflict with PIIDPA. However, the current political culture surrounding privacy, foreign surveillance gathering and the so-called "War on Terror" is unlikely to change any time soon. We can expect to see laws like PIIDPA being passed throughout Canada at the provincial and federal levels, as long as there is potential for the security of private information to be compromised by foreign governments.

References

American Civil Liberties Union. (2007). Reform the Patriot Act, Section 215. Retrieved November 19, 2007 from http://action.aclu.org/reformthepatriotact/215.html

Associated Press, The. (2006, August 17). U.S. judge rules warrantless wiretapping unconstitutional. *International Herald Tribune*. Retrieved December 15, 2007 from Zttp://www.iht.com/articles/ap/2006/08/17/america/NA_GEN_US_ Domestic_Spying_Lawsuit.php

BC Government and Service Employees' Union v. British Columbia (Minister of Health Services). (2007). Burnaby: British Columbia Government and Service Employees Union.

BC Government and Service Employees' Union v. British Columbia (Minister of Health Services). (2004). *Submission on the Patriot Act, Submission to the Information and Privacy Commissioner for British Columbia*. Burnaby: British Columbia Government and Service Employees Union.

Brown, M. P. (1992). Organizational design as policy instruments: Environment Canada in the Canadian bureaucracy. In R. Boardman (Ed.), *Canadian Environmental Policy: Ecosystems, Politics, and Process* (pp. 24-42). Toronto: Oxford University Press.

EKOS Research Associates. (2006). Revisiting the privacy landscape a year later, submitted to the Office of the Privacy Commissioner of Canada, March 2006. Retrieved December 16, 2007 from http://www.privocom.gc.ca/information/survey/2006/ekos_2006_e.asp#section2

Furlong, M. (2007, January 28). Personal information is being protected. *The Chronicle Herald*, p. E7.

Government of Canada. (1985). *Criminal Code of Canada*. Ottawa: Author.

Government of Canada – Department of Justice. (2001). *Backgrounder: highlights of Anti-Terrorism Act*. Retrieved December 15, 2007, from http://canada.justice.gc.ca/en/news/nr/2001/doc_27787.html

Ibbitson, J. (2001, October 27). Antiterrorism bill becomes U.S. law. *The Globe and Mail*, p. A14.

Jenkins, D. (2003). In Support of Canada's Anti-Terrorism Act: A Comparison of Canadian, British, and American Anti-Terrorism Law. *Saskatchewan Law Review*, *66*, 419-454.

MacGregor, R. (2001, October 7). Jefferson's words twisted by terrorists. *The Globe and Mail*, p. A15.

Nova Scotia Legislature. (2006, July 6). Hansard: Debates and Proceedings. Halifax: Queen's Printer.

Office of the Auditor General of Nova Scotia. (2005). Electronic information security and privacy protection. *Annual Report of the Auditor General of Nova Scotia*, 31-41.

Office of the Information & Privacy Commissioner of British Columbia. (2004). Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing. Victoria: Author.

Office of the Privacy Commissioner of Canada. (2007a). Fact Sheet: Privacy Legislation in Canada. Retrieved December 16, 2007, from http://www.privcom.gc.ca/fs-fi/02_05_d_15_e.asp

Office of the Privacy Commissioner of Canada. (2007b). Fact Sheet: Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's Personal Information Protection Acts (PIPAs). Retrieved December 16, 2007, from http://www.privcom.gc.ca/fs-fi/02_05_d_26_e.asp

Patriots to Restore Checks and Balances. (2007). About Us. Retrieved November 20, 2007, from http://www.checksbalances.org/aboutus.php

Privacy International. (2006). 2006 International Privacy Survey: Ranking by Country. Retrieved December 16, 2007, from http://www.privacyinternational.org/article.shtml?cmd %5B347%5D=x-347-545269

Province of Nova Scotia. (2006). Personal Information International Disclosure Protection Act. Halifax: Author.

Province of Nova Scotia. Department of Justice. (2006). "Protection of Privacy Legislation Proclaimed", News Releases, November 15, 2006. Retrieved December 16, 2007 from http://www.gov.ns.ca/news/details.asp?id=20061115005

Province of Nova Scotia – Department of Justice. (2007a). Home page. Retrieved December 16, 2007, from http://www.gov.ns.ca/just/default.asp

Province of Nova Scotia – Department of Justice. (2007b). Privacy. Retrieved December 16, 2007, from http://www.gov.ns.ca/just/Divisions/IM/FOIPOP/Privacy.asp

Sabatier, P., & Mazmanian, D. (1980). The implementation of public policy: A framework of analysis. *Policy Studies Journal*, *8*, 538-560.

Shenon, P. (2003, July 21). Report on U.S. Antiterrorism Law Alleges Violations of Civil Rights. *The New York Times*, p. A1.

Stanley, J., & Steinhardt, B. (2007). Even Bigger, Even Weaker: The Emerging Surveillance Society – Where Are We Now? Washington, D.C.: American Civil Liberties Union.

United States – Department of Justice. (2007). Dispelling the Myths. Preserving Life & Liberty. Retrieved November 20, 2007, from http://www.lifeandliberty.gov/subs/u_myths.htm

United States Senate. (2001, October 24). H.R. 3162, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act. Washington, D.C.: Author.

Wispinski, J. (2006). The USA Patriot Act and Canada's Anti-Terrorism Act: Key Differences in Legislative Approach. Ottawa: Parliamentary Information and Research Service.