

The USA *PATRIOT* Act and Public Sector Outsourcing in British Columbia: An Overview

**Alec Szibbo
Danielle Lemon**

Introduction - A Right to Privacy

The right to privacy is a universal human right that has been enshrined in the *Universal Declaration of Human Rights*. The Supreme Court of Canada has noted that:

“Our notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit.”¹

The right to privacy allows every individual to control the flow of information about themselves to governments, corporations and other individuals. Privacy law in Canada is not primarily focused on protecting anonymity, but on protecting Canadians’ right to control their personal information, recognizing that in some instances personal information must be provided in order to gain access to essential social services.² Our privacy laws aim to protect this right by serving two functions: they protect the privacy of individuals with respect to personal information about themselves held by a government institution, by providing individuals with a right of access to that information, and they support and promotes electronic commerce by protecting personal information that is collected, used or disclosed by private organizations.

Canadian Privacy Legislation

Privacy is protected by legislation at both the federal and provincial levels, which set out the circumstances in which personal information of individuals can be collected, used and disclosed by both governments and organizations.

A. Federal Legislation

1. *Personal Information and Electronic Documents Act* (“PIPEDA”)

PIPEDA establishes rules for the management of personal information by organizations involved in commercial activities, and strikes a balance between an individual's right to the protection of personal information and the need of organizations to obtain and handle such information for legitimate business purposes. PIPEDA came into force in 3 stages beginning January 1, 2001, and as of January 1, 2004, applies to:

¹ La Forest, J., in *R v. Dymnt*, [1988] 2 S.C.R. 417 at 255-256.

² Philippa Lawson, “Finding the Balance Between Privacy and Security,” Address to Annual Conference of the Canadian Access and Privacy Association, Ottawa, November 2005.

- The collection, use and disclosure of personal information by any organization in the course of commercial activity within a province. *Note:* Provinces that have enacted legislation substantially similar to PIPEDA have obtained orders exempting them from PIPEDA's provisions and are governed by their own acts. Currently, **B.C., Alberta, and Quebec have enacted their own private-sector privacy legislation.**
- All personal information in all interprovincial and international transactions by all organizations subject to the Act in the course of commercial activities.

2. *Privacy Act*

The *Privacy Act* took effect on July 1, 1983. This Act imposes obligations on federal government departments and agencies to respect privacy rights by limiting the collection, use and disclosure of personal information. The *Privacy Act* gives individuals the right to access and request correction of personal information about themselves held by these federal government organizations.³

B. Provincial Legislation

1. *Personal Information Protection Act ("PIPA")*

PIPA came into full force on January 1, 2004, and is "substantially similar" to PIPEDA. It governs the collection, use and disclosure of personal information by any organization in the course of commercial activity within the province. Like PIPEDA and the *Privacy Act*, PIPA gives individuals a right of access to personal information about themselves held by these organizations.

2. *Freedom of Information and Protection of Privacy Act ("FOIPPA")*

FOIPPA came into force in 1993 and imposes limits on the collection, use and disclosure of personal information by provincial government public bodies, including government ministries and most government agencies, boards, commissions and Crown corporations. Like the federal *Privacy Act*, FOIPPA gives individuals a right of access to their personal information and to request the correction of personal information about themselves held by these organizations.

Balancing Security and Privacy - Conflicts Post-9/11

After the attacks on the World Trade Centre in 2001, governments across the world sought broader surveillance powers in order to identify potential terrorists and prevent further attacks. Canada passed the *Anti-terrorism Act* in 2001 which provided law enforcement officials with wider discretion to collect information and conduct surveillance. In the United States, Congress adopted the *USA PATRIOT ACT*, which amended a number of U.S. laws in order to extend the reach of FBI

³ Office of the Privacy Commissioner of Canada, "Privacy Fact Sheet," available online: Office of the Privacy Commissioner of Canada <<http://www.privcom.gc.ca>>.

and law enforcement in the collection and use of personal information. These legislative developments justified the intrusion on personal privacy in the name of national security.

The USA PATRIOT ACT and the Foreign Intelligence Surveillance Act

One of the laws amended by the *USA PATRIOT Act* was the *Foreign Intelligence Surveillance Act of 1978* (“FISA”). FISA permits electronic and physical searches for the purpose of gathering foreign intelligence information. A court established under the Act, the Foreign Intelligence Service Court (the “FIS Court”), provides the authorization for these searches in secret proceedings that are rarely published. Prior to the *PATRIOT Act*, a government agent was required to provide the “specific and articulable” facts that gave them reason to believe the person whose records they sought was a foreign power or an agent of a foreign power in order to obtain the approval of the FIS Court for a search.

The *PATRIOT Act* made several changes to FISA which broadened the net of these searches and increased their secrecy. The scope of what information could be obtained and for what purpose was dramatically increased. **Section 218** of the *PATRIOT ACT* made FISA searches easier to obtain by lowering the standard by which a FIS Court could authorize a search. Previously, foreign intelligence gathering had to be the *purpose* of the search; under the new amendment, it had to be only a *significant purpose*. “Significant” was not defined in either *FISA* or the *PATRIOT Act*, and critics were concerned that this vagueness would lead to inconsistent application of *FISA* and potential overuse; specifically, that FISA searches could be obtained for use in domestic criminal investigations, immigration or general government matters, and not in the context of foreign intelligence gathering for which they were originally intended.⁴

Before the *PATRIOT ACT*, government officials could only obtain FISA orders for certain types of information, specifically, business records held by public carriers, accommodation, physical storage or vehicle rental organizations. **Section 215** of the *PATRIOT Act* amended FISA so that the FBI could order any person or entity to disclose “any tangible thing,” so long as the FBI specified “that the order is for an authorized investigation...to protect against international terrorism or clandestine intelligence activities.” **Section 215(d)** prohibited the disclosure of a search or the names of those served with a search order, making it impossible for anyone suspecting they were the subject of a search to confirm it, and effectively eliminating any challenge to an order. The Act provided that “no person shall disclose to any other person (other than those necessary to produce the tangible things in this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.”

The FBI had long enjoyed the ability to issue a “national security letter” directly to financial institutions, phone companies and internet service providers to compel them to disclose information about their customers. Previously, the FBI was only allowed to compel the disclosure of “specific and articulable facts” from the recipient organization; **Section 505** of the *PATRIOT Act* widened the net of national security letter searches: now, the FBI could request the disclosure of information of “relevance to an authorized intelligence investigation.” A prohibition on the disclosure of such letters, similar to that imposed on FISA search orders by

⁴ Electronic Privacy Information Center, “Lowered Standards for Foreign Intelligence Surveillance,” available online: EPIC <<http://www.epic.org/privacy/terrorism/usapatriot>>.

Section 215, was also introduced. The issuance and execution of a search under the authority of a national security letter must take place in secret. In 2004, a U.S. court declared this non-disclosure provision unconstitutional, and the matter is currently under appeal.⁵

The USA PATRIOT Act in a Canadian Context: The Questions Begin

Shortly after the creation of the *PATRIOT Act*, Canadian commentators began to express their concern that the new extended reach of American surveillance powers could capture Canadians' personal information if that information was in the care or control of a US-owned organization, and that privacy rights were directly threatened by this new legislation. Thanks to the removal of many trade barriers within North America, the flow of business between Canada and the United States is stronger than ever. American companies operate subsidiaries or local offices within Canada, and may store information about Canadian customers located in central systems in the United States or at the very least controlled and accessible by U.S. offices. Further, some aspects of Canadian business may be outsourced to American service providers, placing information about Canadians squarely in the path of the *PATRIOT Act*. Could an office in the United States be served with an order requiring the production of information about Canadians within its control? Would Canadian subsidiaries of US companies have to comply with such orders?

The Issue is Raised: Enter MAXIMUS

In March 2004, the B.C. Ministry of Health Services selected MAXIMUS, Inc. ("MAXIMUS") to develop a new service model for the Medical Services Plan ("MSP") and PharmaCare.⁶ A multinational private company, MAXIMUS at that time employed over 5,000 people in 260 offices in Canada, Australia and the United States, providing business and information technology services to governments. The B.C. government planned to outsource the administration of MSP and PharmaCare to MAXIMUS; response to public inquiries, the registration of clients and the processing of individual medical and pharmaceutical claims would be entrusted to MAXIMUS as an "alternate service delivery project" aimed at increasing the efficiency and value of PharmaCare and MSP.

Almost immediately, the British Columbia Government and Service Employees Union (the "BCGEU") became concerned about the implications for British Columbians' privacy rights when sensitive health information was being outsourced to a company with a U.S. presence. The BCGEU petitioned to stop the Ministry of Health Services from contracting out the administration of MSP and PharmaCare to MAXIMUS. They argued that the outsourcing of British Columbians' personal information contravened FOIPPA by putting that information within the reach of U.S. authorities exercising the authority granted in the *PATRIOT Act*.

The Privacy Commissioner Investigates

In the spring of 2004, BC's Information and Privacy Commissioner announced that he would prepare a report on the outsourcing arrangements of the BC government to U.S.-linked service

⁵ See *Doe and ACLU v. Ashcroft*, No. 04-CIV-2614 (S.D.N.Y.) 2004.

⁶ See Ministry of Health Services' Press Release, March 31, 2004, "MSP service delivery model to improve client service," available online: Government of British Columbia <<http://www.gov.bc.ca>>.

providers. Over 500 submissions were made by interested parties in Canada, the United States and Europe over the course of the investigation. In October 2004, the Commissioner issued a 150 page report, entitled “Privacy and the USA PATRIOT Act: Implications for British Columbia Public Sector Outsourcing.” The official Report Summary is provided in Appendix 3.

The Commissioner’s Report: Concerns for British Columbians

The Commissioner’s report highlighted a number of concerns that recurred throughout the submissions process:

1. Outsourced Information Subject to Laws Where it is Stored

The widened reach of the *USA PATRIOT Act* notwithstanding, personal information, if located outside of British Columbia, would be subject to the laws that apply in the location where the information is found, regardless of any terms built into the contract to protect that information. New U.S. anti-terrorism laws demonstrate that “the scope of what are considered to be vital US national interests in ensuring national security and protecting against terrorism had grown,”⁷ and it is unclear that any Canadian laws or policies to protect personal information would overcome these strong U.S. interests.

2. Lower Threshold for FISA Orders

Before the *USA PATRIOT Act*, FISA orders could only be issued where the FBI demonstrated to the FIS Court that there were specific and articulable facts that gave reason to believe the person about whom information was sought was a foreign power or an agent of a foreign power. After the *Act*, a FISA order can be obtained by the FBI if they show that the records are sought for an authorized investigation to obtain foreign intelligence information not concerning a US person, or to protect against international terrorism or clandestine intelligence activities. A person whose information is sought no longer need be a foreign power or an agent of that foreign power. An order could now be issued for personal information of British Columbians in the “care or control” of a U.S.-affiliated company: information located in this province, at a subsidiary of a U.S. company, or located at a U.S. company through an outsourcing arrangement. The scope of the kind of information was also widened, to “any tangible thing.” There was widespread concern in the submissions received that the kind of information that can be obtained and who it can be obtained about is greatly widened under the *PATRIOT Act* and now poses a threat to Canadians’ information privacy.

3. Secrecy of Orders

FISA orders are obtained and executed in secret. If a British Columbian was the target of such an order for their personal information from a U.S. subsidiary in Canada or through an outsourcing arrangement, they would have no notice of such an order and no recourse against it.

⁷ Information and Privacy Commissioner for British Columbia, “Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing,” available online: Information and Privacy Commissioner for British Columbia <<http://www.oipcbc.org>> at 127-128.

The Commissioner was concerned about the lack of opportunity for a British Columbian to challenge such an order.

4. Searches Under Section 218

Section 218 of the *USA PATRIOT Act* widened the authority for physical searches and electronic surveillance so that foreign intelligence gathering need only be a “significant purpose” of the search or surveillance. The Commissioner was concerned that in widening the scope of searches, more opportunity would exist for British Columbians’ information, in the control of American companies, to be seized, and not just for foreign intelligence gathering, but ordinary criminal law enforcement.

5. National Security Letters Under Section 505

Section 505 lowered the threshold for these ordered to be issued directly by the FBI, and the Commissioner was concerned that, as with the searches ordered under Sections 215 and 218, National Security Letters could be used to collect personal information of British Columbians that might pass through or be stored in the U.S. without any notice or recourse for persons affected by those orders.

Commissioner’s Conclusions and Recommendations

The Commissioner made the following conclusions:

1. There were no guarantees that a U.S. court, authorizing a search or surveillance order under the *USA PATRIOT Act* for records in the care or control of a company situated in the U.S. would respect any Canadian laws set in place to protect personal information from disclosure in response to an order issued by a foreign court or authority.
2. Nevertheless, Canadian statutory provisions on privacy of personal information provide U.S. courts with a strong public policy message about the privacy of personal information of Canadian citizens.
3. Any outsourcing arrangements that affect the personal information of British Columbians should ensure that personal records are clearly made subject to FOIPPA, so that as a matter of law in British Columbia, they cannot be disclosed in response to a US court order.
4. Laws that prohibit disclosure in response to any order or request made by a foreign court or authority should have the threat of prosecution or a heavy fine attached to them, to deter them from complying with such orders and breaking BC laws.
5. A complete ban on outsourcing would not be a practical or effective way of ensuring the protection of personal information of British Columbians

BC Government's Statutory Response: Amendments to FOIPPA

FOIPPA applies to provincial government ministries and other BC public bodies. The Commissioner's report found that outsourcing *per se* did not contravene FOIPPA, but recommended stricter statutory controls on the use, collection and disclosure of personal information. On October 21, 2004, the *Freedom of Information and Protection of Privacy Amendment Act* received Royal Assent. The Act was passed in anticipation of the Commissioner's forthcoming report and introduced the following changes to FOIPPA:

1. Repeals a provision that permitted disclosure in order to comply with a subpoena, warrant or order made by a court or body with jurisdiction to compel the production of information, and makes such disclosure only permissible within Canada (Section 33.2)
2. Requires public bodies to report to the government any requests for the disclosure of personal information in response to a foreign court order or subpoena; (Sections 30.4, 33)
3. Includes "whistleblower" legislation to protect employees of companies who know of or suspect a privacy breach or attempts at foreign access and report them; (Section 30.3)
4. Requires that personal information must now only be located in and accessed from Canada, with very limited exceptions; (Section 30.1)
5. Creates fairly substantial fines for disclosure contrary to *FOIPPA*, which includes disclosure in response to a foreign court order or subpoena: a person may be charged up to \$2000, while a partnership or individual who is a service provider may be fined up to \$25,000. In the case of a corporate service provider, the fine can go up to \$500,000 (Section 74.1).

The text of these amendments to FOIPPA is provided in Appendix 4.

Government's Contractual Response: The "Master Services Agreement"

An extra layer of protection was provided by contractual arrangements in the Master Services Agreement between MAXIMUS and the BC government, which was signed November 4, 2004. Structural controls and special rights afforded to the government ensured that personal information of British Columbians would be as far removed from MAXIMUS Inc. (USA) as possible, and that there were steps the government could take under the contract to prevent or deal with the consequences of a privacy breach.

A visual representation of this corporate structure is provided in Appendix 5.

Corporate Structure and Protection Measures

A corporate structure was created by MAXIMUS that ensured that personal information of British Columbians would be as far removed as possible from the U.S. parent company, MAXIMUS Inc. MAXIMUS Canada, Inc., a federally incorporated Canadian subsidiary of MAXIMUS, owns 2 separate B.C. companies, located in Victoria, MAXIMUS BC Health Inc. and MAXIMUS BC Health Benefit Operations Inc. The boards of directors of these two

companies are all Canadian, and resident in British Columbia. Further, MAXIMUS Canada's shares in these 2 BC companies is held in trust by a British Columbia trust company, and in the event of a privacy breach or an anticipated breach, the trust company may immediately transfer temporary or permanent ownership of these 2 BC companies to the provincial government, who can take control of operations until the breach has been resolved.

The Agreement's "corporate protection measures" further ensure that the personal information of British Columbians is protected. These measures include:

- Creation and reference to a detailed privacy plan within the contract;
- Creation of privacy and security officer position by service provider, who monitors compliance with the privacy plan;
- Termination rights in the event of disclosure or a privacy breach, and
- Liquidated damages in the event of disclosure or a privacy breach in response to a requirement of a foreign country or agency.

Privacy and Security Measures

The Master Services Agreement contains many provisions to enhance the privacy and security of operations:

- Firewalls, encryption and physical security measures;
- Restrictions on data access and oversight/supervision requirements, applicable to any U.S. employees;
- Data storage, access and remote access only in Canada, and this provision can only be changed with the consent of the Province;
- Only BC service provider has access to data;
- Outbound web and e-mail access for staff prohibited or restricted, except as required to deliver services;
- Floppy drives, CD burners, USB drives and any hardware that would enable data to be copied and taken offsite restricted to designated personnel

"Operational" Measures

The Master Services Agreement outlines several operational policies that must be followed by the Service Provider to increase the security of personal information in day-to-day operations. These measures include:

- Creation of clear policies and procedures outlining privacy and security objectives, methodologies and disclosure requirements;

- Data access segregated to align with specific job requirements;
- Creation of strict records management and retention policies;
- Privacy Impact Assessments prior to any systems changes;
- Employees with access to data sign non-disclosure agreements directly with the Province which include a requirement for the signer to notify the Province in the event that they become aware of any potential disclosure; and
- Whistleblower protection and hotline for employees.

Developing Standards for the Future: Privacy Protection Measures

On October 5, 2004, the BC government issued its “Privacy Protection Measures” (the “Measures”). The Measures are non-mandatory guidelines for government entities negotiating large, long-term service contracts with U.S or U.S.-linked companies. They offer a range of technological, structural and legal strategies that can be incorporated into the contracts in order to protect personal information from the reach of the *PATRIOT Act*. Government negotiators are free to determine which measures would be most appropriately incorporated into each contract. Areas covered by the Measures include “Technology and Business Processes,” “Employee Strategies,” “Contractual Measures” and “Corporate Structure.”

Highlights of the Measures are provided in Appendix 6.

The MAXIMUS Decision

On March 23, 2005, The Honourable Mr. Justice Melvin issued his decision in the BCGEU’s bid to stop the outsourcing of MSP and PharmaCare to MAXIMUS.⁸ Mr. Justice Melvin found that, having amended FOIPPA, the BC government had done “all within its powers to control the dissemination of information” and to prevent disclosure outside of Canada and to ensure any information in the control of the government or a public body is “reasonably” secure.⁹ The Court rejected the BCGEU’s submission that the Master Services Agreement violated FOIPPA, and declined to declare the contract inoperative. It also found that the contractual provisions in the Master Services agreement, the corporate structure created by BC and MAXIMUS to protect information, and the new-and-improved FOIPPA provided “more than reasonable security” with respect to protecting the personal information of British Columbians from the *PATRIOT Act*.

Renewal of the USA PATRIOT ACT

Key provisions of the *PATRIOT Act*, including Section 215 (the provision dealing with FISA search orders) were set to expire December 31, 2005, and political debate in Washington began in earnest in the Fall of 2005 about whether the Act should be renewed or whether the expiry of certain surveillance provisions provided an important opportunity to reverse the Act and afford

⁸ The full text of the MAXIMUS decision is provided in Appendix 7.

⁹ *Ibid.*, at para 44.

further privacy protections to citizens. Early in 2005, both the Senate and the House of Representatives began a series of hearings on the Act that left Washington deeply divided.

The White House was adamant that the *PATRIOT Act* needed to be renewed in its entirety as a matter of public safety. President Bush called early in 2005 for a full renewal of the Act, commenting that “law enforcement needs this vital legislation to protect [American] citizens” from terrorist threats.¹⁰ A bipartisan group of 6 Democrat and Republican senators, led by Senator Russ Feingold (D), who had been the only senator to vote against the Act when it was originally passed in 2001, introduced a *PATRIOT Act* reform plan called the *Security and Freedom Assured (SAFE) Act*, which attempted to curb the discretion of government and law enforcement to conduct surveillance and searches by codifying standards that had been in place pre-9/11. The progress of the *SAFE Act* came to a halt when it became weighed down by debate in the committee process.

House Republicans began to push to renew the Act in November 2005 with a proposal to renew the Act in its entirety for seven years. This was met by strong opposition by both Republicans and Democrats, and Republican senators then proposed a four year extension of the law. Democrats responded with an offer to agree to a 3 month extension. A joint committee of the Senate and the House worked out a compromise that was released in a Conference Report on December 8, 2005. The Report proposed to make many provisions of the old *PATRIOT Act* permanent, but only renewed Section 215 for four years, making many changes to the section to eliminate the opportunity for misuse of the section by government and law enforcement. The Report proposed that FBI officials applying for a search order under Section 215 would be required to include a statement of facts with each application showing “reasonable grounds to believe” that what they sought was relevant to an authorized investigation into international terrorism or espionage. Recipients of FISA warrants would be permitted to consult with legal counsel and seek judicial review of the warrants. The Conference Report passed the House with strong approval on December 14, 2005 and was sent to the Senate.

Democrat senators and four Republican senators blocked the Conference Report in a filibuster, alleging that the Report did little to protect the civil liberties of citizens while granting wide unchecked powers of discretion to government and law enforcement. The White House was not impressed by this delay tactic or the filibuster backers’ proposal for a three month extension of the current Act in order to buy time for a new compromise to be reached. “No one should be allowed to block the *PATRIOT Act*,” said President Bush.¹¹ White House spokesman Scott McLellan accused Democrat senators of “putting politics before national security.”¹² Political pressure against the filibuster intensified, however by December 21, 2005, the filibuster of the Conference Report proposal had not ended. The vote stood at 52 to 48 in favour of the Conference Report, while 60 votes were needed to end the filibuster. The Senate could only agree to a six-month extension of the current *PATRIOT Act*, in order for debate and revision of

¹⁰ Declan McCullough, “Patriot Act may be renewed without reforms,” *ZDNet News*, December 7, 2005, available online: ZDNET <http://news.zdnet.com>.

¹¹ Sheryl Gay Stolberg, “Senate agrees to six-month extension of Patriot Act,” *New York Times* December 22, 2005, available online: New York Times <<http://www.nytimes.com>>.

¹² Declan McCullagh, “Bush ratchets up Patriot Act pressure,” *CNet News*, December 21, 2005, available online: CNet News.com <<http://news.com.com>>.

the law to continue. President Bush agreed to sign the 6 month extension and the law went back to the House for approval.

House leaders, who had already shut down the House and left Washington for the holidays, condemned the filibuster against the Conference Report and refused to accept the six-month extension. On December 22, the House proposed a one month extension of the Act to prevent the sunset provisions of the Act from expiring on December 31, 2005, in the hope that Senators would be able to end the filibuster against the Conference Report in the new legislative session in January. On the evening of December 22, 2005, Senate Bill 2167 was passed, extending the sunset provisions of the *PATRIOT Act* for five weeks. These controversial provisions of the Act, including Section 215, were set to expire on February 3, 2006.

The Act went before Congress for debate on January 31, 2006. Senators were still demanding revisions to the proposed amendments contained in the Conference Report in the wake of their December filibuster, and supporters of the Act were standing firmly behind the proposed changes which would make the surveillance provisions of the Act permanent. This meant the most likely action would be another short-term extension of the Act in order to allow both sides to resolve their issues surrounding the controversial surveillance provisions of the legislation.

Before the bill containing the Conference Report was tabled to be placed before Congress, Senator Arlen Specter (R.-Pa.), Chairman of the Senate Judiciary Committee, announced an addition had been made to the bill that would permit demonstrators at “any special event of national significance” to be taken to jail on felony charges if they are caught “knowingly or willingly” breaching a security perimeter, regardless of whether the President or any other official normally protected by the Secret Service is present and threatened by the infraction. This controversial addition generated more controversy amongst privacy advocates, which placed the possibility of a renewal before the deadline in jeopardy. Jeff Lungren, spokesman for House Judiciary Committee Chairman James Sensenbrenner (R.-Wis), said that the most realistic expectation was a short-term extension of the Act, as there was no time for a prolonged debate before the legislation expired, and indeed, on February 1, 2006, the Act was renewed in its entirety until March 10, 2006.

Conclusion

In providing public services, governments must balance efficiency with privacy and security. The Commissioner’s Report and the MAXIMUS decision generated considerable dialogue about the standard of privacy and security with which citizens expect governments to protect their personal information. Future amendments to the *USA PATRIOT Act* could bring a new round of debate about how to protect the personal information of Canadians while taking advantage of outsourcing opportunities in the global market.