The Long Arm of the USA Patriot Act:
A Threat to Canadian Privacy?

A Submission on the USA Patriot Act to the B.C. Information and Privacy Commissioner

July 2004

Professor Michael Geist
Canada Research Chair in Internet and E-commerce Law
University of Ottawa, Faculty of Law

And

Milana Homsi, LL.B.

TABLE OF CONTENTS

Executive Summary

This report responds to the Office of the Information and Privacy Commissioner for British Columbia's May 2004 request for comment titled Assessing USA Patriot Act Implications. It addresses the first question on whether the Patriot Act permits U.S. law enforcement authorities to access the personal information of Canadians. With respect to the second question on the applicability of the B.C. FOIPP, it leaves the specific provincial privacy issue to more qualified local experts, focusing instead on the concerns this issue raises in the broader context of PIPEDA, Canada's national private sector privacy legislation.

The report first outlines the Patriot Act powers with specific analysis of Section 215. It also calls attention to alternative U.S. legal instruments, including grand jury subpoenas and national security letters, which can similarly be used to obtain record disclosures without consent. In light of these powers, the report reviews U.S. case law on enforcing disclosure requests where the recipient is subject to U.S. personal jurisdiction.

It concludes that U.S. law does indeed grant law enforcement authorities the power to compel disclosure of personal information without notifying the targeted individual that their information is being disclosed (in fact, disclosing the disclosure is itself a violation of the law). Moreover, the application of these laws is not limited to U.S. companies but actually applies to any company with sufficient U.S. connections such that it could find itself subject to the jurisdiction of the U.S. courts. This is true both for U.S. companies operating subsidiaries in foreign countries as well as for foreign companies with U.S. subsidiaries.

The report then considers the effect of PIPEDA on third party disclosures and whether disclosures compelled by U.S. law would constitute a statutory violation. It concludes that it is currently uncertain whether disclosures compelled by U.S. law would actually constitute a PIPEDA violation. While the law requires user consent where

personal information is disclosed to a third party, the statute contains several exceptions to this general rule which might apply in this situation.

The report concludes with four recommendations on how to eliminate or appropriately mitigate the privacy risks arising from any such disclosures. These include considering a ban on governmental outsourcing of personal information, establishing a formal or informal agreement with U.S. law enforcement agencies on requests involving Canadian data, amending PIPEDA to meet the U.S. blocking statute standard, and clarifying the jurisdictional reach of PIPEDA.

I. Introduction

i. Summary of the Issue

In response to public concern over the privacy implications of a proposed British Columbia government outsourcing of provincial health data, B.C. Information and Privacy Commissioner David Loukidelis launched a public consultation in May 2004 into whether the USA Patriot Act could be used by U.S. law enforcement agencies to compel the disclosure of British Columbians' personal information without prior notice or consent. Similar privacy concerns led the Canadian federal government in May 2004 to place a limit on a contract that had been awarded to the Canadian subsidiary of Lockheed Martin for work on the 2006 census.

ii. Statement of the Facts

The B.C. Ministry of Health Services issued a Request for Proposals ("RFP") in 2004 that sought a private partner to assume responsibility for the operation of its Medical Services Plan ("MSP"). Shortly after the RFP was issued, the B.C. Government and Services Employees' Union ("BCGEU") commenced a campaign to oppose any contracting out of the services to U.S. multinational corporations. The union expressed concerns that Canadian data would be at risk of disclosure to U.S. law enforcement under the Patriot Act. The BCGEU subsequently filed a petition with the Supreme Court of British Columbia seeking a declaration that the contracting out of services contravenes the Medicare Protection Act, the Canada Health Act and the Freedom of Information and Protection of Privacy Act ("FOIPPA"). In the interim, the B.C. government placed the outsourcing on hold, pending resolution of the petition.

II. Patriot Act Powers

i. What is the Patriot Act?

The USA Patriot Act was passed in the aftermath of 9-11 to provide U.S. law enforcement with new measures that expand surveillance capability while minimizing

procedural obstacles.[1] These include new investigative tools that increase information gathering from communication providers, a broadened ability for electronic surveillance, relaxed federal procedure for search warrants, new offenses for money laundering, and new terrorism related federal offences. Many of the provisions included in the act, including Section 215, feature a sunset clause that will cause them to expire on December 31, 2005, unless the U.S. Congress renews the enumerated powers prior to that date.

ii. What is Section 215?

Section 215 of the Patriot Act amends the *Foreign Intelligence Surveillance Act* (FISA) to simplify the procedure for the Federal Bureau of Investigations (FBI) to access business records that relate to foreign intelligence gathering.[2] FISA was established in 1978 to create a separate legal regime for government surveillance pertaining to foreign intelligence. It created a special FISA court to which the government can apply for surveillance orders. Deliberations are conducted in secret and the contents or target of a FISA order do not have to be disclosed. In 1998, FISA amendments allowed law enforcement to obtain business records for intelligence gathering operations. Previously, only telephone, financial and credit records were available through national security letters, which are administrative subpoenas that allow electronic records to be disclosed for foreign intelligence or international counter-terrorism investigations.

To obtain a court order, the 1998 FISA amendments mandated that law enforcement prove "specific and articulable facts" that gave reason to believe that the target of the search was "a foreign power or an agent of a foreign power", as well as provide proof that the information sought was for a foreign intelligence or foreign terrorism investigation.

The Patriot Act amended the business record clause in several important ways. Section 215 now permits the director of the FBI or his designate to request an order for the production "of any tangible things" from any individual or organization that is

---

[1] *The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) of 2001*, Pub. L. 107-56, 115 Stat. 272.
[2] 50 U.S.C. §1861 (1978).

relevant to an investigation of "international terrorism or clandestine intelligence activities". This establishes a lower standard than the "specific and articulable facts" that was previously required. The "tangible things" may include "books, records, papers, documents, and other items" of any subject.

The request is made to the FISA court or to a magistrate judge that is specifically authorized to hear FISA requests. If the request meets the requirements of this section, it is ordered on an ex parte basis. The language of the court's order cannot disclose the investigative purpose.

Anyone served with an order issued under FISA rules may not disclose the existence of the warrant or the fact that records were provided to the government. Although there is not a specified punishment, a Department of Justice ("DOJ") web FAQ on Section 215 states that disclosure by a recipient will be punished as contempt of court under 8 U.S.C. 401, and can lead to imprisonment or fine.[3]

Section 215 cannot be used to obtain the records of a U.S. resident on the basis of activities that are protected by the First Amendment (e.g. free speech, freedom of religion, etc.). This First Amendment protection only applies to persons resident in the U.S.

The Patriot Act requires the Attorney General to semiannually inform the House and Senate Committees on Intelligence on all requests for the production of tangible things. It also requires the Attorney General to report semiannually to the House and Senate Judiciary Committees the number of applications filed under this section and whether they were granted, modified or denied.

---

[3] Eastern District of Michigan Department of Justice, "Question and Answers about Section 215 of the Patriot Act", online: Counter Terrorism Website <http://www.usdoj.gov/usao/mie/ctu/Section_215.htm>.

iii. How is Section 215 being used by law enforcement?

a. Attempts to determine how it is being used

Using the U.S. *Freedom of Information Act*[4] the American Civil Liberties Union (ACLU) and other civil liberties groups obtained disclosure of several FBI memoranda ("FBI memos") that illustrate how the FBI is using Section 215 in practice.[5] The groups also requested statistical data on how the Department of Justice has implemented section 215, but the D.C. district court found that the arguments in favour of disclosure were ultimately insufficient to overcome the DOJ's judgment that withholding the information was reasonably connected to national security.[6] However, the requested statistics were disclosed to the House Judiciary Committee pursuant to an inquiry.[7]

According to one of the FBI memos less than ten business records applications were filed from October 2001 (when the Patriot Act was passed) until February 7th, 2003.[8] The ACLU has received one cover letter that indicates that an additional application was filed on October 15, 2003.[9]

b. Law Enforcement's Actual Use

The FBI memos disclosed through the ACLU FOIA request illustrate the actual practice of obtaining Section 215 orders. An October 2003 memo to FBI field offices includes guidelines for the use of section orders.[10] According to the memo:

---

[4] 5 U.S.C. § 552.
[5] *ACLU v. United States DOJ*, 2004 U.S. Dist. LEXIS 9381 (D.D.C., May 10, 2004).
[6] *ACLU v. United States DOJ*, 265 F.Supp.2d 20 (D.D.C., 2003).
[7] U.S., Assistant Attorney General, 108th Cong., *Answers to Questions Submitted by the House Judiciary Committee to the Attorney General on USA Patriot Act Implementation* (Washington D.C.: July 26, 2002) ("Questions Submitted by the House").
[8] The actual total is blacked out on the document, but it can be deduced to be between 1-10 by the size of the list. See U.S., Assistant Attorney General, 108th Cong., *Business Order Requests since 10/26/2001*, online: ACLU website <http://www.aclu.org/PATRIOT_foia/2003/sec215_fbi.pdf>.
[9] Unnamed FBI Department, *50 U.S.C §1861 Business Order Application*, Memo to Office of Intelligence Policy and Review (OIPR), (Washington D.C.: October 15, 2003).
[10] General Counsel, FBI National Security Law Unit, *Business Record Orders under 50 U.S.C. §1861*, Memo to All Field Offices, (Washington D.C.: October 29, 2003).

1. **Requests must be relevant**: Requests for Section 215 orders must be relevant to foreign intelligence or anti-terrorism efforts and must explain how receiving access to the "tangible thing" can provide foreign intelligence information.
2. **Anyone can be a subject**: The subject of the request does not need to be the subject of investigation. Anyone related to the subject of the investigation can be the subject provided the relevancy test is met.
3. **The request can encompass any tangible thing**: The 'tangible thing" can be any records, books, papers, documents (such as apartment leases or insurance documents), keys or any other item. The FBI cautions against using this section to obtain educational and tax records, since there are "legal questions" about whether such requests are obtainable because they fall under the purview of other statutes. Similarly, the FBI warns field offices that requests for library records undergo strict scrutiny as they may conflict with First Amendment protections.
4. **The request must be for a full field investigation**: The request can currently only be made under the auspices of a full field investigation. Preliminary investigations and inquiries do not qualify. The memo states that preliminary investigations may be allowed in the near future.
5. **The procedure is straightforward**: The procedure for obtaining the "tangible thing" consists of completing a standardized Business Records form and providing a description of the tangible thing and the reason the recipient of the order has it in its possession. The requestor must also describe the investigation for which the tangible thing is sought and explain how the request will assist foreign intelligence gathering. The requests are then approved by the head of the field office and sent to the National Security Letter Bureau, which reviews the request and prepares an application and order for the FISA court which is signed by an attorney from the General Counsel's office. An attorney from either the Department of Justice's Office of Intelligence Policy and Review (OIPR) or the Office of General Counsel (OGC) presents the application to the FISA court by during its regularly scheduled Friday sessions. The signed order is then emailed to the requesting field office within days.

6. **Originals must be kept for two years by the recipient**: If copies instead of originals are requested, the recipient of the order must maintain the originals for two years unless the recipient is notified that earlier destruction is permitted.

Other documents demonstrate that the DOJ is concerned that investigations use the "least intrusive means" available. In discussing National Security Letters, the DOJ warns that Congress will examine their use by the FBI in considering whether the sunset provisions should be extended and they therefore should be used judiciously.[11]

The DOJ has stated that it is unlikely to use Section 215 to obtain library records or bookstore or newspaper records since such electronic communication transactional records are best obtained through National Security Letters.[12]

iv. Is Section 215 Constitutional?

The debate over the Patriot Act's constitutionality has generated considerable controversy. Civil liberties groups such as the ACLU, the Electronic Privacy Information Center (EPIC) and the Electronic Frontier Foundation (EFF), as well as library advocacy groups such as the American Library Association (ALA) argue that provisions of the Act, particularly Section 215, violate the very essence of the First and Fourth Amendment.

The Fourth Amendment protects against unreasonable searches and seizures by requiring probable cause that an individual is engaged in criminal activity or that evidence of a crime will be found. Critics argue that Section 215 violates the Fourth Amendment by allowing law enforcement to search without a warrant and without demonstrating probable cause or a predicate of criminal activity. Instead the more lenient "relevancy" standard requires only that the records sought be related to an ongoing terrorism investigation or intelligence activities and does not necessitate that the records being sought actually belong to a suspect.

---

[11] FBI General Counsel, *National Security Letter Matters*, Memo to all Field Offices (Washington D.C.: November 28, 2001).

[12] U.S., Assistant Attorney General, *Questions Submitted by the House Judiciary Committee to the Attorney General on USA PATRIOT Act Implementation,* Letter to the Chairman of the Committee on the Judiciary (Washington D.C.: August 26, 2002).

Moreover, since there is no requirement that the target of the search be notified, targets never know that their data has been disclosed. This may be contrasted with standard criminal procedure in which targets of criminal searches and wiretaps must eventually be notified of the search. Under FISA, a person is notified of the record disclosure only if they are later prosecuted using the evidence seized. Where a person is not prosecuted, notice will never be provided, and the search can never be challenged unless the target somehow independently discovered it.

Critics argue that Section 215's Fourth Amendment violations are particularly excessive because the court orders can be used to imperil First Amendment rights in two ways. First, Section 215 could be used to compel libraries to produce user records, or an Internet Service Provider to provide subscriber usage records. Secondly, Section 215 affects the First Amendment rights of organizations by prohibiting them from disclosing that they are the subject of any FISA court orders. There has been particular concern regarding the effect of this section on libraries, since it overrides and potentially conflicts with state library confidentiality laws.[13]

Since the implementation of the Patriot Act, there has been virtually no case law interpreting it. The few cases that have emerged focus on the right to detain terrorism suspects,[14] the freezing of corporate assets where there is suspicion of a terrorist link[15] or the prohibition on providing expert advice to terrorist groups.[16] Arab and Muslim organizations launched the only case challenging the constitutionality of Section 215 of the Patriot Act in July 2003 in U.S. District Court in Michigan.[17] A decision is still pending.

---

[13] Steven Aden and John Whitehead, "Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the USA Patriot Act and the Justice Department's Anti-Terrorism Initiatives" (2002) 51 Am. U.L. Rev. 1081 at 1100.
[14] See *Center for National Security Studies v. United States DOJ*, 356 U.S. App. D.C. 333 (2003).
[15] See *Global Relief Foundation, Inc. v. O'Neill*, 315 F.3d 748 (7th Cir. 2002).
[16] *Humanitarian Law Project v. Ashcroft*, 2004 U.S. Dist. LEXIS 926 (C.D. Cal., Jan. 22, 2004) (where prohibition was struck for vagueness).
[17] *Muslim Community Association of Ann Arbor et al. v. John Ashcroft*, Civil Action No. 03-72913 filed in U.S. District Court for the Eastern District of Michigan, Southern Division.

a. Foreigners and the U.S. Constitution

The applicability of the U.S. constitution is limited to U.S. residents and U.S. territory. Cases dating back the World War II limit the application of the Fifth Amendment (traditionally the most liberal in application) to aliens in U.S. territory.[18]

The Fourth Amendment has been held to not apply to non-U.S. citizens or residents located outside the United States. The court in *Verdugo-Urquidez* ruled that the Fourth Amendment does not restrain U.S. government actions against aliens outside U.S. territory.[19] The court states that aliens only hold constitutional rights when they come within U.S. territory and develop substantial connections. The First Amendment also only applies to resident aliens.[20] The case law suggests that even if Section 215 were held unconstitutional in the U.S., any such ruling would not apply to the use of the section to obtain disclosure about foreign suspects.

It is unclear whether Fourth Amendment protections would apply to Canadian-based data that belonged to a U.S. resident or citizen, either living in or visiting Canada. The case law makes clear that Congress has no power to deprive a U.S. citizen of certain constitutional rights even if they live abroad.[21] The Section 215 protection against searches that are based on First Amendment activities would likely apply to any U.S. citizen's Canadian-based data.

III. Alternatives to the Patriot Act

In addition to the powers granted under the Patriot Act, law enforcement can access business records without probable cause by utilizing National Security Letters or grand jury subpoenas.

---

[18] *Johnson v. Eisentrager*, 339 U.S. 763 (1950).
[19] *United States v. Verdugo-Urquidez, 494 U.S. 259* (1990).
[20] *United States ex rel. Turner v. Williams,* 194 U.S. 279, 292 (1904).
[21] *Reid v. Covert,* 354 U.S. 1 (1955).

i. National Security Letters

A national security letter (NSL) is an administrative subpoena that permits an FBI supervisory official to request particular records that relate to counterintelligence or terrorism investigations from third parties, such as telephone and Internet activity records (available under 18 USCS § 2709), as well as financial and credit records from banks and other financial institutions (available under 12 USCS § 3414). Much like Section 215 orders, NSLs, which have the same force and effect as a court order, prohibit recipients from disclosing their existence. The power to issue administrative subpoenas is common in the U.S.; a 2002 study by the Office of Legal Policy identified approximately 335 administrative subpoena authorities. In fact, according to the ACLU FOIA documents, National Security Letters have been used much more frequently then Section 215 orders.

A court's review of an administrative subpoena is limited by the wide discretion given to agency action. The review generally turns on a low threshold reasonableness standard, indicating that an agency is not required to show probable cause. Courts will enforce a subpoena if: (1) the investigation is legitimate, (2) the subpoena is not unnecessarily broad, and (3) the information sought is relevant to the investigation.[22]

The Bush administration has attempted to grant the FBI greater NSL powers. Section 334 of the House-passed Intelligence Authorization bill for FY 2004 (H.R. 2417) and Section 354 of the companion bill passed by the Senate (S. 1025) would expand the reach of NSLs for financial documents, by increasing the types of organizations considered financial institutions and broadening the definition of a record.[23] The Senate Judiciary Committee recently held hearings to contemplate broadening FBI administrative powers

---

[22] *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186 (1946); See also *Marshall v. Barlow's Inc.*, 436 U.S. 307 (1978) (where the reasonableness standard was held to be enough to meet constitutional restrictions on search and seizure).

[23] See Flint, Lara, Administrative Subpoenas for the FBI: A Grab for Unchecked Executive Power, CDT (September 23, 2002), online: <http://www.cdt.org/security/usapatriot/030924cdt.shtml>.

as per Senator Kyl's proposed Judicially Enforceable Terrorism Subpoena Act of 2004 and Representative Feeney's proposed Antiterrorism Tools Enhancement Act of 2003.[24]

ii. Grand Juries

A grand jury is a U.S. constitutional creation composed of between 16 and 23 civilian jurors who investigate the existence of possible criminal conduct under the aegis of a prosecutor.[25] The court in *Whitehouse v. United States Dist. Court for Dist. of R.I.* outlined the distinguishing features of the grand jury process. It is marked by "1) its independence from the court's supervision; 2) its broad investigative powers; 3) the presumption of validity accorded its subpoenas; 4) the secrecy of its proceedings; and 5) its general freedom from procedural detours and delays."[26]

As stated in *Whitehouse*, the grand jury has substantial investigatory power and can investigate on the mere suspicion that the law is being violated without the need for probable cause. Grand juries can subpoena virtually any person or relevant document and they do not operate according to many rules of evidence.[27] The grand jury subpoena is issued under the authority of a court – in practice, a court clerk issues a blank subpoena with the court seal to a prosecutor working with a grand jury.[28] A recipient who does not comply will be in contempt of court. The subpoenas generally cannot be appealed, though the recipient can bring a motion to quash before a district court.

Grand juries operate in secrecy and investigate on an ex parte basis. The secrecy requirement does not always apply to subpoena recipients, however, though special gag orders can be sought. This suggests that once they have testified or disclosed information, witnesses are free to discuss the subject of their grand jury testimony

---

[24] U.S., *Hearing on Tools to Fight Terrorism: Subpoena Authority and Pretrial Detention of Terrorists before the Senate Judiciary Committee, Subcommittee on Terrorism, Technology and Homeland Security*, 108th Cong. (Washington D.C., June 22, 2004).
[25] Fed. R. Crim. P. R 6.
[26] 53 F.3d 1349, 1357 (1st Cir. 1995).
[27] See, e.g., *United States v. Calandra*, 414 U.S. 338 (1974) (allowing evidence to be presented to grand jury despite prior violations of the Fourth and Fifth Amendment); *Costello v. United States*, 350 U.S. 359, (1956) (allowing hearsay).
[28] Fed. R. Crim. P. 17(a)

(although the notes to the Federal rule states that the existing practice on this point varies among the districts).[29] There are exceptions to this rule. For example, a bank cannot, under criminal penalty, notify a customer of the contents of a grand jury subpoena or of its testimony where a money laundering investigation is at issue.[30]

A system of statutory safeguards on the investigative powers of the grand jury exists with a judge and prosecutor overseeing disclosure demands. In *United States v. Williams*, Justice Scalia explained that the grand jury is "[r]ooted in long centuries of Anglo-American history" and "acts "as a kind of buffer or referee between the government and the people."[31] Grand juries are also "not licensed to engage in arbitrary fishing expeditions".[32]

IV. Who is subject to U.S. compelled disclosure?

i. General

The U.S. case law illustrates that the absence of Patriot Act powers has not prevented U.S. law enforcement from obtaining records if needed, even where disclosure might violate another jurisdiction's laws. For the past 50 years, courts have frequently ordered companies to comply with U.S. disclosure orders provided that the court can assert personal jurisdiction over the company in possession or control of the requested material. Courts have commonly ruled that foreign secrecy and confidentiality laws are less important than the U.S. criminal investigations that necessitate disclosure.[33] This trend would presumably also apply to other national privacy laws, including PIPEDA.

The model approach to this issue is that advocated by the *Restatement (Third) of the Foreign Relations Law of the United States* (1987) ("Restatement of Foreign Relations"), which has been widely adopted by U.S. federal and state courts. Section 403 addresses

---

[29] Fed. R. Crim. P. R 6 (e) 2.
[30] 31 U.S.C.S. § 5318(g)(3)
[31] 504 U.S. 36, 47 (1992)
[32] *United States v. R. Enterprises*, 498 U.S. 292, 299 (1991).
[33] See e.g., *First National City Bank of New York v. Internal Revenue Service*, 271 F.2d 616 (2d Cir. 1959); *Hartford Fire Insurance et al. v. California et al*., 509 U.S. 764 (1993); *In re Grand Jury Subpoena dated August 9, 2000*, 218 F. Supp. 2d 544 *(S.D.N.Y. 2002)* at 24.

conflicting laws and advocates a balancing test that considers the following factors: (1) the competing interests of the nations whose laws are in conflict, (2) the hardship of compliance on the party or witness from whom discovery is sought, (3) the importance to the litigation of the information and documents requested, and (4) the good faith of the party resisting discovery. The analysis is not limited to these factors, however, and it may encompass additional considerations. Based on this test, the possibility of civil or criminal sanctions in another jurisdiction will not necessarily prevent enforcement of a subpoena.

As discussed further below, blocking statutes are one of the only successful deterrence mechanisms to disclosure. A blocking statute is a law that effectively prohibits compliance with a foreign legal requirement by creating a punishable offence within the local jurisdiction. In this context, a blocking statute would prohibit an organization from disclosing locally held records for non-domestic investigations, unless specific permission is sought from a court of that jurisdiction.

ii. Data held outside the U.S.

U.S. corporations can generally be compelled to produce documents possessed by foreign offices, unless a strong defence, such as a blocking statute, is raised. This applies both where the documents are held by a foreign subsidiary (and the request is made to a domestic parent company) and where the documents are held by a foreign parent company (and the request is made to the domestic subsidiary).

Section 442(1)(c) of the Restatement of Foreign Relations, which addresses requests for disclosure of foreign records, directs courts to consider the importance of the documents requested to the underlying litigation, the availability of alternative means of disclosure, and the degree of specificity of the request. Section 442 (1)(a) states that a court or agency can compel any person subject to its jurisdiction to produce documents or objects necessary for any investigation "even if the information or the person in possession of the information is outside the United States".

a. U.S subsidiary and foreign parent

U.S. courts have ruled that records of a foreign parent corporation may be reached by an order to a subsidiary subject to U.S. personal jurisdiction. This is evidenced by cases involving grand jury subpoenas where subsidiaries were ordered to compel production of documents controlled by the foreign-based parent company. The courts typically employed a balancing test to determine whether to grant a motion to quash a grand jury subpoena where the records sought are abroad. There appears to be few cases where grand jury discovery was denied in the criminal context.[34]

U.S. courts deference to grand jury subpoenas is illustrated by a case involving the U.S. subsidiary of a Canadian parent company, the Bank of Nova Scotia.[35] The bank's Miami office was served with a U.S. grand jury subpoena to disclose financial documents pertaining to two individuals and several companies. The documents were thought to exist in the bank's Bahamas and Cayman Island branches. The bank claimed that disclosure would violate Bahamian and Cayman Islands secrecy laws. The court rejected the competing interest argument, ruling that although the bank may have believed that local law precluded disclosure, it did "not excuse the Bank's failure to perform a diligent search upon receipt of the trial court's order of enforcement."[36]

The records at issue belonged to U.S. citizens, prompting the court to rule that there is a lower threshold for disclosure of this information to U.S. authorities, even if held by a foreign company in a country where such disclosure is illegal.[37] The bank argued that it was unfair to require it to be "put in the position of having to choose between the conflicting commands of foreign sovereigns".[38] The court was not persuaded by this point, stating that choosing between sovereigns is part of the cost of doing business for

---

[34] See *In re Grand Jury Subpoena* supra note 33 at note 7; see also *In re Arawak Trust Co. (Cayman), Ltd.,* 489 F. Supp. 162 (E.D.N.Y. 1980) (where the defendant bank was not subject to grand jury subpoenas where it had no office in the U.S. and merely maintained a U.S. bank account).
[35] *Re Grand Jury Proceedings the Bank of Nova Scotia*, 740 F.2d 817 (11 Cir.1984) ("*Bank of Nova Scotia*").
[36] *Ibid.,* at 26.
[37] *Ibid.,* at 30.
[38] *Ibid.,* at 31.

multinational corporations. It further concluded that the local laws should be of lesser interest to the bank since it suffered no hardship as a result of inconsistent enforcement actions.

Where the records sought do not involve a U.S. citizen, courts have still ruled in favour of U.S. authorities, particularly where the U.S. national interest is unquestionably strong.[39] For example, in *re Grand Jury Subpoena*, a case concerning international bribery charges, the court considered whether a grand jury subpoena could compel production of documents abroad where production was prohibited by local law. The court held the interest of the United States in enforcing its criminal laws outweighed any difficulties that the corporation may have faced in complying with the subpoena in contravention of the other state's law.[40] In *Ssangyong*, a New York branch of a Hong Kong bank was ordered to produce records from its head office even though doing so violated Hong Kong's bank secrecy laws.[41] The court held that control did not require legal ownership or actual physical possession; but rather only the ability to obtain the documents.

b. U.S. parent and foreign subsidiary

The situation is similar where the U.S. connection is a U.S. parent being compelled to obtain records from its foreign subsidiary. The courts have more often than not rejected the argument that a U.S. parent company does not have access to its subsidiary's records located abroad. The test for determining whether a U.S. court can order an U.S. parent corporation to produce the documents of its foreign subsidiary was formulated in *In Re Investigation of World Arrangements* as follows:

> (I)f a corporation has power, either directly or indirectly, through another corporation or series of corporations, to elect a majority of the directors of another corporation, such corporation may be deemed a parent corporation and in control of the corporation whose directors it has the power to elect to office.[42]

---

[39] *In re Grand Jury Subpoena dated August 9, 2000*, 218 F. Supp. 2d 544 *(S.D.N.Y. 2002)*.
[40] See also *United States v. Toyota Motor Corp*., 569 F.Supp. 1158 (C.D.Cal.1983) (Where the court enforced a court order directed to the parent company in Japan but served in the U.S. to the subsidiary).
[41] *Ssangyong Corp. v. Vida Shoes Int'l, Inc*., 2004 U.S. Dist. LEXIS 9101 (S.D.N.Y. 2004).
[42] 13 F.R.D. 280, 285 (D.D.C.1952). Qtd *In re Uranium Antitrust Litigation*, 480 F. Supp. 1138 at 1145.

In re Grand Jury Subpoenas duces tecum addressed to Canadian International Paper Company et al., the U.S. government attempted to obtain an order against a U.S. parent company for its Canadian subsidiary's refusal to disclose documents in connection with a grand jury investigation into alleged Sherman Act violations. The court dismissed the parent corporation's argument that it lacked possession of the documents, holding that the test was a matter of control, not location.[43] In *United States v. First Nat'l City Bank*, the court rejected the parent company's argument that it could not produce documents from its German office: "It is no longer open to doubt that a federal court has the power to require the production of documents located in foreign countries if the court has *in personam* jurisdiction of the person in possession or control of the material."[44]

Section 414 of the Restatement of Foreign Relations concerns jurisdiction with respect to subsidiaries. Section 414 (2)(b) allows a state to exercise jurisdiction over a parent company's subsidiary in "exceptional cases". Section 414 (2)(c) states that the burden of establishing reasonableness is reduced when the direction is issued to the parent corporation rather than the subsidiary.

V. The Privacy Implications

i. PIPEDA's application to U.S. disclosure powers

a. PIPEDA and third party disclosure

Canada's Personal Information and Electronic Documents Act (PIPEDA) establishes the obligations of organizations with regard to the data that they collect in the course of commercial activity.[45] Unless subject to a substantially similar provincial law, the act applies to every organization in Canada that collects, uses or discloses personal information.

---

[43] 72 F. Supp. 1013 (S.D.N.Y. 1947).
[44] 396 F.2d 897, 901 (2nd Cir, 1968); See also *United States v. Vetco, Inc.*, 691 F.2d 1281 (9th Cir. 1981).
[45] PIPEDA, S.C. 2000, c. 5.

PIPEDA addresses third party disclosures in Principle 4.1.3**.** It states that where organizations transfer data for processing, they must provide for a comparable level of privacy protection for the data through contractual or other means. Accordingly, organizations that transfer personal information must obtain sufficient contractual protections from third parties prior to transferring such information in order to comply with the statute.

This suggests that organizations subject to U.S. personal jurisdiction that disclose personal information without consent or prior disclosure in compliance with U.S. disclosure orders, whether granted by grand jury subpoenas, national security letters or FISA Section 215, risk violating PIPEDA unless (i) the organization obtained prior consent for the disclosure or (ii) the disclosure qualifies for one of the Act's exceptions. This issue is not limited to U.S. information management companies that compete for Canadian outsourcing contracts through their subsidiaries, however, since Canadian companies with a U.S. connection would presumably be subject to the same concerns.

b. Exceptions to Principle 4.1.3

PIPEDA includes several exceptions for disclosure of personal information without knowledge or consent. Section 7 (3) (c) enables an organization to disclose personal information where it is required

> "to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information"

The statute does not address whether foreign orders, such as those made by a FISA court or a grand jury can be considered as made by "a court, person or body with jurisdiction to compel" so as to fall within this exception. The statute is silent on the jurisdictional distinction making it possible that U.S. orders validly made under U.S. personal jurisdiction can be considered an exception.

None of the previous PIPEDA findings that address section 7 (3) (c) shed light on the question of foreign orders. In Finding #96, the Commissioner considered whether a

subpoena by a lawyer in Quebec (allowed under Quebec Civil Law) constitutes a proper subpoena under 7(3)(c). The Commissioner found that the subpoena was not proper because the powers granted to lawyers under Quebec Civil Law do not include compelling disclosure of records.[46]

Section 7 (3) c.1 permits disclosure without consent where the disclosure is made to a government institution where

> (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law.

The inclusion of foreign laws within this exception indicates that disclosure for U.S. counter-terrorism investigations through National Security Letters or Section 215 orders might qualify under the PIPEDA exceptions. The issue once again is whether "government institution" is limited to a Canadian government institution or if a foreign government institution could suffice. If the exception is limited to Canadian government institutions, U.S. authorities would likely need to tender their requests for disclosure through the Canadian Security Intelligence Service (CSIS) or the Canadian Department of Justice to qualify.

None of the Commissioner's findings focusing on section 7 (3) (c.1) address foreign requests. The language found in at least one decision indicates that the exception may not preclude foreign government request, however. The Commissioner opined in Finding #62 that it is "incumbent" on businesses "not to take the submissions of **any** government organization at face value" (emphasis added).

Section 9 (2.1) grants individuals the right to ask an organization whether it has disclosed information about them under section 7(3)(c) or (c.1) and to access that information. If information has been disclosed, Section 9(2.2) provides that the

---

[46] *Finding #96*, (December 3, 2002), Privacy Commissioner Decision, online:< http://www.privcom.gc.ca/cf-dc/cf-dc_021203_2_e.asp>.

organization must notify the requesting institution immediately and wait thirty days for any objections to disclosure. Section 9 (2.3) stipulates that the requesting institution can only object for purposes of national security (although the language does not say whether this is limited to Canadian national security), or for the enforcement of any law, including a law of a foreign jurisdiction, an investigation or for the gathering of intelligence. If the requesting institution objects, then Section 9(2.4) mandates that the organization refuse to provide the information to the individual and notify the Commissioner in writing. No PIPEDA findings have thus far interpreted sections 9 (2.1) – (2.4).

Although the federal Privacy Commissioner has yet to address the issue of disclosure to foreign jurisdictions, there are several findings that may be applicable. In Finding #106, a Canadian pilot did not have to disclose personal information to U.S. authorities where it was necessary to do so in order for him to participate in twice-yearly training on U.S. aircraft simulators. The Commissioner did not think that a reasonable person would find it appropriate to require pilots, who have already disclosed comparable information to Canadian authorities for a security clearance, to "consent to unacceptable collection and disclosure practices at the request of a foreign government." His airline employer was instead required to pay for European training where there were no disclosure requirements.[47] In another airline related case, a Canadian airline was found not at fault for collecting what a crew member argued was excessive amounts of personal information for U.S. transportation authorities. The Commissioner found that a reasonable person would have considered the collection appropriate with regards to compliance with U.S. legislation.[48]

Further, it should be noted that the *Public Safety Act, 2002*[49] recently amended PIPEDA to allow the collection and use of personal information without consent by certain private organizations for purposes of national security. The amendment allows air carriers and

---

[47] *Finding #106* (December 19, 2002), Privacy Commissioner Decision, online: <http://www.privcom.gc.ca/cf-dc/cf-dc_021219_7_e.asp>.
[48] *Finding #128* (March 4, 2003) Privacy Commissioner Decision, online: <http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030304_5_e.asp>.
[49] *An Act to amend certain Acts of Canada, and to enact measures for implementing the Biological and Toxin Weapons Convention, in order to enhance public safety*, SC 2004, C. 15.

reservation systems operators to collect certain passenger information and disclose it to domestic or foreign government officials and law enforcement.[50] The amendment has been heavily criticized by the Federal Privacy Commissioner who argues that the ability to obtain information from private sector businesses without prior judicial authorization is a significant expansion of the powers accorded to law enforcement officials in Canada.[51]

ii. Do the methods for compelled disclosure violate Canada's PIPEDA?

The language of PIPEDA is ambiguous with reference to disclosures to foreign law enforcement authorities, and there is little in the prior findings to provide guidance on this point. This leaves three possible interpretations of whether PIPEDA covers disclosures without consent under FISA orders, National Security Letters and Grand Jury subpoenas.

a. PIPEDA exceptions do not cover the disclosures

The first interpretation posits that the PIPEDA exceptions do not cover the disclosures. Although not explicitly stated in the statute, this interpretation would hold that the exceptions do not encompass disclosure to foreign law enforcement authorities without cooperation of a Canadian institution. If this is the case, disclosures made without consent under a FISA order, an NSL or a grand jury subpoena would result in a violation of PIPEDA.

b. PIPEDA exceptions cover the disclosures in the letter but not the spirit of the law

The second interpretation suggests that the PIPEDA exceptions cover disclosures to foreign law enforcement through its wording, though that this may not have been the intent of the law. It remains unclear whether Canadian legislations envisioned the

---

[50] Ibid., Clause 98.

[51] Privacy Commissioner of Canada, "Speech to Senate Standing Committee on Transport and Communications: Bill C-7, the Public Safety Act, 2002", 18 March 2004, online: <http://www.privcom.gc.ca/speech/2004/sp-d_040318_e.asp>.

prospect of disclosure requests from U.S. authorities, though it is noteworthy that Canada has similar disclosure provisions as those found in the Patriot Act. For example, Section 21 of the Canadian Security Intelligence Act provides for a warrant that permits almost any type of communication interception, surveillance or disclosure of records for purpose of national security. The application is made by the Director of the CSIS or a designate of the Solicitor General to a Federal Court judge. The application must contain an affidavit stating "the facts relied on to justify the belief, on reasonable grounds, that a warrant is required".[52] The application must also outline why other investigative techniques are inappropriate. The warrant will typically last 60 days and is renewable on application. Section 21 orders could presumably also be applied to U.S. companies operating in Canada.

The Section 21 warrant is arguably similar to a Section 215 application made to the FISA court – both do not necessitate probable cause and both can be used to obtain any type of records or any other tangible thing. Moreover, the target of both warrants need not be the target of the national security investigation. Like a FISA application, a Section 21 application is usually heard ex parte. The PIPEDA amendment in the *Public Safety Act* which allows collection and use of information without consent for national security purposes further underscores the potential disclosure of sensitive information by private organizations to Canadian law enforcement.[53]

CSIS works closely with foreign counterparts on counter-terrorism and intelligence investigations. Indeed its mandate includes working with U.S. law enforcement agents to prevent the planning of terrorist activities abroad. It is worth noting that CSIS worked with legislators to redraft PIPEDA to include a national security clause (now section 7 (3) (c.1)). CSIS wanted to ensure that PIPEDA exempted disclosures to investigative agencies to accommodate national security concerns or anti-terrorism activities.[54] CSIS's public concern about exempting access to records for investigative agencies

---

[52] *Canadian Security Intelligence Act*, 1984, c. 21, s. 1. Section 21(2)(a).
[53] See *Public Safety Act supra* note 50.
[54] "CSIS pushed to alter privacy bill: Spy agency wanted security concerns addressed". The Ottawa Citizen, (January 7, 2004).

suggests that legislators might have considered whether foreign and specifically U.S. investigative agencies would also qualify for the exemption.

c. PIPEDA exceptions cover the disclosures

The third interpretation of the PIPEDA exceptions is that they cover disclosures to U.S. law enforcement as the provisions are interpreted broadly to cover non-Canadian jurisdictions. The language does not explicitly prevent disclosure to foreign authorities, and indeed even makes several references to the laws of foreign jurisdictions in 7 (3) (c) and (c.1). If this is the case, the application of U.S. law to companies under U.S jurisdiction would likely not violate PIPEDA.

VI. Recommendations

Several measures might help to eliminate or appropriately mitigate privacy risks from disclosures to U.S. law enforcement. These measures include banning government outsourcing of sensitive data, pursuing agreements with U.S. law enforcement on procedures to facilitate disclosures requests where Canadian companies are concerned, implementing legislation to block disclosures to U.S. law enforcement (a blocking statute), and redrafting PIPEDA to provide more protection for Canadian data. In considering which remedies to implement, there are a number of factors to be considered.

1. **The risk of disclosure is not limited to U.S. parent businesses with Canadian subsidiaries**. Any Canadian business with a subsidiary or office in the U.S. can also be subject to disclosure orders to U.S. law enforcement.

2. **The Patriot Act has not dramatically changed the ability to gather information without consent**. The Patriot Act's effect on U.S law enforcement ability to compel production from a parent company or a subsidiary without probable cause and without notice is not significantly different than that which was available in a pre-Patriot Act era through grand jury subpoenas and national security letters.

3. **PIPEDA may allow for disclosures to U.S. law enforcement**. It is unclear whether a disclosure without consent to U.S. law enforcement contravenes PIPEDA as the language of the statute arguably allows for such a disclosure.

4. **Canada has also enacted provisions that permit disclosure without consent**. Canada has similar national security legislation to the U.S. that permits disclosure of information for terrorism related investigations. Language was added to PIPEDA to exempt such personal information disclosures. Further, since CSIS works closely with U.S. law enforcement agencies on terrorism investigations it is possible that U.S. requests for disclosure could be initiated through CSIS.

These factors should be helpful in considering whether a measure is able to both protect the integrity of Canadian personal information while at the same time not limit the ability of government agencies to perform their jobs effectively.

i. A ban on government outsourcing

The BCGEU has called for a ban on government outsourcing of sensitive data. Although a governmental ban would potentially address the immediate issue of protecting the privacy of B.C. medical data, it does not address the wider privacy issue caused by the application of U.S. law to Canadian businesses. An effective ban on outsourcing would affect not only U.S. companies and their Canadian subsidiaries, but also any Canadian company that is subject to U.S. personal jurisdiction. Any ban would thus become ineffective should third party consultants or others come into possession of the data, even within Canada.

A ban would also create an unfortunate disparity between the protection afforded to publicly held data and privately held data, a distinction that federal legislators tried to eliminate with the establishment of PIPEDA. It is arguable whether in all cases government data is more sensitive than privately held data. Many Canadian citizens

would be more concerned about having their private emails or bank information disclosed to the FBI, rather than their medical information.

Moreover, even personal information in government hands may still be subject to a U.S. court order. Although the Act of State Doctrine (AOSD), a U.S. common law principle, requires courts to decline to exercise jurisdiction over cases that may embarrass or impede the political branches of government in their conduct of foreign affairs, requests for AOSD are rarely granted. In *W.S. Kirkpatrick v. Environmental Tectonics* the court of appeal rejected AOSD and granted anti-corruption action for a bribe paid to the Nigerian government for a defense contract because the State Department was satisfied that foreign policy would not be compromised by the litigation.[55] In *Curtiss-Wright*, the court held that "the act of state doctrine should not be applied to thwart legitimate American regulatory goals in the absence of a showing that adjudication may hinder international relations."[56] Furthermore, the *Foreign Sovereign Immunities Act* (*FSIA*) features several AOSD exceptions, the most relevant of which arises in context of commercial activity of a foreign state.[57] FSIA has been used to obtain judgment against government arms of Argentina, Nigeria and Cuba amongst others.[58]

ii. Informal or formal agreements with FBI on procedures relating to access to Canadian records.

Law enforcement agencies in Canada and the U.S. currently employ a harmonized approach to sharing information related to cross-border crime, terrorist activity and immigration matters. A post 9/11 agreement between Canada and the U.S. establishes a thirty point action plan for creating a secure border.[59] Integrated intelligence is one of

---

[55] 847 F.2d 1052 (3rd Cir. 1987). This case is considered by commentators as the death knell of the Act of State Doctrine.
[56] *Williams v. Curtiss*-Wright, 694 F.2d 300 (3rd Cir. 1982) at 304.
[57] *Foreign Sovereign Immunities Act of 1976* (FSIA), 28 U.S.C.S. § 1604.
[58] See *e.g. Verlinden B.V. v. Cent. Bank of Nigeria*, 461 U.S. 480 (1983); *Republic of Argentina v. Weltover, Inc.*, 504 U.S. 607 (1992); *Alfred Dunhill of London, Inc. v. Republic of Cuba*, 425 U.S. 682 (1976).
[59] Canada-US 30 Point Action Plan (December 12, 2001), online: DFAIT website <http://www.dfait-maeci.gc.ca/can-am/menu-en.asp?act=v&mid=1&cat=10&did=1670>.

eight action items oriented towards coordination and information sharing, including joint data sharing and intelligence analysis. Canada has also established Integrated National Security Enforcement Teams (INSETs) to fight terrorist threats. INSETs include representatives from federal enforcement and intelligence agencies, as well as U.S. law enforcement agencies on a case-by-case basis. The federal government has identified increased joint anti-terrorism efforts as a priority.[60]

A formal or informal agreement on procedures relating to Section 215 orders where Canadian records are at issue may provide additional protection to ensure that disclosures of sensitive personal information occur only for legitimate purposes. Such an agreement could provide for notice to Canadian law enforcement, procedures for treatment and retention of information and limits on the type of information that can be requested. It is worth noting that a similar arrangement already exists for sharing immigration information between Citizenship and Immigration Canada, U.S. Immigration and Naturalization Service and the U.S. Department of State.[61]

iii. Blocking statutes

One of the only effective means of deterrence to disclosure of records to U.S. law enforcement is a blocking statute, which allows a petitioner to mount a foreign compulsion defence in a U.S. court action. The Restatement on Foreign Relations acknowledges their effect through section 442. A blocking statute is enacted to prevent compliance by a domestic entity with a specific foreign law such that compliance would lead to penalties and/or require explicit permission from the domestic government. An example of a Canadian blocking statute is the *Foreign Extraterritorial Measures Act ("FEMA")*.[62] FEMA prevents a Canadian corporation from complying with the disclosure orders of a foreign antitrust or international trade action without the specific permission of Canada's Attorney General. The *Ontario Business Records Protection Act*,

---

[60] Smart Border Declaration (December 12, 2001), online: DFAIT website <http://www.dfait-maeci.gc.ca/can-am/menu-en.asp?act=v&mid=1&cat=10&did=1669>.
[61] *Statement of Mutual Understanding (SMU) on Information-Sharing*, Citizenship and Immigration Canada website, <http://www.cic.gc.ca/english/policy/smu/smu-ins-dos.html>.
[62] *Foreign Extraterritorial Measures Act*, R.S. 1985, c. F-29.

which prohibits the disclosure of Ontario records outside the normal course of business, provides another example.[63]

Canadian blocking statutes have historically been enacted in response to U.S. antitrust laws (*Sherman Act*) or laws that prohibit trade with Cuba (*Helms-Burton*, *Trading with the Enemy Act* ("TWEA"), *Cuban Assets Control Regulations* ("CACRs")); however, there is potential for the use of blocking statutes to protect the privacy rights of Canadians against section 215 or other disclosure to U.S. law enforcement.

According to the case law, the following factors would be necessary for a blocking statute to be successfully used as a defence in a U.S. court to prevent disclosure:

1. ***The blocking statute must be specific and exclusive, not allowing the entity to comply with both Canadian law and the foreign law.***

In *United States v. Brodie*, the blocking statutes of Canada, United Kingdom and the European Union were considered in relation to a Helms-Burton prosecution.[64] The court rejected the argument that FEMA prohibited a Canadian entity from complying with the TWEA and the CACRs because FEMA did not prevent the company from complying with both laws.

The court read FEMA as prohibiting persons from "not trading with Cuba" if the decision to do so was exclusively because of the CACRs. FEMA did not criminalize compliance with the CACRs or compel corporations to trade with Cuba. Since companies could decide not to trade with Cuba for any other reason, it would therefore be possible to comply with both laws. This is consistent with previous U.S. courts decisions which deny a conflict where it is possible to comply with both foreign and U.S. law.[65]

---

[63] R.S.O. 1990, c. B.19, 2(2).
[64] 174 F. Supp. 2d 294 (E.D. Pa. 2001)
[65] See *Timberlane Lumber Co. v. Bank of America*, 549 F.2d 597, (9th Cir. 1977), *Hartford Fire Ins*, 509 U.S. 764 (1993).

The *Brodie* court opined that for the petitioner to mount a successful foreign sovereign compulsion defence it would have to prove that its motivation for trading with Cuba was based on fear of prosecution under Canadian law and that it could not have legally refused to accede to the Canadian government wishes.[66] Moreover, case law demonstrates that U.S. courts tend to be more deferential to the foreign law where it is oriented to domestic use and not only to thwart foreign prosecution.[67]

2. The blocking statute must have a tangible sanction attached

A bona fide compulsion to comply with the foreign law through tangible sanctions for non-compliance is necessary for U.S. court deference. In *Brodie*, the court noted that no information was submitted regarding enforcement under FEMA or the equivalent British law, whether anyone had ever been prosecuted under FEMA or what evidence would be sufficient to establish a violation of the law. The court concluded that there was no such threat of sanction because there was no realistic possibility of prosecution under these laws.

In *Societe Internationale*, the U.S. Supreme Court deferred to the foreign blocking statute because there was a tangible penal sanction for complying with the U.S. law.[68] Societe Internationale ("SI") a Swiss corporation, failed to comply with a grand jury order requiring it to disclose records relating to litigation. SI countered that it was prevented by Swiss banking secrecy law from turning over the documents and the Swiss government even confiscated the relevant records to prevent disclosure. The U.S court held that a specific order or action satisfies the need for a real threat of prosecution and penal sanctions under the foreign law. It arrived at a similar conclusion in *Krupp Mak Maschinenbau*, where a German court ordered a German bank not to comply with a United States grand jury subpoena concerning investigation of its client, causing the subpoena to be dropped. In *In re Uranium Antitrust Litigation* the motion to compel

---

[66] See also *United States v. Watchmakers of Switzerland Information Center*, Inc., 1963 Trade Cases (CCH) P 70,600 (S.D.N.Y.1962), *Mannington Mills, Inc. v. Congoleum Corp*., 595 F.2d 1287 (3rd Cir. 1979).
[67] See *e.g. White v. Kenneth Warren & Son, Ltd*. 203 F.R.D. 369 (2001) and *Reinsurance Co. of America, Inc. v. Administratia Asigurarilor de Sta*t 902 F.2d 1275 (7th Cir. 1990)
[68] 357 U.S. 197 (1958).

disclosure was dropped against one Canadian company because the records in question had been confiscated by the Canadian Ministry of Energy for safekeeping on the basis of a non-disclosure statute.[69]

The presence of criminal sanctions does not guarantee deference to the blocking law, however. In fact, the Seventh Circuit has specifically stated that criminal sanctions in the foreign country based on disclosure to U.S. authorities "does not automatically bar a domestic court from compelling production."[70]

Unlike the Swiss law at issue in the *Societe Internationale* case, it should be noted that Canada's privacy laws do not include any criminal sanctions. Contraventions of the *Ontario Business Records Protection Act* are prosecuted as contempt of court and are liable to one year's imprisonment. However, U.S. courts have not granted the statute high deference due in part to its lax enforcement.[71]

3. A U.S criminal investigation will result in a higher threshold for courts to accept a foreign defence.

The foreign sovereign compulsion defence has rarely been applied to a criminal context as U.S. courts generally find the U.S. interest in prosecution as outweighs any foreign interests. According to *Brodie*, "the fact that a criminal suit has been brought demonstrates the executive branch's determination that the injury to the United States from the alleged conduct outweighs the potential injury to foreign relationships."

In contrast, in an estate matter, the court deferred to the British law that prohibited disclosure of documents. The court's decision was also influenced by the strong civil penalties that awaited the plaintiff if he produced the documents, in addition to the fact

---

[69] *Krupp Mak Maschinenbau G.m.b.H v. Deutsche Bank A.G.*, 22 Int'l Leg. Mat. 740 (1983); *In re Uranium Antitrust Litigation* 480 F. Supp. 1138 (N.D. Ill. 1979).
[70] *United States v. First National Bank of Chicago*, 699 F.2d 341, 345 (7th Cir. 1983).
[71] See *Snowden v. Connaught Laboratories, Inc*., 138 F.R.D. 138 (D.C. Kan. 1991) (where "the court suspects that the statute most likely has not been strictly enforced"); *General Atomic Co. v. Exxon Nuclear Co.*, 90 F.R.D. 290 (S.D. Cal. 1981) and *In re Uranium Antitrust Litigation* (In both cases, arguments relying on the Ontario Act was quickly dismissed).

that the law was oriented to domestic purposes, and not as a blocking statute.[72] In a case concerning the production of documents from Romania for a civil litigation, the court found that U.S. interests are more compelling where national security, tax and patent laws, and antitrust laws were at issue. In that case, the U.S. interest involved was protecting the finality of judgments, which did not outweigh Romania's state secret laws. Consistent with the *White* case, it was important to the court's analysis that strict penalties were involved in the Romanian law at issue, and that the law's objective was not to protect Romanian companies from foreign discovery requests.[73] In both cases above, the courts used Section 442 (1)(a) of the *Restatement of the Foreign Relations Law* to conclude that they did not have jurisdiction to order disclosure.

4. The Defendant must make a good faith attempt to comply with U.S. law

Where U.S. courts have deferred to foreign blocking statutes, there has usually been a good faith attempt to comply with U.S. law. The court in *Societe Internationale* noted that there was no willfulness or bad faith on the part of the petitioner in his inability to comply with the production order, as the petitioner had already produced over 190,000 documents. U.S. courts expect petitioners who face legal obstacles under the laws of their own countries to demonstrate good faith efforts to comply with both legal obligations.

U.S. courts view blocking statutes as one factor in their decision on whether to order disclosure. The Supreme Court has stated that "the blocking statute thus is relevant to the court's particularized comity analysis only to the extent that its terms and its enforcement identify the nature of the sovereign interests in nondisclosure of specific kinds of material."[74] The existence of a blocking statute to prevent disclosure therefore does not prevent the exercise of the ordering of disclosure for anyone subject to U.S. personal jurisdiction.

---

[72] *White v. Kenneth Warren & Son, Ltd supra* note 67.
[73] *Reinsurance Co. of America, Inc. v. Administratia Asigurarilor de Sta*t supra note 67.
[74] *Societe Nationale Industrielle Aerospatiale v. United States Dist*., 482 U.S. 522 (1987).

A blocking statute that successfully prevents disclosure of Canadian records to U.S. law enforcement without due process would have to be (i) exclusive by not allowing companies under Canadian jurisdiction any option but to comply; (ii) rest on the fundamentals of Canadian privacy laws, so that they are based on domestic objectives, rather than attempts to thwart Patriot Act powers; and (iii) contain tangible sanctions and feature consistent enforcement for the law to appear serious to U.S. courts. Given the growing concern over the potential applicability of foreign law to Canadian data, a stronger Canadian privacy statute may be warranted.

iv. Greater clarity for PIPEDA

Whether considered alone or in tandem with other measures, it would be useful for the legislation to provide greater clarity on PIPEDA's jurisdictional scope. As discussed above, PIPEDA's broad language suggests that it is possible that the statute exempts disclosures to U.S. law enforcement agencies. An interpretative document on PIPEDA's jurisdictional scope or a statutory amendment to clarify the language would aid Canadian companies in understanding their responsibilities in regards to requests from foreign law enforcement. Changes could come in the context of the legislative review that is scheduled for next year.

VII. Conclusions

The B.C. request for comment raises two questions. First, whether the USA Patriot Act permits U.S. authorities to access the personal information of Canadians and second, if so, whether Canadian federal and provincial privacy legislation applies to potential disclosures to U.S. law enforcement.

Our analysis concludes that U.S. law does indeed grant law enforcement authorities the power to compel disclosure of personal information without notifying the targeted individual that their information is being disclosed (in fact, disclosing the disclosure is itself a violation of the law). Moreover, the application of these laws is not limited to U.S. companies but actually applies to any company with sufficient U.S. connections such that it could find itself subject to the jurisdiction of the U.S. courts. This is true both for U.S. companies operating subsidiaries in foreign countries as well as for foreign companies with U.S. subsidiaries.

While we have not assessed the applicability of the B.C. privacy statute, we conclude that it is unclear whether disclosures compelled by U.S. law would constitute a PIPEDA violation. While the law requires user consent where personal information is disclosed to a third party, the statute contains several exceptions to this general rule that might apply in this situation.

Given the public concern surrounding this issue, we provide four recommendations on how to eliminate or appropriately mitigate the privacy risks arising from any such disclosures. These include considering a ban on governmental outsourcing, establishing a formal or informal agreement with U.S. law enforcement agencies on requests involving Canadian data, amending PIPEDA to meet the U.S. blocking statute standard, and clarifying the jurisdictional reach of PIPEDA.