CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC

Submission on the *USA Patriot Act*

and its impact on the privacy of B.C. citizens' personal information in the context of government outsourcing of data administration

made to the British Columbia Privacy Commissioner

August 2, 2004

Canadian Internet Policy and Public Interest Clinic (CIPPIC)
University of Ottawa
Ottawa, Ontario, Canada

www.cippic.ca

TABLE OF CONTENTS

Executive Summary

In response to planned outsourcing by the British Columbia government of certain database administrative duties to a U.S.-linked company, the British Columbia Privacy Commissioner invited public input by August 6, 2004 on the following questions:

1. Does the *USA Patriot Act* permit U.S.A. authorities to access personal information of British Columbians that is, through the outsourcing of public services, in the custody or under the control of U.S.-linked private sector service providers? If it does, under what conditions can this occur?

2. If it does, what are the implications for public body compliance with the personal privacy protections in the *FOIPPA*? What measures can be suggested to eliminate or appropriately mitigate privacy risks affecting compliance with the *FOIPPA*?

Based on its analysis of relevant law, CIPPIC is of the view that:

1. Sections 215 and 505 of the *USA Patriot Act* can be used by U.S. law enforcement officials to obtain records, indeed entire databases, from U.S.-linked organizations operating in Canada, as long as the records sought pertain to an investigation to obtain foreign intelligence information or to protect against international terrorism or clandestine intelligence activities. Such information could include health, financial, and other sensitive personal information about Canadian citizens, regardless of existing agreements or applicable data protection laws. Section 505 permits access to financial, telecommunications, and credit records in the possession of U.S.-linked service financial, telecommunications and credit service providers, while s. 215 permits access to any records from any type of organization. Neither provision has a "reasonable or probable grounds" test for ordering production of the information, and both place gag orders on organizations that are subject to the orders. Standards for granting these orders are lower for data about non-U.S. persons than for data about U.S. persons.

It should be noted that even prior to the *USA Patriot Act*, U.S. authorities could access Canadians' personal information in the custody or control of U.S.-linked organizations via National Security Letters and *FISA* orders (as well as Grand Jury subpoenas). The *USA Patriot Act* amendments merely broadened the scope and lowered the standard for the issuance of such orders. Thus, even if the *USA Patriot Act* is repealed, there will remain serious issues involving unauthorized access by U.S. authorities to Canadians' personal data.

2. The B.C. *FOIPPA* requires that public bodies ensure that personal information under their control is disclosed only in specific listed circumstances. Only one of these circumstances applies in this case: that permitting disclosure in accordance with an international treaty. However, the treaty in question applies to a narrower range of disclosures than does the *USA Patriot Act*, can be overridden by mutual agreement of the parties, and is merely a first step requirement, such that the USA can always revert to other procedures, including *Patriot Act* orders, if the treaty route is unsuccessful.

The *BCFOIPPA* further requires that the heads of public bodies protect personal information under their control "by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal."[1] The Minister must therefore ensure that the data in question is not disclosed to U.S. authorities for foreign intelligence or other purposes except as permitted via the treaty process, which must be in accordance with Canadian law. He or she must also make "reasonable security arrangements" to protect against such disclosure.

Given that any personal data in the possession of U.S.-linked organizations could be accessed by U.S. authorities for law enforcement purposes under the *Patriot Act*, "reasonable security arrangements" under *FOIPPA* would necessarily include not outsourcing database administration to U.S.-linked organizations. Less restrictive security arrangements, such as contractual obligations requiring companies to whom data processing has been outsourced to keep all data in Canada, prohibiting disclosure of personal information to affiliates, and requiring notice in the event that a production order is received from a foreign court or body might have a mitigating effect, but would not positively ensure against disclosure by U.S.-linked companies in response to *USA Patriot Act* orders.

****

While this submission focuses on the B.C. government's obligations with respect to outsourced data and privacy protection, all Canadian governments face the same issue. CIPPIC commends the B.C. Privacy Commissioner on undertaking this public consultation. All jurisdictions in Canada should be conducting similar inquiries.

It should also be noted that the privacy issue raised by the B.C. Privacy Commissioner is much larger than might appear, and cannot be resolved by a moratorium on government outsourcing alone. A great deal of Canadians' personal information is already in the hands of private sector companies with U.S. links, and is therefore equally vulnerable to access by U.S. authorities under the *USAPatriot Act* and other statutory mechanisms. Although these companies are, for the most part, subject to *Personal Information Protection and Electronic Documents Act* ("PIPEDA") as a result of their status as federally regulated industries or their interprovincial activities, any PIPEDA obligations are unlikely to hold the same force as *USA Patriot Act* orders. Thus, even if governments take effective steps to keep personal information under their control from access by U.S. authorities (as they should), this will solve only part of the problem.

The time is ripe for a public debate on this issue, based on a thorough study of the extent to which Canadians' personal information is collected, stored, used and shared via private sector databases, and the extent to which this information is accessible by foreign governments.

[1] *FOIPPA*, *supra*, note 4, s. 30.

I. Background

President Bush signed the *USA Patriot Act* into law six weeks after the attacks of September 11, 2001, on October 26, 2001.[2] The Act is 342 pages long, makes amendments to over 15 different statutes, and grants many changes to investigative and criminal laws long sought after by the Department of Justice. The Act gives federal officials greater authority to collect and share evidence for both law enforcement and foreign intelligence purposes, creates new federal crimes, and increases the penalties for existing federal crimes. While John Ashcroft, the Attorney General of the United States, stated that the *USA Patriot Act* reflects modest and incremental changes in the law, human rights organizations, such as the American Civil Liberties Union (ACLU), have raised civil liberties concerns about the Act, and have questioned the lack of judicial and congressional oversight of law enforcement actions authorized under the Act.[3]

The *USA Patriot Act* has also raised concerns in Canada, particularly in British Columbia where the Government and Service Employees Union (BCGEU) has challenged the proposed outsourcing of administrative duties associated with the British Columbia Medical Services Plan (MSP) to U.S.-linked organizations.[4] British Columbia's *Freedom of Information and Protection of Privacy Act* (*FOIPPA*) requires that public bodies protect personal information in their custody or control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.[5] BCGEU claims that the outsourcing of administrative duties associated with the MSP could lead to the disclosure of personal health information of British Columbia residents to U.S. authorities. Specifically, the BCGEU claims that the *USA Patriot Act* could be used to compel U.S.-linked corporations to disclose personal information about BC citizens to U.S. authorities for counter-terrorism and foreign intelligence purposes, in violation of contractual agreements and Canadian privacy laws.[6]

---

[2] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (U.S.A PATRIOT ACT) Act of 2001*, Public Law 107-56, 115 Stat. 272 (2001) [*USA Patriot Act*]. The *USA Patriot Act* is a merger of two similar bills. The Senate passed S.1510 (*U.S.A Act*) on October 11, 2001, and the House passed H.R. 2975 (*Patriot Act*) the following day. The differences between the bills were resolved in H.R. 3162 (*USA Patriot Act*), which was passed by the House (357-66) on October 24, and approved by the Senate (98-1) the same day. The *USA Patriot Act* was signed by President Bush on October 26, 2001.

[3] The ACLU filed a constitutional challenge on July 30, 2003, claiming that "section 215 violates the First, Fourth and Fifth amendments to the U.S. Constitution." More information regarding this action is available at http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12126&c=207. See also www.epic.org/privacy/terrorism/usapatriot/ .

[4] By "U.S.-linked organization", we mean an organization with a physical presence in the U.S., either directly or via an affiliate, or an organization engaging in continuous and systemic activities in the U.S.

[5] *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165 [*FOIPPA*].

[6] The BCGEU has applied for (1) a declaration that the contracting out of services as proposed in the Joint Solution Request for Proposal issued by the Minister of Health Services on July 29, 2003 is *ultra vires*; (2) an Order quashing any contracts or agreements which involve the contraction out of duties or powers listed in s. 5(1) of the *Medicare Protection Act*; and (3) an Order quashing any contacts or agreements which involve the disclosure of personal information to either of the proponents. A complete copy of the BCGEU

On May 28, 2004, the Information and Privacy Commissioner for British Columbia declared his intent to examine issues relating to the *USA Patriot Act* and British Columbians' personal information affected by the outsourcing of public services to U.S.-affiliated private sector service providers.[7] In examining these issues, the Privacy Commissioner requested submissions addressing the following questions:

1. Does the *USA Patriot Act* permit U.S.A. authorities to access personal information of British Columbians that is, through the outsourcing of public services, in the custody or under the control of U.S.-linked private sector service providers? If it does, under what conditions can this occur?

2. If it does, what are the implications for public body compliance with the personal privacy protections in the *FOIPPA*? What measures can be suggested to eliminate or appropriately mitigate privacy risks affecting compliance with the *FOIPPA*?

CIPPIC's responses to these questions, and accompanying analysis, are provided below.

II. Does the *USA Patriot Act* permit U.S. authorities to access personal information of British Columbians?

(a) Section 215 of the *USA Patriot Act*

Section 215 of the *USA Patriot Act* amends the *Foreign Intelligence Surveillance Act* (*FISA*) and expands the powers of law enforcement authorities to conduct searches.[8] Prior to the enactment of *FISA* and the *USA Patriot Act*, law enforcement authorities were generally required to show probable cause that a crime had been or was being committed in order to obtain a warrant from a judge or magistrate before conducting certain types of surveillance or a search.[9] *FISA*, enacted in 1978, provided an exception to that rule in respect of agents of a foreign power suspected of being engaged in

---

petition is available at: http://www.righttoprivacycampaign.com/keydocs/KeyDocuments/BCGEU_PDF/BCGEU%20Petition%20for%20Injuction.pdf.

[7] A copy of the Request for Submissions is available on the website of the Office of the Information and Privacy Commissioner for British Columbia at: http://www.oipcbc.org/new/21120publicinvite.pdf.

[8] *Foreign Intelligence Surveillance Act of 1978*, Pub. L. No. 95- 511, 92 Stat. 1783 (codified as amended at 50, U.S.C. § 1801-1862) [*FISA*]. While the *USA Patriot Act* contains a sunset provision that states section 215 "shall cease to have effect on December 31, 2005," there have been attempts by the Bush administration to reintroduce section 215 as a permanent measure. See Charles Lane "U.S. May Seek Wider Anti-Terror Powers" *The Washington Post* (8 February 2003).

[9] These requirements are codified in the Fourth Amendment of the *U.S. Constitution* which protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," and states that no warrants shall be issued, "but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The precise meaning of "probable cause" is somewhat uncertain. The often cited definition from *Draper v. United States* (1959), 358 U.S. 307, defines probable cause as where the known facts and circumstances, of a reasonably trustworthy nature, are sufficient to justify a man of reasonable caution or prudence in the belief that a crime has been or is being committed.

espionage or international terrorism.[10] Prior to the *USA Patriot Act* amendments, applications under *FISA* were granted on the certification of a law enforcement official that (a) the "purpose of the surveillance [was] to obtain foreign intelligence information," and that (b) on the basis of the facts submitted, there existed "probable cause to believe that the target [was] a foreign power or an agent of a foreign power."[11] While originally limited to electronic surveillance, *FISA* was expanded to permit covert physical entries and pen/trap orders in 1994 and 1998, respectively.[12]

The Act also established a special court, the Foreign Intelligence Surveillance Court, to review government applications for the surveillance and/or search of agents of a foreign power. Unlike traditional applications for warrants, Foreign Intelligence Surveillance Court proceedings, records, and orders are classified (held in secret). Applications for surveillance and/or searches under *FISA* are nearly always approved without modification; between 1978 and 2003, the Foreign Intelligence Surveillance Court heard over 14,000 applications and approved all but five without modification.[13]

Section 215 of the *USA Patriot Act* amended *FISA* to allow the Director of the FBI, or a designee of a rank not lower than Assistant Special Agent in Charge, to:[14]

> [M]ake an application [to the Foreign Intelligence Surveillance Court] for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information[15] not concerning a United States person or to

---

[10] *Supra*, note 9, § 1805(a)(3)(A).

[11] *FISA*, *supra* note 9, § 1804(a)(7) and 1805(a)(3)(A). The criteria differed slightly if the target was a U.S. person in that there needed to be probable cause to believe that the individual's activities involved or "may involve a violation of the criminal statutes of the United States." This probable cause could not be based solely upon "activities protected by the first amendment to the Constitution of the United States;" see *FISA*, *supra* note 9, § 1801(b)(2) and 1805(a)(3)(A).
In addition to the amendments discussed in the body of this text, the *USA Patriot Act* also lowered the threshold at which law enforcement could apply to conduct surveillance and/or searches by amending *FISA* to allow surveillance and/or searches where the significant purpose, rather than primary purpose, of the investigation is to obtain foreign intelligence information; see *USA Patriot Act*, *supra* note 1, § 218.

[12] Pen/trap orders allow the use of trap and trace devices and pen registers to secretly monitor the source and destination, but not the content, of communications made by a particular communication device.

[13] *FISA* requires that the Department of Justice report to congress the number of applications sought, approved, and rejected by the Foreign Intelligence Surveillance Court. Copies of these reports are available online at: http://www. fas.org/irp/agency/doj/fisa.

[14] *USA Patriot Act*, *supra* note 1, § 215(a)(1). The first amendment to the United States Constitution provides that **"**Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."

[15] "Foreign intelligence information" is defined as: (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United

> protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

Such applications are to be granted as long as minimal conditions are met:[16]

> Upon an application made pursuant to this section, the judge shall enter an *ex parte* order as requested, or as modified, approving the release of records if the judge find that the application meets the requirements of this section.

Those requirements are as follows:[17]

(a)(2) An investigation conducted under this section shall--
> (A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and
> (B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(b) Each application under this section--
> (1) shall be made to--
> > (A) a judge of the court established by section 103(a); or
> > (B) a United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and
>
> (2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) to protect against international terrorism or clandestine intelligence activities.

Similar to past *FISA* provisions, applications made under the *USA Patriot Act* amendment do not require law enforcement authorities to show probable cause that a crime has been or is being committed in order to obtain authorization to conduct a search. However, in contrast to past *FISA* provisions, the *USA Patriot Act* amendment focuses not on individuals, but rather on tangible things, and no longer requires that there exist "probable cause to believe that the target is a foreign power or agent of a foreign power."[18]

While this difference may be subtle, the effect is dramatic. Taken together, the lack of a probable cause requirement and the shift in focus from surveillance and/or search of individuals to production of tangible things allows the U.S. government to engage in large-scale fishing expeditions. It authorizes U.S. law enforcement officials to obtain entire databases of information from any organization, as long as sought for an investigation to obtain foreign intelligence information about non-U.S. persons or to protect against international terrorism or espionage.

States person is necessary to (A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States: *FISA*, *supra*, note 9, §1801(e).

[16] *Ibid.*, § 215(c)(1).

[17] *Ibid.*

[18] *FISA*, *supra* note 9, § 1804(a)(7) and 1805(a)(3)(A).

Under section 215, law enforcement agencies can collect and match information from a wide range of organizations, such as libraries,[19] political organizations, insurance agencies, internet service providers (ISP), and hospitals, in order to search for clues or anomalies suggestive of terrorist activities.[20] For example, a law enforcement agent may choose to serve a section 215 order on a library to obtain a list specifying members who had checked out a certain book in the last two years, and then serve a similar order on an ISP to obtain copies of emails sent and received an individual appearing on the list obtained from the library.

Organizations served with section 215 orders are required to disclose the requested documents or face the possibility of potentially severe penalties. While the Act does not itself set out penalties for the failure to comply with a section 215 order, the refusal to follow a judicial order in the United States constitutes contempt of court and is punishable by "fine or imprisonment" at the discretion of the Court.[21]

Moreover, s. 215 orders come with "gag orders," prohibiting targeted organizations from disclosing to anyone else that law enforcement officials have "sought or obtained tangible things" under section 215.[22] Thus, individuals who have had their personal information disclosed to law enforcement officials are unlikely ever to be informed of the disclosure.

(b) Section 505 of the *USA Patriot Act*

Section 505 of the *USA Patriot Act* amends three other U.S. statutes: the *Electronic Privacy Act*, the *Right to Financial Privacy Act*, and the *Fair Credit Reporting Act*.[23] The amendments give greater flexibility for government officials to issue National Security Letters (NSLs) to obtain phone, financial, and credit records for investigations "to protect against international terrorism or clandestine intelligence activities."[24] NSLs, the equivalent of administrative subpoenas, can be issued by specified U.S. law enforcement officials to order the disclosure of certain confidential records from wire or electronic communication service providers, financial institutions, and consumer reporting

---

[19] While it was originally uncertain whether the government could access information held by libraries and bookstores, Attorney General John Ashcroft confirmed in his testimony before the House Judiciary Committee on June 5, 2003 that the FBI could use section 215 to obtain records held by organizations such as libraries, and bookstores.

[20] The FBI already compiles data from selected federal agencies as well as state, local, and federal law enforcement agencies in an attempt to "identify foreign terrorists or U.S. citizens connected to foreign terrorists. A recent report issued by the General Accounting Office revealed that federal agencies are engaged in at least 131 data mining projects. A copy of the report is available at: http://www.gao.gov/new.item/d04548.pdf.

[21] 18 U.S.C. § 401.

[22] *Supra* note 1, § 215(d). Specifically, the section mandates in subsection (d) that: "[n]o person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section."

[23] *Electronic Privacy Act*, 18 U.S.C. § 2709; *Right to Financial Privacy Act*, 12 U.S.C. § 3401-3422; *Fair Credit Reporting Act*, 15 U.S.C. § 1681 – 1681(u).

[24] *Ibid.*

agencies.[25] Organizations served with NSLs are prohibited from disclosing to any person that the FBI has sought or obtained access to any information or records.[26]

Prior to the *USA Patriot Act* amendments, only the "Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director" could issue these letters. The *USA Patriot Act* amendments allow NSLs to be issued as well by the "a Special Agent in Charge in a Bureau field office designated by the Director."[27] In other words, a greater number of individuals are now authorized to compel the disclosure by private documents of documents and records containing personal phone, financial, and credit information.

The *USA Patriot Act* also broadens the circumstances under which NSLs can be issued. Prior to the section 505 amendments, an FBI official was required to certify (1) that the information sought was related to a foreign power, foreign agent, or individual engaged in terrorism or espionage, and (2) that there were "specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power."[28] The *USA Patriot Act* amendments altered these requirements to allow NSLs, like s.215 orders, to be issued merely upon the certification that the "records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States."[29]

Because of the secrecy surrounding NSLs, we don't know the extent to which they have been used by the U.S. government to obtain documents containing the personal information of Canadians from U.S.-linked organizations. However, there is nothing to suggest that NSLs cannot be used by the U.S. government to obtain phone, financial, and credit records pertaining to Canadians from U.S.-linked organizations, especially where the information is easily accessible to companies in the U.S. Like s. 215 orders, NSLs are

---

[25] Financial institutions mean any "bank, savings bank, [organizations that issue credit cards], industrial loan company, trust company, savings associations, building and loan, or homestead association (including cooperative banks), credit union, or consumer finance institution, located in any State or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, or the Virgin Islands," 12 U.S.C. § 3401.

[26] *Electronic Privacy Act*, *supra* note 24, § 2709(c); *Right to Financial Privacy Act*, *supra* note 24, § 3414(a)(5)(D); *Fair Credit Reporting Act*, *supra* note 24, § 1681(d).

[27] *Supra*, note 1, § 505.

[28] *Electronic Privacy Act*, 18 U.S.C. § 2709(b) [as amended 5 January 1999]. The *Right to Financial Privacy Act*, and the *Fair Credit Reporting Act* contain similar requirements; see 12 U.S.C. § 3414(a)(5) [as amended 23 January 2000], and 15 U.S.C. § 1681(u) [as amended 23 January 2000].

[29] *Electronic Privacy Act*, *supra* note 24. Similar to above, although the wording of each Act varies slightly, the effect of each provision, in our opinion, is the same. For example the amendment to *Right to Financial Privacy Act* requires that the "records are sought for *foreign counter intelligence purposes* to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States; *supra* note 24 § 3414(a)(5). See also *Fair Credit Reporting Act*, *supra* note 24, § 1681(u).

issued without any requirement for reasonable and probable cause, they can compel disclosure of entire databases of information, and they focus on the production of records rather than searches of individuals.

It should be noted that, while NSLs can currently only be used to obtain access to certain records held by communication, financial, and credit reporting agencies, President Bush has pushed for additional amendments that would allow NSLs to be issued for ISPs, credit card companies, libraries, hospitals and a range of other organizations.[30] If these amendments receive approval, it could mean that U.S. law enforcement officials have secret access to an even wider range of Canadians' health and other personal information held by U.S.-linked organizations, via FBI-issued NSLs.

(c) Jurisdiction of U.S. court orders and National Security Letters

The US can establish jurisdiction over an organization as long as the organization has a physical presence in the U.S., conducts "continuous and systematic" activities in the U.S., or "purposefully avails" itself of the privilege of conducting business in the U.S.A.[31] U.S. court orders can be enforced against foreign corporations as long as the company has assets in the U.S. or has U.S. customers with payment obligations. Thus, any Canadian or other company with U.S.-links is potentially subject to *FISA* orders, and would be required to comply without challenge or even disclosure of the event.

However, the *Mutual Legal Assistance in Criminal Matters Treaty* (*MLAT*) between Canada and the U.S. places an obligation upon both countries when "seeking to obtain documents, records or other articles known to be located in the [other country's] territory" to "request assistance pursuant to the provisions of [the] Treaty."[32] The Treaty requires that each country make best efforts to execute requests from the other, in accordance with its own laws. Thus, in matters involving the investigation, prosecution or suppression of offences, the U.S. is required under this treaty to submit requests for information known to be located in Canada to Canadian authorities for execution via Canadian courts, before attempting to make or enforce the order unilaterally.

As discussed below, the effect of the *MLAT* on *USA Patriot Act* orders is unclear. First, some – possibly many - *Patriot Act* orders may fall outside the scope of the *MLAT*, since they need not be related to any specific offence. Second, the *MLAT* can be overridden by other arrangements between the two countries. Arrangements for mutual assistance

---

[30] See Eric Lichtblau and James Risen "Broad Domestic Role Asked for C.I.A. and the Pentagon" *The New York Times* (2 May 2003), online: New York Times <http://www.nytimes.com/2003/05/02/international/worldspecial/02 TERR.html>.

[31] *International Shoe Co. v. Washington*, 326 U.S. 310 (1945) [*Shoe*]; *Helicopteros Nationales de Columbia, S.A. v. Hall*, 466 U.S. 408 (1984).

[32] *Treaty between the Government of Canada and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters (with Annex)*, Canada/United States (January 24, 1990) 1990 Canada Gazette Part I, p. 953 [*MLAT*]. The Act stipulates that "[a]ssistance shall include: (a) examining objects and sites; (b) exchanging information and objects; (c) locating or identifying persons; (d) serving documents; (e) taking the evidence of persons; (f) providing documents and records;(g) transferring persons in custody; (h) executing requests for searches and seizures." *MLAT*, Article II(2).

beyond the *MLAT* in the more recent war against terrorism are likely. Third, the *MLAT* merely sets out a first step that must be taken; it does not prohibit the requesting country from pursuing other methods of compelling disclosure of the documents. In other words, the treaty requires that the U.S. request the assistance of the Canadian government when seeking documents or records that are held within Canada. However, if Canada refuses to assist the U.S. in compelling the disclosure of the documents or records, there is nothing to prevent the U.S. from attempting to exercise its own jurisdiction.

Due to the classified nature of Foreign Intelligence Surveillance Court and NSL proceedings and records, it is impossible to know whether there have been any orders commanding the production of documents held by U.S.-linked organizations operating in Canada. However, American case law dealing with judicial orders for the production of documents held by foreign affiliates of U.S. corporations suggests that just because documents are situated in a foreign country does not bar their production as long as the documents are within the organization's custody or control.[33]

For example, in *Ssangyong Corporation v. Vida Shoes International Inc.*, the New York Southern District Court ordered the disclosure of the defendants' bank records from the Shanghai Commercial Bank (SCB).[34] SCB had offices located in New York, but the required records were located at their Hong Kong headquarters. The New York branch of SCB argued that they could not be compelled to disclose the documents because (1) they did not have the requisite control over the documents to disclose them to the plaintiff; and (2) Hong Kong common law relating to bank secrecy prohibited the production of the documents. In response to the first argument, the Court in *Ssangyong* reiterated that 'control' does not require that a party have legal ownership or actual possession of the documents, but rather that the party has the right, authority, or practical ability to obtain the requested documents.[35] That the bank would have access to the documents for purposes of dealing with consumer accounts or to protect itself in litigation was sufficient to demonstrate the required control over the requested documents.

In response to the second argument, the Court concluded that the production of documents in a civil action for fraud, conversion, unjust enrichment, and fraudulent transfer outweighed the interests protected by the Hong Kong common law concerning bank secrecy. The Court also suggested that the interest in disclosing the documents would be greater had the United States government had a stake in their disclosure.[36]

---

[33] See *Hunter Douglas, Inc. v. Comfortex Corp*., 1999 U.S. Dist. LEXIS 101 (S.D.N.Y.1999); *United States v. Chase Manhattan Bank, N.A. and F.D.C. Co. Ltd.*, 584 F.Supp. 1080, 1085 (S.D.N.Y. March 1984).

[34] 2004 WL 1125659 (S.D.N.Y. May 2004) [S*sangyong*]. District Courts have the authority to order the production of documents under 18 U.S.C. § 3102.

[35] *Ibid*., at page 3.

[36] *Ibid*., at page 10-11. A similar conclusion was reached in *Minpeco, S.A. v. Conticommodity Services, Inc.*, 116 F.R.D. 517 (S.D.N.Y.1987) where the Court stated that "the interest of the United States in criminal and civil enforcement suits is normally greater than its interest in private disputes."

Given that the U.S. Court was willing to order the disclosure of documents held in another country and protected by that country's privacy laws in a suit between private litigants, it is likely that the Foreign Intelligence Service Court, which nearly always approves government applications without modification, would order the disclosure of documents held by Canadian affiliates of U.S. corporations for an investigation by U.S. law enforcement authorities under the *USA Patriot Act*.

Because they are not court orders, it is not clear whether, or to what extent, National Security Letters can be enforced against foreign organizations operating in the U.S., or against U.S. organizations regarding data held outside the U.S. However, if a court order is needed for enforcement purposes, an NSL could simply be made the subject of a *FISA* court order under s. 215 of the *USA Patriot Act* and enforced as such.

(d) Conclusion re: impact of *USA Patriot Act*

Sections 215 and 505 of the *USA Patriot Act* can be used by U.S. law enforcement officials to obtain records, indeed entire databases, from U.S.-linked organizations operating in Canada, as long as the records sought pertain to an investigation to obtain foreign intelligence information or to protect against international terrorism or clandestine intelligence activities. Such information could include health, financial, and other sensitive personal information about Canadian citizens, regardless of existing agreements or applicable data protection laws. Section 505 permits access to financial, telecommunications, and credit records in the possession of U.S.-linked service financial, telecommunications and credit service providers, while s. 215 permits access to any records from any type of organization. Neither provision has a "reasonable or probable grounds" test for ordering production of the information, and both place gag orders on organizations that are subject to the orders.

It should be noted that even prior to the *USA Patriot Act*, U.S. authorities could access Canadians' personal information in the custody or control of U.S.-linked organizations via National Security Letters and *FISA* orders (as well as Grand Jury subpoenas). The *USA Patriot Act* amendments merely broadened the scope and lowered the standard for the issuance of such orders. Thus, even if the *USA Patriot Act* is repealed, there will remain serious issues involving unauthorized access by U.S. authorities to Canadians' personal data.

III. What are the implications for public body compliance with the *BC Freedom of Information and Protection of Privacy Act?*

(a) British Columbia's *Freedom of Information and Protection of Privacy Act*

One of the stated purposes of British Columbia's *Freedom of Information and Protection of Privacy Act* (*FOIPPA*) is to protect personal privacy by "preventing the unauthorized collection, use or disclosure of personal information by public bodies."[37]

Personal information is defined in the Act as "recorded information about an identifiable individual," a definition that would most certainly include records associated with the administration of the British Columbia Medical Services Plan (MSP).[38]

A "public body" is defined in the Act as:[39]

> [A] ministry of the government of British Columbia, an agency, board, commission, corporation, office or other body designated in, or added by regulation to, Schedule 2, or a local public body, [but not] the office of a person who is a member or officer of the Legislative Assembly, or the Court of Appeal, Supreme Court or Provincial Court.

The Ministry of Health Services clearly falls within the meaning of a "public body" for the purposes of the Act.

The term "unauthorized" is not defined in the Act; however, the term 'authorized' appears throughout the Act and, in each instance, the Act identifies the source of the authorization as an Act, a regulation, the data subject, or the Commissioner.[40] It is a basic principle of statutory interpretation that words are given the same meaning throughout a statute.[41] Considering the context of the Act as a whole and its purposes, it can be presumed that the term "unauthorized," where not otherwise stated, means not authorized under *FOIPPA*, or, at most, not authorized under Canadian law more generally.[42]

---

[37] *Supra* note 4, s. 2(d). Emphasis added.

[38] *Ibid*., Schedule 1.

[39] *Ibid*.

[40] For example, section 12(3) of the Act states that:

> The head of a local public body may refuse to disclose to an applicant information that would reveal (b) the substance of deliberations of a meeting of its elected officials or of its governing body or a committee of its governing body, if an Act or a regulation under this Act authorizes the holding of that meeting in the absence of the public. Emphasis added.

See also section sections 15(3), 22(4), 26, 27(1), 33, 42(1), 43, 47, 55, and 77.

[41] *R. v. Zeolkowski*, [1989] 1 S.C.R. 1378 at 1387. See also Ruth Sullivan. *Statutory Interpretation.* (Toronto: Irwin Law, 1997) ch. 4.

[42] References in Canadian statutes to "Acts" and "regulations" presumably refer to Canadian statutes and regulations, unless otherwise stated.

(i) Permitted Disclosures under *FOIPPA*: section 33

Section 33 of *FOIPPA* prescribes that personal information in "the custody or under [the] control" of a public body may be disclosed only under specific circumstances.[43] Information collected by the Ministry of Health Services for the purposes of administering the MSP, but in the custody of a third party to whom these duties have been outsourced, remains under the control of the Ministry of Health Services; the Ministry remains responsible for the data, and exercises control through the outsourcing contract. Moreover, any other interpretation would be absurd, in that if personal information outsourced by a public body to a third party was not considered to remain under the control of the public body, *FOIPPA* obligations could be easily avoided through the simple act of outsourcing.

The Act authorizes non-consensual disclosure of personal information in the "custody or under [the] control" of a public body in a number of specified circumstances, two of which are potentially applicable here.[44] The first possible exception allows for the disclosure of personal information by a public body:[45]

> for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of information.

This raises the question: does the U.S. have jurisdiction to compel the production of information from Canadian governments? Under the doctrine of state immunity, U.S. courts, including the Foreign Intelligence Surveillance Court, do not have jurisdiction to compel Canadian government bodies to produce or disclose information.[46] Hence, if the information were not outsourced by the B.C. government, it would be out of reach of the *USA Patriot Act.*

The second possible exception allows for the disclosure of personal information by a public body:[47]

---

[43] *Ibid*., s. 33.

[44] The two other circumstances under which *FOIPPA* allows the disclosure of personal information to law enforcement agencies are (1) "if the public body disclosing the information is a law enforcement agency and the information is disclosed to another law enforcement agency in Canada or to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority," and (2) if one public body is disclosing to another "public body or a law enforcement agency in Canada if the information is required to assist in an investigation undertaken with a view to a law enforcement proceeding, or from which a law enforcement proceeding is likely to result." *FOIPPA*, *supra*, note 4, ss. 30(o) and s. 30(n). Emphasis added.

[45] *Ibid*., s. 30(e).

[46] The doctrine of state immunity flows as a corollary of the principal of the sovereign equality of states; that is that all states are equal under international law. The doctrine of state immunity rests upon two principals: (1) that entities of equal standing cannot have their disputes settled in the courts of one of them, and (2) a duty of non-intervention in areas of exclusive jurisdiction of other states: Ian Brownlie, *Principles of Public International Law*, 6th Ed., (New York: Oxford University Press, 2003) at 323. See also John Currie, *Public International Law* (Toronto: Irwin Law Inc., 2001) at 317.

[47] *FOIPPA*, *supra*, note 4, s. 30(d.1)

> in accordance with a provision of a treaty, arrangement or agreement that (i) authorizes or requires its disclosure, and (ii) is made under an enactment of British Columbia or Canada.

The *Mutual Legal Assistance Treaty ("MLAT")* between Canada and the U.S.A., discussed above, applies to U.S. requests for "documents, records or other articles known to be located in [Canada]",[48] in relation to the "investigation, prosecution and suppression of [criminal] offences."[49] It is thus significantly narrower in scope than orders under the *USA Patriot Act*, which are issued for proactive investigations "to protect against international terrorism or clandestine intelligence activities". Unlike MLAT assistance, no offence or suspected offence need be identified in order for *Patriot Act* orders to be issued.

Moreover, the treaty explicitly allows for the parties to provide assistance to each other "pursuant to other agreements, arrangements or practices."[50] It could well be the case, given the current climate of fear and pressure from the U.S.A. on Canada to cooperate in the war against terrorism, that Canada and the U.S.A. agree or have agreed to a less rigorous procedure for enforcing U.S. information requests in Canada.

Even if the MLAT applies to a given U.S. request for information in Canada, it is important to note that the purpose of the treaty is not to protect Canadians' privacy or due process. Rather, the purpose is "to improve the effectiveness of both countries in the investigation, prosecution and suppression of crime through cooperation and mutual assistance in law enforcement matters."[51] While it does require that all U.S. requests be executed in accordance with Canadian law (including the *Charter*), the MLAT requires that Canada "use its best efforts to keep confidential a request and its contents". Thus, even if the MLAT applies to a given request for data from the U.S., the resulting confidential process could still be subject Canadians' personal information to access by U.S. authorities in violation of Canadian privacy laws and *Charter* rights.

Finally, as noted above, Canada can deny assistance to the U.S.A. under the treaty to the extent that the request is not in accordance with Canadian law, or where its execution would be contrary to "essential public policy" in Canada.[52] In such cases, the U.S.A. is free to pursue the matter through other means, including *USA Patriot Act* or other court orders.

Hence, although the *MLAT* establishes a default process for the U.S. government to access personal information about Canadians from a source in Canada, which process invokes Canadian law and all the protections therein, it is narrower in scope than the *USA Patriot Act*, can be overridden by other arrangements between the two countries, and does not guarantee that requests granted under the MLAT will be executed in accordance with Canadian laws. Moreover, if a request under the *MLAT* is unsuccessful, the U.S. is still free to pursue the matter by other means.

---

[48] *MLAT*, *supra note X*, Article IV(1).
[49] *Ibid.*, Article II(1).
[50] *Ibid.*, Articles IV(1) and III(1).
[51] *Ibid.*, preamble.
[52] *Ibid.*, Article V.

(ii) "Reasonable security arrangements": section 30, *FOIPPA*

FOIPPA also requires a public body to protect personal information in its custody or control from unauthorized access. Section 30 states:[53]

> The head of a public body must protect personal information in the custody or under the control of the public body by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

As explained above, personal information outsourced by the Ministry for administrative purposes remains "under its control". Hence, the Ministry must ensure that any private body to which it entrusts personal information does not permit access, and is not compelled to permit access, beyond that which the B.C. government would permit were the information in its possession. More specifically, it must make "reasonable security arrangements" to protect the outsourced information from unauthorized access, including by the U.S. government for counter-terrorism purposes where such access is not authorized under *FOIPPA* (e.g., not authorized in accordance with an *MLAT* process).[54]

Short of not outsourcing personal information to companies with U.S. links, Canadian governments can reduce the risk of exposing such data to unauthorized access by U.S. authorities by:

- legislating and including in all outsourcing contracts a provision that all outsourced data must remain in Canada and be outside the control (technically and legally) of any U.S. affiliates;

- requiring, by legislation and by contract, that the government be immediately notified of any foreign court orders or other requests for the production of outsourced information;

- establishing significant penalties for breach of these provisions – penalties that include immediate termination of the contract, fines and damages.

However, the only way to ensure against unauthorized access by U.S. authorities is not to allow the information to get into the possession of U.S.-linked organizations in the first place. Less restrictive security arrangements, such as those identified above, will have a mitigating effect but will not positively ensure against disclosure in response to *USA Patriot Act* orders. This is because U.S.-linked organizations served with a *USA Patriot Act* production order will be faced with conflicting obligations. In that context, they will choose to respect the obligation that is most likely to be enforced and that carries the most significant penalties for non-compliance. Given the confidentiality associated with *Patriot Act* orders, and the potentially heavy penalties associated with non-compliance, a company would likely decide to comply with the U.S. request over its conflicting

---

[53] *Supra*, note 4, s. 30.

[54] As mentioned above, that access is authorized by U.S. legislation or court does not mean that such access is authorized under Canadian law.

Canadian obligations. In such a case, it is unlikely that the Canadian or B.C. government would even know about the information transfer.

In this context, not outsourcing the administration of personal information databases clearly constitutes a "reasonable security arrangement". It is worth noting that Statistics Canada took this approach recently in respect to an outsourcing contract it signed with Lockheed Martin: while initially planning to have the firm provide services for the 2006 census, Statistics Canada cancelled the contract as a result of public pressure.[55] Lockheed Martin is still providing software to StatsCan but will not have access to any census data.

It is unclear whether legislative and/or contractual limitations could effectively limit the ability of private companies to comply with *USA Patriot Act* orders. Even so-called "blocking statutes" that attempt to negate the effectiveness of foreign court orders cannot negate the reality that a company faces when ordered by one country to breach another country's laws.

(b) The *Canadian Charter of Rights and Freedoms*

In addition to the privacy protections codified in British Columbia's *Freedom of Information and Protection of Privacy Act*, Canadians enjoy privacy rights under the *Canadian Charter of Rights and Freedoms*.[56] Section 8 of the *Charter* enshrines a right to privacy in the context of "unreasonable search and seizure," while there is an emerging body of case law suggesting privacy rights are also inherent in the section 7 right to "life, liberty and security of the person."[57]

(i) Section 8 of the *Charter*

The Supreme Court of Canada has held that a core component of the section 8 right "to be secure against unreasonable search and seizure" is the protection of an individual's privacy, specifically, an individual's "reasonable expectation of privacy."[58] An order to produce documents constitutes a "search" for the purposes of section 8 of the *Charter*, provided that there is a reasonable expectation of privacy with respect to the documents.[59] An individual's "reasonable expectation of privacy" extends to "a biographical core of personal information which individuals in a free and democratic society would wish to

---

[55] Joe Paraskevas, "StatsCan kills census deal over privacy concerns", *The Ottawa Citizen* (May 9, 2004), p.A3.

[56] Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11 [*Charter*].

[57] For a more in depth analysis of the law of privacy in Canada, and, in particular, the emergence of a right to privacy under the *Charter* see: Barbara McIsaac, Rick Shields & Kris Klien, *The Law of Privacy in Canada*, looseleaf (Scarborough: Thomson Carswell, 2004).

[58] *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145 [*Hunter*].

[59] *Thomson Newspapers Ltd. v. Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)*, [1990] 1 S.C.R. 425. Five separate opinions were written by five separate judges. On the questions of whether an order to produce documents was a seizure, there was a majority of four. See also Peter W. Hogg, *Constitutional Law of Canada*, looseleaf (Toronto: Thomson Carswell, 1997) at 45-18 [Hogg].

maintain and control from dissemination to the state," and includes "information which tends to reveal intimate details of the lifestyle and personal choices of the individual."[60]

In *R. v. Plant*, the police accessed records held by the City indicating the electricity consumption of an individual suspected of cultivating marijuana in the basement of his home.[61] The City had given the police access to its computerized records and had arranged for an access terminal to be located at the police station. In response to the accused's challenge under s. 8 of the *Charter*, the Supreme Court agreed unanimously that an individual had a reasonable expectation of privacy with respect to information that was "personal and confidential."[62] The majority in *Plant* determined that electricity records were not personal and confidential because they revealed so little about the personal lifestyle or private decisions of the accused.

However, the same cannot be said about medical records.[63] In fact, the Supreme Court has characterized the information in medical records as "profoundly intimate."[64] In other words, an order for the production of medical records will infringe upon an individual's expectation of privacy and will violate section 8 of the *Charter* if the search is not reasonable under the circumstances.

A search or seizure will be reasonable for the purpose of section 8 only if it is authorized by a statute that requires (1) prior authorization, (2) that the authorization be issued by an impartial arbiter capable of balancing the conflicting interests of the state and the individual, and (3) that the arbiter find, at a minimum, that there are "reasonable and probable grounds, established upon oath, to believe that an offence has been committed and that there is evidence to be found at the place of the search."[65] Because production orders and NSLs under sections 215 and 505 of the *USA Patriot Act* do not require the establishment of reasonable and probable grounds, they fail this test of reasonableness.

As pointed out by Dickson C.J. in delivering the judgment of the Court in *Hunter v. Southam*, the requirement of prior authorization is only meaningful if the person authorizing the search is able to assess the evidence as to whether as to whether the

---

[60] *R. v. Plant*, [1993] 3 S.C.R. 281 at ¶20 [*Plant*].

[61] *Ibid*.

[62] *Ibid*.

[63] McLachlin J. disagreed with the majority and took the view that the accused had a reasonable expectation that the records would be used solely for billing purposes and that the access by police violated the accused's reasonable expectation of privacy. See also *R. v. Smith*, [2001] 3 S.C.R. 902, where the Court, using the same reasoning as *Plant*, held that an individual did not have a reasonable expectation of privacy in a customs declaration form.

[64] *R. v. O'Connor* (1995), 130 D.L.R. (4th) 235 [*O'Connor*]. See also R. v. Mills, [1999] 3 S.C.R. 668, where the Court discussed the procedures governing the production of the medical records of complainants in sexual assault trials.

[65] *Hunter, supra*, note 52. It was recognized in *Hunter* that prior judicial authorization was not feasible in every situation, and thus, in some circumstances, a warrantless search could be upheld as reasonable under the circumstances. However, for the purposes of the current analysis these situations are not applicable.

standard has been met in and entirely neutral and impartial manner.[66] A corollary of this statement is that prior authorization is meaningful only if the arbiter is capable of denying authorization based on his or her assessment of the evidence. Section 215 of the *USA Patriot Act*, however, leaves the arbiter very little room to assess the evidence or to deny a requested order. As long as the application specifies that the records concerned are sought for an authorized investigation to protect against international terrorism or clandestine intelligence activities, "the judge shall enter an *ex parte* order as requested."[67]

In *Hunter v. Southam*, one of the challenges to the *Combines Investigation Act* was that the standard for authorizing a search was not sufficiently objective to allow for meaningful assessment. The Act authorized officers to enter and examine documents on the basis that (1) an inquiry under the Act was in progress, and that (2) the Director believed that the premises might contain relevant evidence.[68] In analyzing the *Combines Investigation Act* standard the Supreme Court held that:[69]

> Such an amorphous standard cannot provide a meaningful criterion for securing the right guaranteed by s. 8. The location of the constitutional balance between a justifiable expectation of privacy and the legitimate needs of the states cannot depend on the subjective appreciation of individual adjudicators. Some objective standard must be established.

The standards proposed by the *Combines Investigation Act* and the *USA Patriot Act* are remarkably similar. Both permit searches upon the subjective belief or certification of law enforcement officials; neither requires applicants to establish reasonable and probable grounds to that an offence has been committed or that there is evidence to be found at the place of the search. In fact, the *USA Patriot Act* goes further and requires judicial authorization based on mere statements by government officials (whereas the *Combines Investigation Act* merely empowered a member of the Restrictive Trade Practices Commission to issue a certificate authorizing the search).

It is CIPPIC's view therefore that the *USA Patriot Act*, if enacted in Canada, would violate section 8 of the *Charter*.

---

[66] *Hunter, supra*, note 52.

[67] *USA Patriot Act, supra* note 1, § 215(c)(1). As mentioned above, applications for surveillance and/or searches under *FISA* are nearly always approved. In fact between 1978 and 2003 the Foreign Intelligence Surveillance Court heard over 14,000 applications and approved all but five without modification.

[68] *Hunter, supra*, note 52. Subsections 10(1) and 10(3) of the Combines Investigation Act provided:
10. (1) Subject to subsection (3), in any inquiry under this Act the Director [of Investigation and Research of the Combines Investigation Branch] or any representative authorized by him may enter any premises on which the Director believes there may be evidence relevant to the matters being inquired into and may examine any thing on the premises and may copy or take away for further examination or copying any book, paper, record or other document that in the opinion of the Director or his authorized representative, as the case may be, may afford such evidence.
…..
(3) Before exercising the power conferred by subsection (1), the Director or his representative shall produce a certificate from a member of the [Restrictive Trade Practices] Commission, which may be granted on the ex parte application of the Director, authorizing the exercise of such power.

[69] *Ibid.*

(ii) Section 7 of the *Charter*

Section 7 of the *Charter* protects an individual's right to life, liberty and security of the person. Specifically, it provides:

> Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice.

In *R. v. Dyment*, La Forest J. stated "privacy is at the heart of *liberty* in a modern state. Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection."[70] Similarly, in *R. v. O'Connor*, L'Heureux-Dubé J., writing in dissent on the main issue, but receiving general agreement from four other members of the Court on her privacy views, cited with approval the decision of Wilson J. in *R. v. Morgentaler* in which she stated "the *Charter* requires that the right to liberty contain in s. 7 be read to 'guarantee to every individual a degree of personal autonomy over important decisions.'"[71] L'Heureux-Dubé elaborated further stating that:[72]

> Respect for individual privacy is an essential component of what it means to be "free". As a corollary, the infringement of this right undeniably infringe upon an individual's "liberty" in our free and democratic state.

The existence of a right to privacy under section 7 of the *Charter* was more recently canvassed by the Federal Court of Appeal in *Ruby v. Canada (Attorney General)*.[73] In *Ruby*, the appellant sought the disclosure of information about himself contained in information banks maintained by the Canadian Security Intelligence Service (CSIS), the Department of External Affairs (DEA), and the RCMP. The organizations had refused to disclose the existence and/or content of any records in their possession under various

---

[70] [1988] 2 S.C.R. 417 [*Dyment*]. In *Dyment*, a doctor took a sample of blood for medical purposes from an individual involved in a traffic accident, without the knowledge or consent of the individual. Shortly after, the doctor gave the sample to a police officer. The sample was subsequently analyzed and found to contain a blood alcohol concentration in excess of the 0.08%. The individual was charged and convicted of impaired driving.

[71] *R. v. Morgentaler*, [1988] 1 S.C.R. 30, as cited in *O'Connor*, *supra* note 58, at 287.

[72] *O'Connor*, *supra* note 58, at 288. In *O'Connor*, an individual accused of sexual assault requested access to the medical and counseling records of the complainants. These records were not in the possession of the Crown, but rather in the possession of the various doctors and professionals who had created the records. In deciding that the complainants had a right to privacy in the documents, the Court was careful to specify that this right had to be carefully balanced against the accused's right to make full answer and defence. It should be noted, that only L'Heureux-Dubé defined the complainants' right to privacy in the documents as stemming from the right to 'liberty' found in section 7.

[73] [2000] 3 F.C. 589 at 166 [*Ruby*], rev'd [2002] 4 S.C.R. 3. The Supreme Court of Canada determined that "it [was] unnecessary to the disposition of [the appeal] to decide whether a right to privacy comprising a corollary right of access to personal information triggers the application of s. 7 of the *Charter*." The Supreme Court instead held that even in "assuming, for the purposes of analysis, that [Rudy] suffered a deprivation of his liberty or security of the person interest, that deprivation is not contrary to the principles of fundamental justice."

sections of the *Privacy Act*.[74] In response to the appellant's section 7 arguments, the court stated:

> At present the law recognizes three distinct "zones" of privacy. The territorial zone refers to places such as one's home. Personal or corporeal privacy is concerned with the human body (body, image such as photographs, voice or name). Finally, a person can make a claim to informational privacy which shelters intimate details concerning matters such as health, sexual orientation, employment, social views, friendships and associations.[75]

Thus, the confidential disclosure of health or other "core biographical" information about Canadians to U.S. authorities under the *USA Patriot Act* could be found to violate section 7 rights under the *Charter*, as well as the right to be free from unreasonable search and seizure guaranteed by section 8.

(iii) Is the privacy invasion justified under s. 1 of the *Charter*?

All rights guaranteed under the *Charter* are subject to reasonable limits that can be "demonstrably justified in a free and democratic society." The criteria that must be satisfied to establish that a limit is reasonable and demonstrably justified in a free and democratic society have been laid out in *R. v. Oakes*:[76]

1. The government's objective in limiting a *Charter*-protected right must be a pressing and substantial objective.

2. If the objective is deemed to be pressing and substantial, the court analyzes the proportionality between the objective and the means used to further that objective. In analyzing proportionality, the court examines:
   (a) whether the legislative means are rationally connected to the objective of the legislation;
   (b) whether the means chosen impair the *Charter* right in question as minimally as possible; and
   (c) whether the measures that are responsible for limiting the *Charter* right proportional to the objective.

If legislation, having been found to violate a *Charter* right, fails to meet any of the above criteria, it is unconstitutional.

Applying the *Oakes* test to ss.215 and 505 of the *USA Patriot Act*, a court would likely find, first, that the provisions pursue a sufficiently important objective: "to protect against international terrorism or clandestine intelligence activities." Sections 215 and 505 are

---

[74] R.S.C., 1985, c. P-21.

[75] *Ibid*, at ¶166. Emphasis added.

[76] [1986] 1 S.C.R. 103. While it is *theoretically* possible that a search found to be an "unreasonable" under section 8, could still be upheld as a "reasonable" limit under section 1, there are no cases in which this has ever occurred: Hogg, *supra*, at 45-2.

rationally connected to that objective, insofar as they are provide U.S. law enforcement agencies with greater powers to facilitate the fight against international terrorism.[77]

However, the "minimal impairment" test under s. 1 is not met here. The sweeping powers conferred upon law enforcement authorities by these provisions impair *Charter* rights far more than necessary. Moreover, these powers are disproportionately broad and invasive in relation to their objective. The lack of meaningful judicial oversight under the *USA Patriot Act* could easily be rectified so as to conform with rights guaranteed under the *Charter*, while still permitting U.S. authorities to protect against international terrorism.

It is therefore our view that any infringement of *Charter* rights as a result of a *USA Patriot Act* order would not be considered "demonstrably justified in a free and democratic society".

(iv) Application of the *Charter* to U.S. orders

For the same reason that U.S. courts cannot order the production of documents from Canadian public bodies, the *Charter* cannot be used to strike down foreign laws.[78] However, the *Charter* has been used in the past to prevent the extradition or deportation of an individual to a jurisdiction where he or she may face the possibility of execution or torture.[79] In other words, in certain circumstances the *Charter* has been employed to override decisions of the Canadian government or government officials, where those decisions would subject Canadians to foreign laws which would violate the *Charter*. To date, the circumstances in which the *Charter* has been used in this manner have been limited to situations where the decision of a government official to expose an individual to a foreign law would violate section 7 rights in a manner that would "shock the Canadian conscience."[80]

The sweeping investigatory powers given to U.S. law enforcement authorities under the *USA Patriot Act*, and the actual or potential use of such powers by U.S. officials to gather personal information about Canadians and to use it for their own purposes would, in our view, "shock the conscience" of Canadians. This conclusion is supported by Supreme Court jurisprudence as well as the reaction of Canadians to the case of Maher Arar, described below.

---

[77] It is extremely rare that a law will be found to have a sufficiently important objective, but then be struck down for failure to satisfy the requirement of rational connection. There is a general presumption that the legislature would not enact a law that is not rationally connected to its objective. See Hogg, *supra*, note 53.

[78] See text accompanying note 47, *supra*.

[79] In *United States of America v. Burns*, [2001] 1 S.C.R. 283 [*Burns*], the Court ruled that the failure of the British Columbia Minister of Justice to obtain assurances that the accused would not face the death penalty violated section 7 of the *Charter* and could not be justified under section 1. See also *Suresh v. Canada*, [2002] 1 S.C.R., where the Court held that the deportation of an individual to face torture would 'usually' be a breach of the principles of fundamental justice.

[80] *Burns, ibid.*

In *R. v. Dyment*, the Supreme Court found that the taking of a sample of blood from an individual involved in a traffic accident without his knowledge or consent, and subsequent analysis and use of that sample to charge and convict the individual of impaired driving, would shock the community. La Forest J., writing for the majority, stated that the lower court judge was substantially right when he stated:[81]

> [The actions of the police] constitute such a gross violation to the sanctity, integrity and privacy of the appellant's bodily substances and medical records that the community would be shocked and appalled if the court allowed the admission of this evidence in the face of the Charter.

While there is no doubt that the feelings of shock in this case would be owed in part to the violation of the integrity and privacy of Dyment's bodily substances, it is important to note that they are also connected to the invasion of the information held in Dyment's medical records. If warrantless access to the medical records of an individual by Canadian law enforcement agents in the context of a suspected offence is enough to shock and appal the community, it is realistic to believe that similar access by foreign law enforcement agencies to large databases of sensitive personal information of Canadians would "shock the Canadian conscience" and require *Charter* scrutiny.

A more recent and relevant example which has shocked the Canadian conscience is the detainment and deportation of Maher Arar by U.S. authorities. Arar, a Canadian citizen who immigrated from Syria in 1987, was detained by U.S. officials on a stopover in New York as he was returning to Canada from a vacation in Tunisia in September 2002.[82] Arar was deported to Syria, despite the fact that he was carrying a Canadian passport, where he was question about links to al-Qaeda and tortured at length.[83] It has been alleged that U.S. officials' assertions of Arar having links to al-Qaeda were based in part on information obtained from the RCMP.[84] Arar's case prompted an outcry from his family, opposition politicians, Canadian Arab groups, Amnesty International, and the public at large. In response to that outcry, the Canadian government finally agreed to hold a public inquiry into the case. (That inquiry is currently underway.)

While the information received from the RCMP in the Arar case was not likely obtained under section 215 of the *USA Patriot Act*, the public outrage which led to the inquiry illustrates that unrestricted disclosure of personal information by Canadian authorities to U.S. authorities for counter-terrorism purposes can indeed "shock the conscience" of Canadians, and suggests that the disclosure of personal *health* information of ordinary Canadians to U.S. authorities would also meet this test.

---

[81] *R.* v. *Dyment* (1984), 47 Nfld. & P.E.I.R. 350, as cited in *Dyment*, *supra* note 64 at 287. Emphasis added.

[82] "RCMP official at Arar inquiry says innocent people placed in national database" *CBC News* (30 June 2004), online: CBC News Online <http://www.cbc.ca/stories/2004/06/30/canada/ArarRCMP_040630>.

[83] "Arar says he was tortured in Syria" *CBC News* (30 October 2003), online: CBC News Online <http://www.cbc.ca/stories/2003/10/30/arar_031030>; "Canadian sues U.S. over deportation" *BBC News* (23 January 2004), online: BBC News <http://news.bbc.co.uk/1/hi/world/americas/3421743.stm>.

[84] "Arar inquiry to hear torture tale from another Canadian" CBC News Online (7 July 2004), online: CNC News Online <http://www.cbc.ca/stories/2004/07/06/canada/Ararinquiry_040706>. More information regarding the inquiry is available on the Maher Arar website at: http://www.maherarar.ca/.

(v) Conclusion on *Charter* implications of *USA Patriot Act* and B.C. government outsourcing

If enacted in Canada, the *USA Patriot Act* would likely be found to violate the *Charter* right to freedom from unreasonable search and seizure, and possibly also the right to "life, liberty and security of the person." While the *Charter* cannot be used to strike down foreign laws, it can be used to override decisions of the Canadian government or government officials, where those decisions would subject Canadians to foreign laws which would violate *Charter* principles and shock the Canadian conscience. As illustrated by both *Dyment* and the public inquiry into the deportation of Maher Arar, unauthorized access by U.S. law enforcement authorities to records containing the personal health information of Canadians would likely to "shock the conscience" of Canadians. Thus, the decision to outsource the administration of the British Columbia MSP to a U.S.-linked organization, and thereby potentially expose such information to access by U.S. law enforcement agencies, could constitute an infringement of privacy rights protected by sections 7 and 8 of the *Charter*.

IV. Conclusion

The *USA Patriot Act* authorizes access by U.S. law enforcement agents to personal information (indeed, entire databases of information) about non-U.S. citizens for counter-terrorism purposes, regardless of whether or not the individual is engaged in terrorism, espionage, or any other criminal activity. The sole requirement for obtaining access to these documents and records under the *USA Patriot Act* is certification by law enforcement officials to a judge of the Foreign Intelligence Surveillance Court (or to FBI officials themselves in the case of National Security Letters) that the purpose of the investigation is to obtain foreign intelligence information or to protect against international terrorism or clandestine intelligence activities. Applications to the Foreign Intelligence Surveillance Court are rarely rejected or modified, and once issued, cannot be challenged. Organizations are prohibited from divulging the fact that they have been compelled to disclose information under the *USA Patriot Act*, and are subject to heavy fines and/or imprisonment if they refuse to comply.

Organizations based outside the U.S or holding information outside the U.S. are not immune from *USA Patriot Act* orders. As long as the organization has a link to the U.S.A., it can be made subject to a U.S. court order. American case law dealing with judicial orders for the production of documents suggests that neither the location of documents in a foreign country, nor the protection of foreign privacy laws, will prevent the court from ordering production and punishing organizations heavily for failing to comply. The *Mutual Legal Assistance Treaty in Criminal Matters* ("*MLAT*") between Canada and the U.S.A. does not ensure that *USA Patriot Act* orders will be made and executed in accordance with Canadian law.

In view of the fact that the *USA Patriot Act* can be used to compel Canadian organizations with U.S. links to disclose information in their possession without the data subject's knowledge and for purposes inconsistent with those for which the data was collected, the British Columbia Ministry of Health Services cannot outsource data administration involving personal information of its citizens to U.S.-linked organizations without breaching its obligations under the *FOIPPA.*

Although *FOIPPA* authorizes the disclosure of personal information in certain circumstances, it does not authorize the disclosure of personal health information by public bodies to U.S. law enforcement agencies for counter-terrorism purposes, except as permitted via the *MLAT* process. Indeed, *FOIPPA* requires that the Minister of Health Services make "reasonable security arrangements" protecting the information from unauthorized access by U.S. law enforcement agencies. The most effective security arrangement in these circumstances is clearly not outsourcing the administration of personal information databases to U.S.-linked organizations in the first place. Less restrictive measures, such as contractual restrictions on companies to whom data has been outsourced, would put U.S.-linked companies in the situation of having to choose between two conflicting legal obligations. Given the secrecy attached to *Patriot Act* orders and the relative size and importance of the U.S. market, it is likely that Canadian obligations would give way to U.S. orders.

Furthermore, exposing the personal health information of British Columbians to access by U.S. law enforcement agencies could well constitute a violation of Canadians' informational privacy rights inherent in sections 7 and 8 of the *Charter*. It is likely that Canadians would be shocked to find out that their personal health records were subject to U.S. investigations for counter-terrorism purposes. This being so, the Minister's decision to outsource the management of these records to a U.S.-linked organization could be challenged under the *Charter*, as well as under the BC *FOIPPA*.

V. Postscript

While this submission focuses on the B.C. government's obligations with respect to outsourced data and privacy protection, all Canadian governments face the same issue. CIPPIC commends the B.C. Privacy Commissioner on undertaking this public consultation. All jurisdictions in Canada should be conducting similar inquiries.

It should also be noted that the privacy issue raised by the B.C. Privacy Commissioner is much larger than might appear, and cannot be resolved by a moratorium on government outsourcing alone. A great deal of Canadians' personal information is already in private sector hands: U.S. linked insurance companies, financial institutions, telecommunications companies, and credit bureaus, for example, hold vast amounts of highly sensitive personal information in databases that are equally vulnerable to access by U.S. authorities under the *USAPatriot Act* and other statutory mechanisms. Although these companies are, for the most part, subject to *Personal Information Protection and Electronic Documents Act* ("PIPEDA") as a result of their status as federally regulated industries or their interprovincial activities, any PIPEDA obligations are unlikely to hold the same

force as *USA Patriot Act* orders. Thus, even if governments take effective steps to keep personal information under their control from access by U.S. authorities (as they should), this will solve only part of the problem. The time is ripe for a thorough study of the extent to which Canadians' personal information is collected, stored, used and shared via private sector databases, and the extent to which this information is accessible by foreign governments.

Submitted by:

Philippa Lawson
Executive Director, CIPPIC
University of Ottawa
www.cippic.ca

Matthew Kindree
CIPPIC Summer Fellow