OUTSOURCING OUR PRIVACY?: PRIVACY AND SECURITY IN A BORDERLESS COMMERICAL WORLD

Michael Geist* and Milana Homsi**

I. Introduction

January 1, 2001 stands as one of the highpoints in recent Canadian privacy history. Following years of discussion, drafting, and debate, Canada's national privacy legislation took effect on that New Year's Day. The *Personal Information Protection and Electronic Documents Act (PIPEDA)*[1] initially applied solely to federally regulated organizations, though three years later that limitation expired and it was extended to all organizations in Canada.[2] The law provided Canadians with a new series of privacy rights and the promise that the Federal Privacy Commissioner would act on their behalf in the event that those rights are not respected.

Less than 10 months later, the priority ascribed to privacy in *PIPEDA* was called into question as terrorists struck the United States on September 11, 2001. In the immediate aftermath of 9/11, the balance between privacy and security was fundamentally re-evaluated in both Canada and the United States. Law enforcement, particularly in the U.S., demanded and received significant new powers. The centrepiece of this shift in the United States was the enactment of the *USA Patriot Act*, a lengthy statute that dramatically increased the scope of permitted law enforcement surveillance and investigative techniques.[3] Alarmed critics reacted to these changes, and argued that these new powers encroached on longstanding privacy rights and civil liberties.

---

* Canada Research Chair in Internet and E-commerce Law, University of Ottawa, Faculty of Law.

* LL.B., Milana Homsi articled at Stikeman Elliott LLP in Toronto in 2004-05 and is currently an associate at Wilson, Sonsini, Goodrich and Rosati in Palo Alto, California.

An earlier version of this article was submitted to B.C. Privacy Commissioner David Loukidelis in July 2004.

[1] The *Personal Information Protection and Electronic Documents Act*, R.S.C., 2000, c-5 [*PIPEDA*].

[2] See *PIPEDA* Implementation Schedule, online: Office of the Privacy Commissioner of Canada <http://www.privcom.gc.ca/legislation/02_06_02a_e.asp>.

[3] *The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* of 2001, Pub. L. No. 107-56, 115 Stat. 272 [*USA Patriot Act*].

This ongoing tension between privacy and security rights captured the attention of the Canadian public in an interesting and unexpected manner in the summer of 2004. As part of the global shift toward cost-efficient data outsourcing, the British Columbia government proposed outsourcing the management services associated with its Medical Services Plan.[4] The proposal was challenged by the affected union. It argued that the data generated under the plan,[5] which included sensitive health information, could be put at risk due to provisions found in the *USA Patriot Act*. Sceptics dismissed the union's opposition as a transparent attempt to protect local labour, but the concerns resonated with a wide range of communities, including privacy advocates, civil liberties groups, and health care activists.[6] Soon after, David Loukidelis, the British Columbia Privacy Commissioner, called for a public study into the matter.[7]

Months later, the issue remains at the forefront of privacy policy in Canada. The British Columbia government quickly introduced and passed legislation designed to temper public concern,[8] yet the clash between privacy rights and security interests remains on the federal privacy agenda. The debate is further complicated by a growing commercial dependence on data outsourcing arrangements.

This article examines the competing interests raised by this issue. We unpack the legal arguments raised by both the business community in support of data outsourcing arrangements.[9] As well, we explore those expressed by the privacy community, which maintains that additional legal protections are needed in order to provide the public with the effective privacy protections envisioned by *PIPEDA*.[10]

---

[4] B.C. Ministry of Health Services, News Release, "New Service Delivery Model to Improve MSP" (29 July, 2003) http://www2.news.gov.bc.ca/nrm_news_releases/2003HSER0038-000687.htm.

[5] *British Columbia Government & Services Employees' Union v. The Minister Of Health Services*, (Filed 23 February 2004) Victoria VIC-S-S-040879 (BCSC).

[6] The Right to Privacy Coalition was launched in June 2004 by a wide variety of B.C. and Canadian organizations and labour groups concerned about the privacy protection of health care information. See http://www.righttoprivacycampaign.com.

[7] Office of the Information and Privacy Commissioner for British Columbia, News Release, "BC Privacy Commissioner to Examine Implications Of *USA Patriot Act* on Government Outsourcing"(28 May, 2004).

[8] Bill 73, *Freedom of Information and Protection of Privacy Amendment Act*, 5th Sess., 37th Parl., 2004.

[9] See for example, the submission to the OIPC by the Information Technology Association of Canada, August 5, 2004, available online: Office of the Information and Privacy Commissioner <http://www.oipcbc.org/sector_public/usa_patriot_act/pdfs/ITAC(08052004).pdf>.

[10] See *e.g.*, Memorandum from Christopher Calabrese on behalf of the ACLU to the Office of the Information and Privacy Commissioner of British Columbia (10 August 2004) online: OIPCBC <http://www.oipcbc.org/sector_public/usa_patriot_act/pdfs/American%20Civil%20Liberties%20Union.pdf>.

Part two of the article examines the phenomenal growth of data outsourcing and its implications for privacy protection. We chronicle the privacy controversy in B.C. regarding data outsourcing and place the issue in a global context, given the similar concerns expressed in other jurisdictions worldwide.

Part three assesses the power of U.S. authorities to compel the disclosure of personal information held by both U.S. and foreign companies. While the *USA Patriot Act* is frequently used as shorthand for the extra-territorial application of U.S. law, the reality is that law enforcement authorities can employ a wide range of options to compel disclosure, the vast majority of which predate the enactment of the *USA Patriot Act*. Moreover, a close examination of U.S. law and practice demonstrates that law enforcement authorities, supported by national courts, regularly apply U.S. law to any entity provided the organization is subject to U.S. personal jurisdiction, regardless of geographic location,.

After considering the effect of U.S. law, part four then turns to the Canadian response. We focus on *PIPEDA*, and highlight the strengths of the new privacy statute. We also assess the significant limitations that likely preclude *PIPEDA*'s effectiveness in prohibiting a Canadian entity from disclosing personal information to U.S. authorities if required to do so under a court order.

In part five, we conclude our analysis by outlining several recommendations for Canadian legislative reform that could help restore the balance between security and privacy. These include *PIPEDA* amendments that would raise the legislation to the status of a "blocking statute". Canadian organizations could then credibly argue that they are prohibited from complying with foreign court orders.

II. The Clash of Three Titans: Business Efficiency vs. Privacy vs. Security

The use of third party contractors to manage information technology and data has increased dramatically in recent years. Companies and governments frequently find that "outsourcing" is more efficient and cost effective for tasks like payroll management, data processing, and systems maintenance, compared with undertaking them in-house.[11] This move toward outsourcing is a global phenomenon, and is exempli-

[11] A 2004 PriceWaterhouseCooper white paper predicts that Canadian businesses will increasingly turn to outsourcing for IT management. See PriceWaterhouseCooper and David Ticoll, "A Fine Balance: The Impact of Offshore IT Services on Canada's IT Landscape", (April 2004).

fied in many industrial countries like the United Kingdom and the U.S.[12]

Notwithstanding privacy concerns, Canadian governments are attracted by significant potential cost savings, and have outsourced various services at both the federal and provincial levels. For example, Maximus, a leading multinational outsource provider, has maintained the British Columbia Family Maintenance Enforcement Program since 2002.[13] At the federal level, the Canada Revenue Agency contracted with CGI Group, a leading Canadian outsourcer, in December 2004 to provide large-scale information technology services.[14] Moreover, demand for government data management is expected to grow substantially.[15] As the Canadian experience illustrates, governments award the majority of financially significant outsourcing contracts to large multinational firms such as Maximus, CGI Group, Lockheed Martin IT, EDS and Accenture. All of these firms are either based in the United States or maintain sizable U.S. practices.

The growing popularity of outsourcing coincides with the public's heightened sensitivity to privacy protection. The rise of identity theft in Canada,[16] the barrage of personalized marketing, and news stories about cross-border data-sharing have increased consumer fears that personal information is regularly placed at risk.[17]

Controversy over Canadian government outsourcing to U.S. companies first emerged in spring 2004 with the revelation that Statistics Canada awarded a 2006

---

[12] See "*UK public sector outsourcing: the big picture to 2007/08*", Kable Research, Study, December 2004. The United Kingdom government's use of outsourcing is expected to grow by almost 50% by 2006 to £67 billion (approximately $126 billion U.S.) Also see: Andy McCrue, "Global IT outsourcing deals rocket up to $163bn", January 18, 2005, Silicon.com. In the U.S., the information technology outsourcing market grew to $163 billion (U.S.) in 2004, with government procurement comprising a healthy share of the overall total.

[13] The original contract was given to Themis Ltd., a local company. It was acquired by Maximus in 2002. See Themis Ltd., website for further information about its government outsourcing work <http://www.themis.bc.ca/about.html>.

[14] CGI, News Release, "The Canada Revenue Agency Selects CGI for Key IT Initiatives" (9 December 2004) online: <http://www.cgiusa.com/web/en/news_events/press_releases/2004/332.htm>.

[15] "Accenture to hire 550 in Canada" *Tech Investor* (January 14, 2005) online: Canoe News <http://cnews.canoe.ca/CNEWS/TechNews/TechInvestor/2005/01/14/898632-cp.html>.

[16] In 2003, there were 13,359 incidents of identity theft in Canada, an increase of 5172 since 2002. See "Phonebusters statistics on phone fraud" online: Phonebusters <http://www.phonebusters.com/english/statistics.html>.

[17] For concerns about cross-border data sharing, see e.g. Jim Bronskill, "Ottawa's security plan to collect more traveller information in limbo" *CNEWS* (21 October 2004) online: Canoe News http://cnews.canoe.ca/CNEWS/Canada/2004/10/21/679643-cp.html. See also David Akin, "CIBC faxes go to scrapyard", *The Globe and Mail* (26 November 2004) online: Globe and Mail <http://cibc-dayone.notlong.com>.

census contract to the Canadian subsidiary of Lockheed Martin.[18] A small but vocal opposition pressured the federal government to place limits on that outsourcing contract. The government eventually assured Canadians that their personal information would not be disclosed during the census collection process.[19]

Concern over the privacy risks associated with outsourcing gained national momentum when the B.C. Government and Services Employees' Union ("BCGEU") campaigned in opposition contracting the B.C. Medical Services Plan out to U.S.-based multinational corporations.[20] The campaign was in response to a Request for Proposals issued by the B.C. Ministry of Health Services, which sought a private partner to operate its Medical Services Plan. The BCGEU subsequently filed a petition, seeking a declaration that the contracting out of services contravened the *Medicare Protection Act,* the *Canada Health Act* and the *B.C. Freedom of Information and Protection of Privacy Act (FOIPP).*[21]

Armed with an American Civil Liberties Union (ACLU) opinion concluding that the *USA Patriot Act* could be used to compel secret disclosure of personal health information,[22] the BCGEU asked Commissioner Loukidelis to hold a public inquiry into the matter. In the interim, the BC government placed the contract on hold, pending the resolution of the case.[23]

The B.C. Privacy Commissioner's request for comment concerning the privacy implications of the *USA Patriot Act* on outsourcing received more than 500 submissions from across Canada and around the world.[24] Just days prior to the release

---

[18] Jill Mahoney "Census at risk if U.S. firm in on it, critics say" *The Globe and Mail* (14 October 2003) A4. See also Vive le Canada, Press Release "Pro-Canadian Website Calls Census Boycott" (28 April 2004) online: ViveLe Canada <http://www.vivelecanada.ca/article.php?story=20040508114837477&query=lockheed%2Bmartin>.

[19] See Statistics Canada, Press Release, "Role of private contractors in the census" (13 May 2004) online: Statistics Canada <http://www12.statcan.ca/english/census06/info/outsource/outsourcing.cfm>.

[20] British Columbia Government & Services Employees Union [BCGEU], Alert, "BCGEU calls for public inquiry on government contracts"(10 May 2004).

[21] *British Columbia Government & Services Employees' Union v. The Minister of Health Services*, (Filed 23 February 2004) Victoria VIC-S-S-040879 (BCSC).

[22] Jameel Jaffer, Affadavit in support of BCGEU, Sworn February 23, 2004. available online: BCGEU <http://www.bcgeu.ca/bbpdf/040309_us_patriot_act.pdf>.

[23] The B.C. government originally planned to start negotiations with Maximus soon after it announced the selection in March 2004. The original contract was slated to be signed in August 2004. Ministry of Health Services, Information Bulletin, "MSP Service Delivery Model to Improve Client Service" (31 March 2004).

[24] See the posted submissions on the OIPC website at: <http://www.oipcbc.org/sector_public/usa_patriot_act/submissions.htm>.

of the Office's report, the B.C. government introduced Bill 73 to amend the public sector privacy act, *FOIPP*, in order to provide more robust privacy protection against disclosure to foreign authorities without consent.[25] Most stringently, the law now prohibits provincial government entities from outsourcing data beyond Canada's borders: personal information must be stored and accessed only in Canada, unless prior consent has been obtained from any affected persons.[26]

The *FOIPP* was also broadened to apply to private sector organizations engaged in contract work for provincial governments.[27] Most importantly, it prohibits disclosures of data for the purpose of complying with a non-Canadian subpoena, obligates those affected to disclose such a subpoena to the Minister responsible and makes individuals liable for contraventions of the Act.[28] The Information and Privacy Commissioner is also granted the authority to issue binding orders against contractors regardless of whether they are public or private.

Notwithstanding the introduction of Bill 73, Commissioner Loukidelis issued his report. It contained several recommendations designed to minimize the risk of outsourced data disclosure to foreign law enforcement.[29] Contractual issues between public bodies and private sector information management companies were addressed, as well as legal restrictions to protect the integrity of outsourced data. The B.C. government had already implemented several of the Bill 73 recommendations, including a prohibition on the transfer of personal information in the control of a public body outside Canada for data management, and a requirement that information management companies notify the government when a disclosure request by a foreign government is made.[30]

The high-profile case quietly came to a close in March 2005. A B.C. court gave the government the go-ahead to outsource data to Maximus.[31] The court affirmed the importance of privacy protection but allowed the outsourcing largely due to a series

---

[25] The public sector act is the *Freedom of Information and Protection of Privacy Act [FOIPP]*.

[26] Bill 73, Section 30.1; This approach is similar to one found in a recent California privacy bill, ultimately vetoed by California Governor Arnold Schwarzenegger, that limited the outsourcing of medical data to foreign countries without the consent of the individuals to whom the data pertains.

[27] Bill 73, Section 31.1 (b)

[28] Bill 73, Section 30.2 (1).

[29] British Columbia Office of the Information & Privacy Commissioner, *Privacy & the USA Patriot Act - Implications for British Columbia Public Sector Outsourcing* (29 October 2004) at 133-137 ("OIPC Report") online: OIPCBC <http://www.oipcbc.org/sector_public/usa_patriot_act/patriot_act.htm>.

[30] *Ibid.* at 134.

[31] *BCGEU v. British Columbia (Minister of Health Services)*, 2005 BCSC 446.

of significant new protections introduced by Maximus in response to the public outcry. These included a $35 million penalty for breach of confidentiality, extensive provisions to ensure that the data remained in the province, and a contractual term prohibiting disclosure of the data.

Although the B.C. case generated global attention,[32] Canada's experience is not unique. The issue was brought to the Australian government, which promised to investigate the impact of the *USA Patriot Act* on Australian government outsourcing contracts.[33] Meanwhile, citizens in Mexico and several other Latin American countries expressed fear that the U.S. Immigration and Naturalization Service obtained access to national driving record and voter databases after they were sold to a U.S. company.[34] In the wake of those revelations, those countries launched investigations and soon generated proposals for stronger data protection laws.[35]

In fact, even the U.S. has witnessed fears over the privacy impact of data outsourcing. The California legislature passed a bill requiring companies to notify consumers prior to any transfers of medical data to offshore outsourcing providers, though Governor Schwarzenegger ultimately vetoed that legislative initiative.[36] Senator Hillary Clinton introduced a similar bill in Congress in 2004, calling for the creation of a private right of action for damage arising from the improper sharing of personally identifiable information by a foreign affiliate.[37] A second Clinton bill targeted the transmission of personally identifiable information to foreign affiliates and subcontractors.[38]

With the Canada's experience mirrored elsewhere, it is apparent that the growing trend of government outsourcing to multinational corporations is on a collision course with public concerns for personal privacy. This potential clash between economic efficiency and privacy, along with national security, has led to a volatile pub-

---

[32] Declan McCullagh, "Labor groups raise outsourcing privacy concerns", News.com (26 July 2004) online: News.com <http://news.com.com/Labor+groups+raise+outsourcing+privacy+concerns/2100-1011_3-5283935.html>

[33] Simon Hayes, "U.S. law raises privacy worries", *News.com.au* (2 November 2004) online: News.com <http://www.news.com.au/common/story_page/0,4057,11256981%255E15319,00.html>.

[34] "Mexico to investigate who sold citizens' personal data to Washington", *Associated Press* (15 April 2003). See also EPIC's Choicepoint Page, online: Electronic Privacy Information Center <http://www.epic.org/privacy/choicepoint/>.

[35] *Ibid.*

[36] U.S., S.B. 1492, *An Act to add Chapter 6.5 to Part 2.6 of Division 1 of the Civil Code, relating to confidential information*, 2004, Reg. Sess., Cal., 2004 (Passed by Senate August 27, 2004, vetoed by Governor September 29, 2004).

[37] U.S., Bill S.6, SAFE-ID Act, S. 2312, 108th Cong. § 3 (2004).

[38] *Ibid.*

lic policy debate that hinges on the two key legal questions: first, to what extent can foreign authorities compel the disclosure of personal information? Second, assuming that at least some compulsion is possible, what legal responses are available to restore public confidence in personal privacy?

III. The Long Arm of U.S. Law

Supported by the national judicial system, law enforcement authorities in the U.S. rarely hesitate to assert the long-arm of U.S. law to obtain sensitive information about people and businesses beyond their borders. Foreign records are often needed for antitrust and criminal money-laundering investigations. Increasingly, such information is reputedly sought in connection with national security investigations involving terrorism and foreign intelligence.[39] Different avenues are open to U.S. law enforcement agencies to obtain sensitive information situated outside its borders.

a. Law Enforcement Options

U.S. law enforcement agencies have several options when they seek to obtain records from U.S. and foreign companies subject to U.S. personal jurisdiction. One option is a grand jury subpoena – a powerful investigative order that can be used to obtain records for mostly federal criminal offences. The *USA Patriot Act*'s Section 215 orders can be used to obtain business records and other information for counter-terrorism or foreign intelligence investigations. National Security Letters ("NSL") can also be used for terrorism investigations. Each of these options provide limited due process rights to the recipient of the order and can even prevent the recipient from divulging its existence.

If a foreign company falls outside U.S. personal jurisdiction, the ability to obtain records is more limited. Authorities are forced to rely on the cooperation of the country where the records are located. One available option in such an instance is the use of Mutual Legal Assistance Treaties ("MLAT"), bilateral treaties requesting evidentiary assistance directly from the justice departments of foreign countries. Another is letters rogatory, court documents that request formal assistance for evidence from a foreign court.

i. Grand Juries Subpoenas

A grand jury subpoena is the best known instrument for obtaining sensitive records in criminal investigations. A grand jury is a U.S. constitutional creation composed of 16 to 23 civilian jurors who investigate the existence of possible criminal conduct

[39] Prevention of terrorism through increased access by law enforcement to international passenger airline databases is an example. See EPIC's page on EU-US Airline Passenger Data Disclosure, last updated February 3, 2005, online: <http://www.epic.org/privacy/intl/passenger_data.html>.

under the aegis of a prosecutor.[40] The court in *Whitehouse v. United States Dist. Court for Dist. of R.I.* outlined the distinguishing features of the grand jury process, 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.[41]

As stated in *Whitehouse*, grand juries have substantial investigatory powers and can base investigations merely on suspicion that a law is being violated, without the need to show probable cause. Grand juries can subpoena virtually any person or relevant document and do not operate according to many rules of evidence.[42] A grand jury subpoena is issued under the authority of a court. However, in practice, a court clerk issues a blank subpoena complete with a court seal to a prosecutor working with a grand jury.[43] A recipient who does not comply can be held in contempt of court. Generally, these subpoenas cannot be appealed; however, a recipient can bring a motion to quash. The motion is then typically litigated before a district court.[44]

Grand juries operate in secrecy and investigate on an *ex parte* basis.[45] The secrecy requirement does not always apply to subpoena recipients, though special gag orders can be sought. This suggests that witnesses, once they testify or disclose information, are free to discuss the subject of their grand jury testimony.[46] 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.[47]

A system of statutory safeguards on grand jury investigative powers 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

---

[40] Fed. R. Crim. P. 6.

[41] 53 F.3d 1349 at 1357 (1st Cir. 1995).

[42] 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).

[43] Fed. R. Crim. P. 17(a).

[44] Fed. R. Crim P. 17 (c) (2).

[45] Fed. R. Crim. P. R 6 (e) (2) (b).

[46] Fed. R. Crim. P. R 6 (e) (2 (a).

[47] 31 U.S.C.S. § 5318(g)(3).

Government and the people".[48] The U.S. Supreme Court also cautioned, however, that grand juries are also "not licensed to engage in arbitrary fishing expeditions".[49]

ii. The *USA Patriot Act* and Section 215 orders

After 9/11, the U.S. Congress enacted the *USA Patriot Act*. Several measures grant U.S. law enforcement agencies stronger powers to expand surveillance activities while minimizing procedural obstacles.[50] These include new investigative tools that increase information gathering from communication providers,[51] a broadened ability for electronic surveillance,[52] relaxed federal procedure for search warrants,[53] new offences for money laundering,[54] and new terrorism-related federal offences.[55] Many of the provisions included in the Act feature a sunset clause that causes the provision to expire on December 31, 2005, unless the U.S. Congress renews the enumerated powers prior to that date.[56]

Section 215 of the *USA Patriot Act* also amends the *Foreign Intelligence Surveillance Act ("FISA")*. The procedure for the Federal Bureau of Investigations ("FBI") to access business records related to foreign intelligence gathering is simplified.[57] *FISA* was established in 1978 to create a separate legal regime for government surveillance pertaining to foreign intelligence.[58] 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.[59] There is a review court for *FISA*, but as of December 2004 it has only been used once. In 1998, *FISA* amendments allowed law enforcement to obtain business

---

[48] 504 U.S. 36 at 47 (1992).

[49] *United States v. R. Enterprises*, 498 U.S. 292 at 299 (1991).

[50] *USA Patriot Act* Pub. L. No. 107-56, 115 Stat. 272.

[51] See *ibid*, sections 204, 210, 211 and 217.

[52] See *ibid*, sections 206 and 216.

[53] See *ibid*, ss. 204, 213, 216, 218, 220.

[54] *Ibid*, s. 311.

[55] *Ibid*, s. 201.

[56] *Ibid*, § 224. Only the following sections will not sunset on December 31, 2005: 203(a), 203(c), 205, 208, 210, 211, 213, 216, 219, 221, and 222.

[57] *Foreign Intelligence Surveillance Act of 1978*, Pub. L. No. 95- 511 [FISA].

[58] For an overview of the *Foreign Intelligence Surveillance Act*, see EPIC's website at <http://www.epic.org/privacy/terrorism/fisa/default.html>. For more in-depth treatment, see Peter Swire, "Surveillance Law: Reshaping the Framework: The System of Foreign Intelligence Surveillance Law" (2001) 72 Geo. Wash. L. Rev. 1306.

[59] 50 U.S.C. § 1803 (c) and 50 USC § 1805 (e).

records for intelligence gathering operations.[60] Previously, only telephone, financial and credit records were available through National Security Letters, as described further below.[61]

The *USA 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 relevant to an investigation of "international terrorism or clandestine intelligence activities".[62] This is a lower standard than the previous "specific and articulable facts" threshold.[63] "Tangible things" may include "books, records, papers, documents, and other items" of any subject.[64]

Such requests are made to the *FISA* Court or to a magistrate judge that is specifically authorized to hear *FISA* requests.[65] If the request meets the requirements of this section, it is ordered on an *ex parte* basis.[66] The language of the Court's order cannot disclose the investigative purpose.[67] 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.[68] Although there is no specified punishment, the U.S. Department of Justice has publicly stated that disclosure by a recipient would be punished as contempt of court and could lead to imprisonment or a fine.[69]

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 or freedom of religion).[70] This First Amendment protection only applies to persons located in the

---

[60] 50 U.S.C. § 1803 (b).

[61] The authority to issue National Security Letters was created for financial records and telephone records in 1986, and for credit records in 1996. See *Electronic Communications Privacy Act of 1986* § 201[a]; *Intelligence Authorization Act for Fiscal Year 1987*, Pub. L. No. 99-569, 404 (1986); *Intelligence Authorization Act for Fiscal Year 1996*, Pub. L. No. 104-93, 601.

[62] Codified as 50 U.S.C. § 1861 (a)(1).

[63] P.L. 105-272, title VI, § 602 (b), Oct. 20, 1998

[64] 50 U.S.C. § 1861 (a)(1).

[65] 50 U.S.C §1861 (b)(1).

[66] 50 U.S.C §1861 (c).

[67] 50 U.S.C §1861 (c)(2).

[68] 50 U.S.C §1861 (d).

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

[70] 50 U.S.C §1861 (a)(2)(b).

U.S.[71] As of December 2004, Section 215 has not been subject to any court challenges, although there have been several challenges to other sections of the *USA Patriot Act*, including the provisions dealing with National Security Letters.[72]

In the most relevant court case to date, the Foreign Intelligence Surveillance Court of Review considered the constitutionality of the post-*USA Patriot Act* version of *FISA*,[73] assessing whether the *USA Patriot Act*'s amendment to *FISA* offends the Fourth Amendment. The Court found that it did not, reasoning that the requirement that foreign or counter-terrorism intelligence is a "significant purpose" of the surveillance comes close to the reasonableness standard required under the Fourth Amendment.[74]

iii. 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. These include telephone records, Internet activity records[75], and financial and credit records from financial institutions NSLs have the same force and effect as a court order, and prohibit recipients from disclosing their existence like Section 215 orders.[76] The *USA Patriot Act* gave the FBI greater powers to use NSLs by making them available to special agents in charge rather than only to Deputy Assistant Directors and above.[77] In the case of financial records, the FBI need only certify that the records "are sought for foreign counter intelligence purposes to protect against international terrorism" in order to receive

---

[71] *United States ex rel. Turner v. Williams*, 194 U.S. 279, 292 (1904).

[72] *Doe v. Ashcroft*, 334 F. Supp. 2d 471. Other Patriot Act challenges include *Humanitarian Law Project v. Ashcroft*, 309 F. Supp. 2d 1185, where the plaintiff organization, a humanitarian group that assisted Kurdish and Sri Lankan revel organizations challenged the provision preventing the provision of "expert advice or assistance" to designated foreign terrorist organizations. The court found that the term "expert advice or assistance" was too vague, and granted a summary judgement for the plaintiffs that enjoined the Department of Justice from enforcing the provision against groups that aided the specified Kurdish and Sri Lankan organizations. The court declined to make it a nationwide injunction.

[73] In re: Sealed Case No. 02-001, 310 F.3d 717 (FISA Ct. App. 2002).

[74] *Ibid* at 88.

[75] 18 USCS § 2709.

[76] 18 USC § 2709 § (c) and 12 USC § 3414 (a)(3).

[77] Pub. L. 107–56, § 505(a)(1)

[78] 12 USCS § 3414 (a)(5)(a).

them.[78] The Justice Department acknowledged that NSLs are the preferred route to obtain computer-use records such as library records.[79]

The power to issue administrative subpoenas is common in the U.S. A 2002 Office of Legal Policy study identified approximately 335 administrative subpoena authorities.[80] 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; an agency is not required to show probable cause.[81] 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.[82]

A recent court decision puts the future of NSLs in doubt, however. In *Doe v. Ashcroft,* the ACLU successfully challenged the constitutionality of NSLs pertaining to telephone and Internet records.[83] In that case, the manager of an internet service provider claimed that the NSLs violated both the Fourth and First Amendment. The Fourth Amendment issue was that the NSL did not give him the opportunity to judicially challenge the request, while the First Amendment claim was that the NSL prevented him from speaking about the request indefinitely.[84]

The District Court for the Southern District of New York agreed, concluding that the NSL telephone and Internet record provision deterred any judicial challenge to the propriety of an NSL request and violated fundamental constitutional rights that could not be saved by the objectives of anti-terrorism measures.[85] Specifically, the Court found that even if a reading of the statute could construe some judicial oversight, the gag provision restraining recipients from disclosing the order's existence still went beyond what is permissible under the First Amendment.[86] The Court

---

[79] Letter from Daniel J. Bryant, Assistant Attorney General, to Patrick J. Leahy, Chairman, Committee on the Judiciary (July 29, 2002) (response to written questions at the "Oversight Hearing for the Department of Justice" on July 25, 2002).

[80] Office of Legal Policy, *Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities* (May 13, 2002) at 5, online: United States Department of Justice <http://www.usdoj.gov/olp/intro.pdf>.

[81] 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.

[82] *Ibid.*

[83] *Doe v. Ashcroft*, 334 F. Supp. 2d 471.

[84] The U.S. First Amendment protects the right to free speech. The U.S. Fourth Amendment protects the right of the people to be secure against unreasonable search and seizure.

[85] *Doe, supra* note 83 at 501.

[86] *Ibid.* at 514 to 525.

accordingly found that the provision was "too broad and open-ended".[87] Since the gag provision could not be severed from the rest of the statute, the Court had to strike it down.[88] The U.S. Department of Justice is expected to appeal, since striking down section 2709 has implications for the *USA Patriot Act*'s section 215. Both provisions feature similar procedures for obtaining records.[89]

iv. Mutual Legal Assistance Treaties

Prosecutors use Mutual Legal Assistance Treaties ("MLATs") to access foreign business records in criminal investigations.[90] MLATs formally obligate and provide a framework for countries to assist each other in prosecution and law enforcement activities to the extent permitted by their laws. The MLAT between Canada and the United States facilitates the cross-border production of individual, business and government documents for law enforcement purposes, among other forms of help.[91] The assistance is rendered "...without regard to whether the conduct under investigation...constitutes an offence...by the Requested State".[92] Search and seizure of documents can be requested.[93] U.S. law enforcement officials can also request Canadian government documents and records, including provincial records, "to the same extent and under the same conditions" as would be available to Canadian law enforcement.[94] The United States has 48 MLAT agreements with other countries.

The MLAT process requires U.S. law enforcement to request assistance from the Canadian Minister of Justice when the documents sought are located in Canada.[95] If more than a 30-day delay or a denial of assistance occurs, the U.S. is free to compel production by other methods.[96] Denials are made if the "execution of the request is contrary to [Canada's] public interest".[97] Public interest is defined as "any sub-

---

[87] *Ibid.* at 476.

[88] *Ibid.*

[89] Both 18 U.S.C. §2709 and 50 U.S.C. § 1861 (Section 215) contain similar procedures for application, orders and rules about non-disclosure.

[90] For general information about U.S. MLATs see Ellis & Pisani, "The United States Treaties on Mutual Assistance in Criminal Matters: A Comparative Analysis" (1985) 19 Int'l Law 189.

[91] *Treaty with Canada on Mutual Legal Assistance in Criminal Matters,* Canada and United States, March 18, 1985, O.A.S.T.S.. Doc. 100-14 (1985) online: OAS <http://www.oas.org/juridico/MLA/en/traites/en_traites-mla-usa-can.pdf>.

[92] *Ibid.* at Article II, s.3.

[93] *Ibid.* at Article II, s.2(h).

[94] *Ibid.*, Article XIII, s.2.

[95] *Ibid.* at Article VI, s.1.

[96] *Ibid.* at Article IV, ss.1-3.

[97] *Ibid.* at Article V, s.1(b).

stantial interest related to national security or other essential public policy".[98] In practice, U.S. federal prosecutors receive guidance from the Office of International Affairs (OIA) on cross-border document production, and prosecutors must contact the OIA before any contact "with persons in a foreign country".[99]

Unlike section 215 orders and NSLs, MLATs require participation by foreign government agencies, at minimum foreign justice ministries, to effect delivery of records. In sensitive national security investigations, this may decrease reliability and security of the investigative process.[100] Moreover, MLATs may not provide the expeditious results necessary for a counter terrorism investigation.

The ACLU noted that an MLAT will unlikely be used to obtain business records for foreign terrorism investigations.[101] The B.C. Privacy Commissioner's Office agreed, making clear that it believed the U.S. was unlikely to use the Canada-U.S. MLAT in the context of national security related investigations.[102] The Office reasoned that the MLAT is primarily a vehicle for criminal investigations, as stated in the preamble of the MLAT itself.[103] Moreover, the MLAT is not necessary to obtain documents held by entities subject to U.S. personal jurisdiction.[104]

Despite their drawbacks, MLATs were recently used to process requests for foreign intelligence investigations. In November 2004, an online alternative media collective's computer servers were seized pursuant to an MLAT that the U.S. has with an unnamed country.[105] The collective's hosting company, Texas-based Rackspace, was ordered to not disclose which country made the request, and the only information released was that the seizure was part of an "ongoing criminal terrorism investigation".[106] Rackspace's servers in London, England were also seized.[107] The

---

[98] *Ibid.* at Article I.

[99] United States Department of Justice, *United States Attorney's Manual*, (Washington, D.C.: United States Government Printing Office) at s. 9-4.146 (E)(2).

[100] See Jessica Romero, "Prevention of Maritime Terrorism: The Container Security Initiative" (2003) 4 Chi. J. Int'l L. 597, which discusses MLATs in the context of terrorism prevention.

[101] Christopher Calabrese, Submission of the American Civil Liberties Union, August 10, 2004 at 12.

[102] OIPC Report, *supra* note 29 at 117.

[103] *Ibid.* at 102-103.

[104] See Christopher Calabrese, *supra* note 101.

[105] See Electronic Frontier Foundation (EFF) webpage for more information, "Indymedia Server Seizures", online: Electronic Frontier Foundation <http://www.eff.org/Censorship/Indymedia/>.

[106] *Ibid.* Contrary to the assertions of the B.C. submissions, Rackspace was clear in its press release about the seizure to describe the MLAT as "establish[ing] procedures for countries to assist each other in investigations such as international terrorism, kidnapping and money laundering."

[107] Associated Press, "Web Server Takedown called Speech Threat" (26 October 2004) online: ABC News <http://abcnews.go.com/Business/wireStory?id=200007&CMP=OTC-RSSFeeds0312>.

Electronic Frontier Foundation successfully filed a motion in a federal court to unseal the original order in the case and confirmed that the subpoena came from the Bologna (Italy) public prosecutor's office.[108]

v. Letters Rogatory

Letters rogatory are formal requests from a domestic court to a foreign court requesting aid in obtaining evidence or testimony.[109] Unlike an MLAT, a letter rogatory is not based on any compunction to produce records.[110] Rather, they are based on comity of nations and the goodwill of the recipient court.[111] They have been used occasionally in civil matters, but are most often used to obtain evidence for criminal and administrative cases, such as cases involving allegations of antitrust violations or tax evasion.[112]

In the U.S., letters rogatory are increasingly discouraged since they are cumbersome and time-consuming.[113] Letters rogatory travel through diplomatic channels and must be authenticated by multiple parties, often including the embassy of the foreign country where the records are located, before they can be registered with foreign courts.[114] They are also inconsistent with the grand jury tradition because there is no guarantee that the order remains confidential.[115] For these reasons, it is very unlikely that a U.S. law enforcement agency would use a letter rogatory to obtain sensitive records relating to a national security investigation.

---

[108] Electronic Frontier Foundation, Motion to Unseal and for Expedited Hearing (22 October 2004) online: EFF <http://www.eff.org/Censorship/Indymedia/20041022_Indymedia_Motion_to_Unseal.pdf>; Electronic Frontier Foundation, Order granting in Part Motion to Unseal (July 20, 2005) online: EFF < http://www.eff.org/Censorship/Indymedia/order_unsealing.pdf>. The unsealed order showed that the Italian subpoena was seeking log files that included information relating to certain URLs on Indymedia's servers. See generally Electronic Frontier Foundation, Indymedia Server Takedown information page, online: EFF <http://www.eff.org/Censorship/Indymedia/>.

[109] See Restatement 3rd of the Foreign Relations Law (1988) at § 474 and accompanying reporter notes for general information about the use of letters rogatory.

[110] Restatement at § 474, Reporter Notes (3).

[111] *Ibid.*

[112] U.S. Department of State, Office of American Citizens Services, Brief, "Preparation of Letters Rogatory" online: <http://travel.state.gov/law/info/judicial/judicial_683.html>.

[113] The U.S. Department of State advises U.S. citizens not to use them. See U.S. Department of State, *Ibid.*

[114] *Ibid.*

[115] Marian Nash, Contemporary Practice of the United States Relating to International Law, (1997) 91 A.J.I.L. 93 at 103.

vi. Other Information Sharing Regimes

MLATs and letters rogatory are not the only bilateral instruments used to obtain foreign records. Law enforcement agencies in Canada and the U.S. currently employ a harmonized approach to share information related to cross-border crime, terrorist activity and immigration matters. For example, a post-9/11 agreement between Canada and the U.S. established a 30-point action plan for creating a secure border.[116] Moreover, integrated intelligence is one of eight objectives oriented towards joint data sharing and intelligence coordination. Canada also established Integrated National Security Enforcement Teams ("INSETs") to fight terrorist threats.[117] 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 identified increased joint antiterrorism efforts as a priority.[118]

Information-sharing instruments are also used to obtain information relating to financial investigations. For example, the U.S. Securities and Exchange Commission has Memorandums of Understandings with foreign securities regulators to cooperate and share information on the regulation of the financial industry.[119]

Several Canadian statutes specifically authorize cross-border information transfers. *The Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, authorizes the Financial Transactions and Reports Analysis Centre of Canada to share financial information to prevent money laundering and terrorist financing.[120] The *Department of Immigration and Citizenship Act* includes a provision that allows the Minister to implement agreements with foreign governments facilitating the coordination of policies for which he or she is responsible.[121] In fact, the Federal Privacy Commissioner's submission to the B.C. review notes that some Canadian legislation may override our federal privacy protections to enable cross-border infor-

---

116 Canada-US 30 Point Action Plan (12 December 2001), online: Department of Foreign Affairs and International Trade [DFAIT] <http://www.dfait-maeci.gc.ca/can-am/menuen.asp?act=v&mid=1&cat=10&did=1670>.

117 Public Safety and Emergency Preparedness Canada, News Release, "New Technologies, Intelligence Sharing and Integrated Law Enforcement to Improve Safety and Security of Canadians" (12 October 2001).

118 Smart Border Declaration (December 12, 2001), online: DFAIT <http://www.dfait-maeci.gc.ca/can-am/menu-en.asp? act=v&mid=1&cat=10&did=1669>.

119 See generally, Kanishka Jayasuriya, "Globalization, Law, and the Transformation of Sovereignty: The Emergence of Global Regulatory Governance" (1999) 6 Ind. J. Global Leg. Stud. 425.

120 *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, S.C. 2000, c. 17. See, supra, note 45.

121 *Department of Citizenship and Immigration Act*, S.C. 1994, c. 31, s. 4.

mation sharing.[122] The Commissioner cites the *Aeronautics Act* as an example of a Canadian statute that permits airlines to share information about passengers.[123]

b. Application of U.S. Law Enforcement Options

i. Model Law

Notwithstanding the novelty presented by data outsourcing, the issue of the extra-territorial application of U.S. law is not a new concern. A review of U.S. case law illustrates that the absence of *USA Patriot Act* powers did not prevent U.S. law enforcement from obtaining records, even where disclosure would violate another jurisdiction's laws. For the past 50 years, courts frequently ordered corporate compliance with U.S. disclosure orders, provided the court can assert personal jurisdiction over the company in possession or control of the requested material. Furthermore, courts commonly ruled that foreign secrecy and confidentiality laws are superseded by U.S. criminal investigations that necessitate disclosure.[124] This trend would presumably also apply to other national privacy laws, such as *PIPEDA*.

The widely adopted *Restatement (Third) of the Foreign Relations Law of the United States ("Restatement")* provides the model approach for this issue. Section 403 of the *Restatement* addresses 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 connections between the regulating nation and the person to be regulated; and (3) the extent the regulations are in line with the international system.[125] The analysis is not limited to these factors, however.[126] Based on this test, the possibility of civil or criminal sanctions in another jurisdiction will not necessarily prevent enforcement of a subpoena.

---

[122] Privacy Commissioner of Canada, "Transferring Personal Information about Canadians Across Borders, Submission: Implications of *USA Patriot Act*" (16 August 2004) online: http://www.oipcbc.org/sector_public/usa_patriot_act/pdfs/Office%20of%20the%20Privacy%20Commissioner%20of%20Canada%20(English).pdf.

[123] *Ibid.*

[124] 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 at note 24 (S.D.N.Y. 2002).

[125] Restatement (Third) of Foreign Relations Law § 403 (2) (a) to (h) (1987) ("Restatement").

[126] Restatement § 403 (2) states that the balancing test is "determined by evaluating all relevant factors, including..." and lists factors (a) to (h). The accompanying comment state that the list of consideration in (2) is not exhaustive (Comment (b)).

Courts can compel U.S. corporations to produce documents possessed at foreign branches unless a strong defence, such as a blocking statute, is raised.[127] This applies both to documents held by a foreign subsidiary when the request is made to a domestic parent company; and to documents held by a foreign parent company when the request is made to the domestic subsidiary.

Section 442(1)(c) of the *Restatement* addresses foreign record disclosure requests. Courts must consider the importance of the documents requested, the availability of alternative means of disclosure, and the degree of specificity of the request.[128] 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".[129]

ii. Foreign Companies Subject to U.S. Jurisdiction

U.S. courts have ruled that a foreign parent corporation's records may be captured by an order to a subsidiary subject to U.S. personal jurisdiction.[130] This suggests that courts can order multinational companies to provide records through their U.S. offices or subsidiaries, even if headquartered outside the U.S.. In some cases involving grand jury subpoenas, U.S. subsidiaries were ordered to compel production of documents held by their foreign-based parent company.[131] Courts typically employ a balancing test to determine whether to grant a motion to quash a grand jury subpoena when the records sought are located abroad. There are few cases where grand jury discoveries were denied in the criminal context.[132]

A case involving the U.S. subsidiary of a Canadian parent company, the Bank of Nova Scotia, illustrates the U.S. courts' deference to grand jury subpoenas.[133] The

---

[127] See *In Re Investigation of World Arrangements infra note 142* , *In re Grand Jury Subpoenas duces tecum addressed to Canadian International Paper Company et al* infra note 143 and *United States v. First Nat'l City Bank infra note* 145 , all discussed below.

[128] Restatement § 442(1)(c).

[129] Restatement § 442(1)(a).

[130] See *Ssangyong Corp. v. Vida Shoes Int'l.* 2004 U.S. Dist. LEXIS 9101 (S.D.N.Y. 2004); *United States v. Toyota Motor Corp.*, 569 F. Supp. 1158 (C.D. Cal. 1983).

[131] See *Re Grand Jury Proceedings the Bank of Nova Scotia*, 740 F.2d 817 (11th Cir.1984) ("*Bank of Nova Scotia*") discussed below.

[132] See *In re Grand Jury Subpoena, infra*, note 146, 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).

[133] *Bank of Nova Scotia, supra* note 131.

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 Island's secrecy laws. The U.S. 11th circuit Court rejected the argument, ruling that although the bank may believe that local laws preclude disclosure, they do "...not excuse the Bank's failure to perform a diligent search upon receipt of the trial court's order of enforcement".[134]

The records at issue belonged to U.S. citizens, and the Court ruled 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.[135] The bank argued that it was unfair to put it "in the position of having to choose between the conflicting commands of foreign sovereigns".[136] The Court reasoned that choosing between sovereigns is part of the cost of doing business for multinational corporations. It further concluded that local laws should be of lesser interest to the bank since it suffered no hardship as a result of inconsistent enforcement actions.[137]

Courts have ruled in favour of U.S. authorities where the records sought do not involve a U.S. citizen, particularly where the U.S. national interest is strong.[138] For example, in *Re Grand Jury Subpoena*, an international bribery charge case, a U.S. District Court considered whether a grand jury subpoena could compel production of documents abroad where local law prohibited production. The Court held that the U.S. interest in criminal laws enforcement outweighed any difficulties that the corporation may face in complying with the subpoena in contravention of the other state's law.[139] Similarly, in *Ssangyong v. Vida Shoes*, a New York branch of a Hong Kong bank was ordered to produce records from its head office even though that violated Hong Kong's banking secrecy laws.[140] The same U.S. District Court held that control did not require legal ownership or actual physical possession, rather only the ability to obtain the documents.[141]

---

[134] *Ibid.*, at 826.

[135] *Ibid.*, at 828.

[136] *Ibid.*

[137] *Ibid.*

[138] *In re Grand Jury Subpoena dated August 9, 2000*, 218 F. Supp. 2d 544 (S.D.N.Y. 2002).

[139] 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).

[140] *Ssangyong Corp. v. Vida Shoes Int'l, Inc.*, 2004 U.S. Dist. LEXIS 9101 (S.D.N.Y. 2004).

[141] *Ibid*, at 10.

iii. Foreign Subsidiaries of U.S. Companies

The situation is clearer where the U.S. connection is a domestic parent compelled to obtain records from its foreign subsidiary. Courts more often than not reject 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 a 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.[142]

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 antitrust violations.[143] The U.S. District Court for the Southern District of New York dismissed the parent corporation's argument that it lacked possession of the documents, holding that the test was a matter of control, not location.[144] Similarly, in *United States v. First Nat'l City Bank*, the U.S. 2nd Circuit Court rejected the parent company's argument that it could not produce documents from its German office, concluding that "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".[145]

Section 414 of the *Restatement* addresses jurisdiction with respect to subsidiaries. Section 414(2)(b) permits a state to exercise jurisdiction over a parent company's subsidiary in "exceptional cases".[146] Section 414(2)(c) states that the burden of establishing reasonableness is lessened when the direction is issued to the parent corporation rather than its subsidiary.[147]

---

[142] *In Re Investigation of World Arrangements* 13 F.R.D. 280, 285 (D.D.C. 1952). Quoted *In re Uranium Antitrust Litigation*, 480 F. Supp. 1138 at 1145.

[143] In *re Grand Jury Subpoenas duces tecum addressed to Canadian International Paper Company et al* 72 F. Supp. 1013 (S.D.N.Y. 1947).

[144] *Ibid*, at 1020.

[145] *United States v. First Nat'l City Bank* 396 F.2d 897, 900 (2d Cir. 1968); see also *United States v. Vetco, Inc.*, 691 F.2d 1281 (9th Cir. 1981).

[146] Restatement § 414 (2)(b).

[147] Restatement § 414(2)(c).

From the above cases and the principles found in the *Restatement*, we see that the power to compel disclosure of sensitive personal information is not limited to U.S.-located companies. U.S. law applies to any company with sufficient connections 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. Although there have yet to be cases assessing the application of NSLs and Section 215 orders outside the U.S., the precedent set with grand jury subpoenas, along with importance attached to national security interests, makes it highly likely that such orders would be granted.

IV. The Response of Canadian Law

In today's global business environment, a complete ban on data outsourcing contracts is not a viable option. Such an approach likely violates international trade rules and could cause a country to lose the benefits associated with outsourcing, including reduced costs and opportunities for national firms. While a ban is not possible, our analysis of U.S. law demonstrates that the terms of an outsourcing contract alone are not sufficient to prevent disclosure of personal information in a foreign jurisdiction.[148] For information in the hands of multinational companies, whether Canadian or U.S., only the strength of local law prevents disclosure.

In this section, we assess whether current Canadian law can prevent unauthorized disclosures of personal information to foreign law enforcement authorities. We believe that, at present, Canadian federal privacy legislation is unable to protect records that were outsourced for data management from disclosure.

a. Personal Information Protection and Electronic Document Act

The *Personal Information Protection and Electronic Document Act* establishes the obligations of private organizations with regard to the data they collect in the course of commercial activity.[149] The Act applies to every private-sector organization in Canada that collects, uses or discloses personal information, unless it is subject to a substantially similar provincial law.[150]

The statute addresses third party disclosures in principle 4.1.3.[151] Where organizations transfer data for processing, they must provide a comparable level of privacy protection for the data through contractual or other means. Accordingly, in

---

[148] The B.C. Privacy Commission Report came to a similar conclusion, stating that domestic law is needed to prevent disclosures to foreign law enforcement agencies at 132.

[149] *PIPEDA*, S.C. 2000, c. 5.

[150] *PIPEDA* § 26 (2) (b).

[151] *PIPEDA* § 5 (4.1.3).

order to comply with *PIPEDA*, organizations that transfer personal information must obtain sufficient contractual protections from third parties prior to transferral. Therefore, organizations subject to U.S. personal jurisdiction that disclose personal information without consent in compliance with U.S. disclosure orders – whether granted by grand jury subpoenas, NSLs or Section 215 orders – risk violating *PIPEDA*, unless: (1) the organization obtained prior consent for the disclosure, or (2) the disclosure qualifies for one of the Act's exceptions. This is not limited to U.S. companies that compete for Canadian outsourcing contracts through subsidiaries, since Canadian companies with a U.S. connection sufficient to fall under U.S. personal jurisdiction rules would presumably be subject to the same concerns.

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...."[152]. The statute does not address whether foreign orders, such as those made by a *FISA* court or a grand jury fall under this exception, and can be considered made by "a court, person or body with jurisdiction to compel". The statute is silent on the jurisdictional distinction, making it possible that U.S. orders validly made under U.S. personal jurisdiction are an exception. None of the previous *PIPEDA* findings shed light on the question of foreign orders.[153] The Federal Privacy Commissioner submitted to the B.C. Privacy Commission that it is her position that compliance with any U.S. orders made against a commercial organization located in Canada would violate *PIPEDA* if disclosures were made without consent.[154]

Section 7(3)(c.1) permits disclosure to a government institution without consent 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[155]

---

[152] *PIPEDA* § 7 (3)(c).

[153] The closest case is Finding #96, where the Commissioner considered whether a subpoena by a lawyer in Quebec (allowed under Quebec Civil Law) constitutes a proper subpoena under s. 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. Using the logic from this Finding, if statutory powers granted an authority the power to compel disclosure, it would constitute a proper subpoena. *Finding #96*, (December 3, 2002), Privacy Commissioner Decision, online:<http://www.privcom.gc.ca/cf-dc/cf-dc_021203_2_e.asp>.

[154] *Supra* note 29.

[155] *PIPEDA* § 7(3)(c.1).

The inclusion of foreign laws within this exception indicates that disclosure for U.S. counter-terrorism investigations through NSLs or Section 215 orders might qualify under the Act's exceptions. A related issue is whether "government institution" is limited to a Canadian institution or whether a foreign institution suffices. If the exception were 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.

None of the Commissioner's findings to date focusing on s. 7(3)(c.1) address foreign requests. However, the language in at least one finding indicates that the exception may not preclude foreign government requests. 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).[156] Section 9(2.1) grants individuals the right to ask an organization whether it has disclosed information about them under s. 7(3)(c) or (c.1) and to access that information. If information has been disclosed, s. 9(2.2) provides that the organization must notify the requesting institution immediately and wait 30 days for any objections to disclosure.[157]

Section 9(2.3) stipulates that the requesting institution can only object for purposes of national security (although it is unclear 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.[158] If the requesting institution objects, then s. 9(2.4) mandates that the organization refuse to provide the information to the individual and notify the Commissioner in writing.[159] No *PIPEDA* findings have thus far interpreted Sections 9(2.1) – (2.4).

Although the Federal Privacy Commissioner has not yet addressed the issue of disclosure to foreign jurisdictions in a finding, there are several findings that hint at the potential analysis. In Finding #106, a Canadian pilot did not have to disclose personal information to U.S. authorities where in order for him to participate in twice-yearly training on U.S. aircraft simulators.[160] 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

---

[156] *Finding #62* (July 22, 2002), Privacy Commissioner Decision, online: <http://www.privcom.gc.ca cf-dc/cf-dc_020722_e.asp>.

[157] *PIPEDA* § 9(2.2).

[158] *PIPEDA* § 9(2.3).

[159] *PIPEDA* § 9 (2.4).

[160] *Finding #106* (December 19, 2002), Privacy Commissioner Decision, online: <http://www.privcom.gc.ca/cf-dc/cf-dc_021219_ 7_e.asp>.

"...consent to unacceptable collection and disclosure practices at the request of a foreign government".[161] In another airline-related case, a Canadian airline was not found at fault for collecting what a crew member argued was excessive amounts of personal information for U.S. transportation authorities.[162]

Further, it should be noted that the Public Safety Act, 2002 amended *PIPEDA* to allow the collection and use of personal information without consent by certain private organizations for purposes of national security.[163] The amendment allows air carriers and reservation systems operators to collect certain passenger information and disclose it to domestic or foreign government officials and law enforcement.[164] The Federal Privacy Commissioner criticized the amendment, arguing 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.[165]

b. *PIPEDA* and the Application of U.S. Law

The language of *PIPEDA* is ambiguous regarding disclosures to foreign law enforcement authorities. There is little in the prior findings to provide guidance on this point. There are three possible interpretations whether *PIPEDA* covers disclosures without consent. The first interpretation posits that *PIPEDA* exceptions do not cover the disclosures. Although not explicitly stated in the statute, this interpretation holds that the exceptions do not encompass disclosure to foreign law enforcement authorities without cooperation of a Canadian institution. If this were the case, disclosures made with respect to a Section 215 order, an NSL or a grand jury subpoena would result in a clear violation of *PIPEDA*.

The second interpretation suggests that the *PIPEDA* exceptions cover disclosures to foreign law enforcement through its wording, though this may not have been the intent of the law. It remains unclear whether Canadian legislators envisioned the prospect of disclosure requests from U.S. authorities, though it is noteworthy that Canada has similar disclosure provisions as those found in the *USA Patriot Act*. For example, s. 21 of the Canadian Security Intelligence Act provides for a warrant that

---

[161] *Ibid.*

[162] *Finding #128* (March 4, 2003) Privacy Commissioner Decision, online: <http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030304_ 5_e.asp>.

[163] *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*, S.C. 2004, c. 15.

[164] *Ibid.*, s. 98.

[165] 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>.

permits almost any type of communication interception, surveillance or disclosure of records for purpose of national security.[166] To obtain such a warrant, the Director of the CSIS or a designate of the Solicitor General is required to file an application with a Federal Court judge.[167] The application must contain an affidavit stating "the facts relied on to justify the belief, on reasonable grounds, that a warrant... is required".[168] The application must also outline why other investigative techniques are inappropriate.[169] The warrant will typically last 60 days and is renewable on application.[170] 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 require 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. As with a s. 215 application, a s. 21 application is usually heard *ex parte*.[171] 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.[172]

CSIS works closely with its foreign counterparts on counter terrorism and intelligence investigations.[173] Indeed, its mandate includes working with foreign intelligence services to prevent the planning of terrorist activities abroad.[174] It is worth noting that CSIS worked with legislators to redraft *PIPEDA* to include a national security clause (now s. 7(3)(c.1)). This ensures that *PIPEDA* exempts disclosures to investigative agencies to accommodate national security concerns or anti-terrorism activities.[175] CSIS's public concern about exempting access to records for investigative agencies suggests that legislators might have considered whether foreign and specifically U.S. investigative agencies also qualify for the exemption.

---

[166] *Canadian Security Intelligence Act*, R.S.C. 1985, c. C-23, §21.

[167] *Ibid*, § 21 (1).

[168] *Ibid*, § 21(2)(a).

[169] *Ibid*. § 21 (1) (b).

[170] *Ibid*., § 21 (5) (a) and (22)

[171] *Ibid*., § 27.

[172] See *Public Safety Act, supra*, note 163.

[173] See *e.g*., CSIS, "Counter-Terrorism" (9 August 2002) online: <http://www.csis-scrs.gc.ca/eng/operat/ct_e.html/>.

[174] Canadian Security Intelligence Service, 2003 Public Report, Cat No. JS71-2/2003-1E-HTML.

[175] See e.g., "CSIS pushed to alter privacy bill: Spy agency wanted security concerns addressed" *The Ottawa Citizen* (7 January 2004).

The third interpretation of the *PIPEDA* exceptions is broader. Disclosures to U.S. law enforcement are permitted, since the language does not explicitly prevent disclosure to foreign authorities. Indeed several references are made to the laws of foreign jurisdictions in s. 7(3)(c) and (c.1). If this were the case, the application of U.S. law to companies under U.S. jurisdiction would likely not violate *PIPEDA*.

V. Reconciling Privacy, Security and Data Outsourcing

Bill 73 and the B.C. Privacy Commissioner's recommendations naturally focused on the potential for reform at the provincial level. However, the privacy implications of data outsourcing and the extra-territorial application of U.S. law raise issues that apply equally on a national basis. In this section, we address three options for action at the national level. First, as recommended by the BCGEU,[176] we assess a government ban on outsourcing that either prohibits government outsourcing as a whole, or limits outsourcing contracts to domestic companies. Second, we look at the creation of a blocking statute that limits the ability of foreign enforcement agencies from accessing records held in Canada. Lastly, we recommend a stronger *PIPEDA* to increase its deterrent value against disclosure.

a. A Government Ban on Outsourcing

In British Columbia, the BCGEU called for a ban on government outsourcing of sensitive data to prevent disclosure to foreign law enforcement agencies.[177] Although a governmental ban potentially addresses the immediate issue of protecting the privacy of B.C.'s medical data, it does not address the wider privacy issue caused by the application of U.S. law to Canadian businesses. A 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. In its report, the B.C's Privacy Commissioner's office agreed that a ban on government outsourcing of data management tasks "would not be a practical or effective plan of action".[178]

This impasse between privacy advocates and governments on allowing governments to outsource data management functions is unfolding in a different manner

---

[176] BCGEU Submission on the *USA Patriot Act* to the Information and Privacy Commissioner for British Columbia (6 August 2004) online: BCGEU http://www.bcgeu.ca/bbpdf/040806_privacy_submission_1.pdf

[177] *Ibid* at vi; also see BCGEU, News Release "Leave personal data with government where it belongs" (6 August 2004).

[178] Office of the Information & Privacy Commissioner, "Privacy & the *USA Patriot Act* - Implications for British Columbia Public Sector Outsourcing" (29 October 2004) at 133, online: <http://www.oipcbc.org/sector_public/usa_patriot_act/patriot_act.htm>.

in the U.S, where the focus of the outsourcing debate lies in domestic worker job losses. The primary concern in the U.S. is that increased government outsourcing will lead to a dramatic transfer of jobs to lower-wage jurisdictions.

Various U.S. legislative initiatives aimed at preventing government outsourcing to foreign companies. However, thus far only one has made it into law. The 2004 *Omnibus Appropriations Bill* (the Thomas-Voinovich Amendment), a massive bill that dictates yearly funding for federal programs and agencies, includes a provision relevant to outsourcing. The section prevents funds appropriated by the Bill to outsource functions to entities outside the U.S.[179] Although it was not enacted into law, more pointed was the U.S. Senate version of the *Jobs Creation Act of 2004*, which would have prohibited foreign outsourcing of federal government data management contracts, federal procurement of goods and services, and state government procurement for contracts using federal funds.[180] The text passed in the Senate by a 92-5 vote, but was cut from the enacted legislation in a conference agreement.[181] Some amendments considered as part of the bill included withholding funds for state financial assistance unless the state certifies that none of the funds would be used for the performance of state contracts outside the U.S.[182]

Ironically, the U.S. assumed the lead on prohibiting government outsourcing to foreign entities, despite the fact that their legislation is potentially the basis for such prohibitions in Canada. However, this irony is lost on U.S legislators, since their prime motivation for outsourcing bans is domestic job loss, not privacy. Privacy protection of outsourced records is a secondary issue, sometimes leading to efforts to ensure the security of outsourced personal records, rather than preventing outsourcing altogether.[183]

---

[179] The text reads: "An activity or function of an executive agency that is converted to contractor performance under Office of Management and Budget Circular A-76 may not be performed by the contractor at a location outside the United States except to the extent that such activity or function was previously performed by Federal Government employees outside the United States." Public Law 108-199, Section 647 (e).

[180] Title V: Protection of United States Workers From Competition of Foreign Workforces, S. 1637: *Jumpstart Our Business Strength (JOBS) Act.*

[181] *American Jobs Creation Act of 2004*, Conference Report to Accompany H.R. 4530, October 7, 2004 at 440.

[182] A bill to protect American workers from competition of foreign workforces for performance of Federal and State contracts, S. 2148, *USA Jobs Protection Act of 2004*. Later become part of S. 2094: The United States Workers Protection Act.

[183] See for example, the federal *SAFE-ID Act* espoused by Senator Hillary Clinton.

Given the economic stakes of outsourcing in Canada, the second largest recipient worldwide of outsourcing projects,[184] an outright outsourcing prohibition is not viable. Moreover, international trade obligations may prevent such action even if it becomes politically desirable. Many commentators expressed concern that the Thomas-Voinovich Amendment violates U.S. trade obligations under the World Trade Organization's Government Procurement Agreement ("GPA").[185] The GPA requires signatories to practice "non-discrimination" in government procurement of products, services and suppliers, prohibiting less favourable treatment of foreign contractors.[186] Further, it requires governments to treat local companies with foreign affiliations, such as foreign parent companies, in the same manner as local companies.[187] Canada and the United States, along with 35 other countries, are signatories to the GPA.[188]

If an individual province legislated an outsourcing ban, the resulting statute might also be vulnerable to constitutional challenge. In the U.S., a study by the National Foundation for American Policy, a non-partisan think-tank, argues that state bans on government outsourcing to foreign companies intrudes on federal powers over international trade.[189] Although it is unclear whether such a ban would be unconstitutional in Canada, there may be some merit to the argument.[190]

b. Blocking statutes

One of the only effective means of deterring disclosure of records to U.S. law enforcement is the implementation of a blocking statute, which enables a petitioner

---

184 United Nations Conference on Trade and Development, World Investment Report 2004, United Nations 2004; Barrie McKenna, Offshoring of jobs big benefit for Canada, *The Globe and Mail* (23 September 2004) A1.

185 See for example, Shannon Klinger and M. Lynn Sykes, "Exporting the Law: A Legal Analysis of State and Federal Outsourcing Legislation" (April 2004) online: The National Foundation for American Policy <http://www.nfap.net/researchactivities/studies/NFAPStudyExportingLaw_0404.pdf>.

186 WTO, Government Procurement Agreement, Article III:1.

187 WTO, Government Procurement Agreement, Article III:2.

188 The WTO website lists the parties to the agreement as well as those countries negotiating accession online: World Trade Organization <http://www.wto.org/english/tratop_e/gproc_e/memobs_e.htm>.

189 Shannon Klinger and M. Lynn Sykes, "Exporting the Law: A Legal Analysis of State and Federal Outsourcing Legislation", April 2004, The National Foundation for American Policy at 4.

190 As outlined in the Supreme Court's decision in Parsons, the federal power over trade is limited to international and inter-provincial trade, as well as to general trade. *Citizen's Insurance Co. v. Parsons* (1880) 4 S.C.R. 215. See generally Patrick Monahan, "Canadian Federalism and its Impact On Crossborder Trade" (2001) 27 Can.-US LJ 19.

to mount a foreign compulsion defence to a U.S. court action.[191] The *Restatement on Foreign Relations* acknowledges their effect through s. 442, which states that courts must balance the interests of the domestic court or agency with those of a foreign sovereign.[192] 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 any compliance would require explicit permission from the domestic government. Successful blocking statutes include Switzerland's financial privacy law, which has proved resilient against attempts for disclosure of documents in the possession of Swiss banks.[193]

The *Foreign Extraterritorial Measures Act ("FEMA")* provides a Canadian example.[194] *FEMA* prevents Canadian corporations from complying with disclosure orders issued as part of a foreign antitrust or international trade action without the specific permission of Canada's Attorney General.[195] The *Ontario Business Records Protection Act* prohibits the disclosure of Ontario records outside the normal course of business, and provides another example.[196]

Canadian blocking statutes have not held much sway with foreign courts. In *United States v. Brodie*,[197] the blocking statutes of Canada, United Kingdom and the European Union were at issue in relation to prosecution under the *Trading with the Enemy Act ("TWEA")*, the U.S. law that prohibits trade with Cuba.[198] A U.S. district court rejected the argument that *FEMA* prohibited a Canadian entity from complying with *TWEA* because *FEMA* did not prevent the company from complying with both the Canadian and American laws.[199]

---

[191] See generally Jennifer Mencken for a discussion of the effect of blocking laws, especially relating to financial privacy. "Supervising Secrecy: Preventing Abuses Within Bank Secrecy and Financial Privacy Systems" (1998) 21 B.C. Int'l & Comp. L. Rev. 461. See also Bret A. Sumner for a discussion of blocking laws relating to trade with Cuba, "Due Process and True Conflicts: The Constitutional Limits on Extraterritorial Federal Legislation and the Cuban Liberty and Democratic Solidarity (Libertad) Act Of 1996" (1997) 46 Cath. U.L. Rev. 907.

[192] Restatement (Third) Of Foreign Relations Law (1987), Section 442(1)(a).

[193] RS 952.0, Art. 47, Loi fédérale sur les banques et les caisses d'épargne, online: <http://www.admin.ch/ch/f/rs/952_0/a47.html>.

[194] *Foreign Extraterritorial Measures Act*, R.S.C. 1985, c. F-29.

[195] *Ibid*, § 3 (1).

[196] R.S.O. 1990, c. B.19, 2(2).

[197] *United States v. Brodie*, 174 F. Supp. 2d 294 (E.D. Pa. 2001).

[198] *Trading with the Enemy Act*, P.L. 65-91

[199] *United States v. Brodie, supra* note 197.

The court interpreted *FEMA* as prohibiting persons from "not trading with Cuba" if the decision to do so was exclusively a result of the U.S. laws. *FEMA* did not criminalize compliance with the *TWEA*, nor did it compel corporations to trade with Cuba.[200] 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. court decisions that deny a conflict where it is possible to comply with both foreign and U.S. law.[201]

In addition, *FEMA* has been discounted because of its weak enforcement measures. For example, in *Brodie*, the court noted that no information was submitted regarding enforcement under *FEMA*, whether anyone has ever been prosecuted under *FEMA*, or what evidence would be sufficient to establish a violation of the law.[202] The court concluded that there was no such threat of sanction because there was no realistic possibility of prosecution under these laws.[203] Although contraventions of the *Ontario Business Records Protection Act* are prosecuted as contempt of court, with punishments of up to one-year imprisonment, U.S. courts have similarly dismissed arguments related to the Act because it has not been rigorously enforced.[204]

Canadian blocking statutes such as *FEMA* and the *Ontario Business Records Protection Act* were historically enacted in response to U.S. antitrust laws such as the *Sherman Act*[205] or laws that prohibit trade with Cuba.[206] However, blocking statutes could potentially protect the privacy rights of Canadians against NSLs, Section 215 orders, or other disclosures to U.S. law enforcement.

According to U.S. case law, three factors would be necessary for a blocking statute to successfully prevent disclosure in a U.S. court: (1) the blocking statute must be specific and exclusive, not allowing the entity to comply with both Canadian law and the foreign law; (2) the blocking statute must have a tangible sanction

---

200 *Ibid*, at 301.

201 See *Timberlane Lumber Co. v. Bank of America*, 549 F.2d 597, (9th Cir. 1977), *Hartford Fire Ins*, 509 U.S. 764 (1993).

202 *United States v. Brodie, supra* note 197 at 298.

203 *Ibid.*, at 301.

204 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* 480 F. Supp. 1138 (N.D. Ill. 1979).

205 *Sherman Antitrust Act*, 15 U.S.C. §§ 1-7

206 *Cuban Liberty and Democratic Solidarity (Libertad) Act of 1996*, P.L. No. 104-114 and the *Trading with the Enemy Act*, No. P.L. 65-91.

attached; and (3) the defendant must make a good faith attempt to comply with U.S. law.[207]

U.S. courts treat blocking statutes as merely one factor in their decision to order disclosure.[208] The U.S. Supreme Court stated that "[t]he 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".[209] The existence of a blocking statute to prevent disclosure therefore does not prevent the exercise of a disclosure order for anyone subject to U.S. personal jurisdiction.

A blocking statute that successfully prevents disclosure of Canadian records to U.S. law enforcement without due process has to: (1) be exclusive, and not allow companies under Canadian jurisdiction any option but compliance; (2) rest on the fundamentals of Canadian privacy laws, based on domestic objectives rather than attempts to thwart *USA Patriot Act* powers; and (3) contain tangible sanctions and have consistent enforcement for the law to appear serious to U.S. courts.[210] Given the growing concern over the potential applicability of foreign law to Canadian data, a stronger Canadian privacy statute may be needed.

The B.C. government has attempted to create an effective blocking statute with the recent amendments to its public sector privacy law.[211] The prohibitions against disclosures based on foreign court orders and the penalties for non-compliance are similar to successful blocking statutes in other countries. As mentioned, Switzerland has one of the strongest blocking statutes in its banking secrecy law, providing significant incentives against disclosure.[212] Under Swiss law, keeping personal information confidential is both a contractual requirement and a civic duty:[213] Switzerland provides for criminal sanctions for divulging bank secrets, and banking officials can be sent to jail for six months or receive fines of up to 50,000 Swiss Francs (approx-

---

[207] In cases were blocking statutes were successful, these factors were all present. See *Societe Nationale Industrielle Aerospatiale infra* note 208 and *Krupp Mak Maschinenbau infra* note 229.

[208] *Societe Nationale Industrielle Aerospatiale v. United States Dist.*, 482 U.S. 522 (1987).

[209] *Ibid.*, at 544.

[210] See discussion on *Brodie, supra.*

[211] See also the submission of the Canadian Union of Public Employees, BC Division to the Information and Privacy Commissioner for British Columbia, the *USA Patriot Act*, August 4, 2004, at 9 which comes to the same conclusion, online: <http://www.oipcbc.org/sector_public/usa_patriot_act/pdfs/CUPEBC(08042004).pdf>.

[212] RS 952.0, Art. 47, Loi fédérale sur les banques et les caisses d'épargne, online: <http://www.admin.ch/ch/f/rs/952_0/a47.html>.

[213] Embassy of Switzerland in Washington D.C., Fact Sheet, "Swiss Banking Confidentiality and Related Issues" (16 May 2002).

imately $50,000 CDN).[214] A banking official's violation can be prosecuted even if he leaves the bank's employ or changes professions.[215] The B.C. law creates an offence for unauthorized disclosure as well: an individual can be fined up to $2,000 for a violation, while a corporation can be fined up to $500,000.[216] However, the B.C. law does not provide the same stick as the Swiss law, since a charge can only be laid for up to a year after it allegedly occurred, and due diligence in the handling of the disclosed personal information provides an effective defence.[217]

Note that the presence of criminal sanctions does not guarantee deference to blocking laws. In fact, the U.S. Seventh Circuit Court specifically stated that criminal sanctions in foreign countries based on disclosure to U.S. authorities "does not automatically bar a domestic court from compelling production."[218]

The U.S. experience suggests that it is more effective to follow the sanction with a government order. In *Societe Internationale v. Rogers*, 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.[219] The Swiss corporation at issue failed to comply with a grand jury order requiring it to disclose records relating to litigation. The corporation argued that it was prevented by Swiss law from turning over the documents and the Swiss government 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.[220]

A national blocking statute could be established in two ways – either incorporated into *PIPEDA* or established as a separate act. Alternatively, the federal government could establish a separate act that specifically relates to the disclosure of outsourced business records. Care is necessary to ensure that the law is not interpreted as an attempt to stymie U.S. law enforcement agencies, since U.S. courts tend to be more deferential to foreign laws when they appear oriented to domestic use and not solely to thwart foreign prosecutions.[221]

---

[214] *Ibid* at §1.

[215] *Ibid* at §3.

[216] Bill 73, Section 74.1 (5).

[217] *Ibid* at 74.1 (6) and (8).

[218] *United States v. First National Bank of Chicago*, 699 F.2d 341, 345 (7th Cir. 1983).

[219] 357 U.S. 197 (1958).

[220] U.S. courts 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. *Krupp Mak Maschinenbau G.m.b.H v. Deutsche Bank A.G.*, 22 Int'l Leg. Mat. 740 (1983).

[221] 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 Stat* 902 F.2d 1275 (7th Cir. 1990)

c. Further *PIPEDA* Reform

Whether considered alone or in tandem with other measures, greater clarity is needed in legislation 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 assist Canadian companies in understanding their responsibilities with regard to requests from foreign law enforcement. Specifically, there should be a clear indication whether *PIPEDA* exempts foreign law enforcement agencies from consent requirements.

PIPEDA could be amended into a successful blocking statute, such as the Swiss financial privacy law, if it were clear from the language of the law that disclosures to foreign law enforcement would not be an exception to Principle 4.1.3. The definition of "orders" would have to be changed to exclude "foreign orders", while the definition of "government institution" would need to exclude the words "a foreign government institution".

Furthermore, substantial penalties for non-compliance would need to be established. Although *PIPEDA* carries fines of up to $100,000 for investigatory non-compliance, they have yet to be levied. The court in *Brodie* opined that in order for the petitioner to mount a successful foreign sovereign compulsion defence it would have to prove that the petitioner's 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.[222] Currently, *PIPEDA*'s enforcement has generally been lax. Commentators argue that the law is dangerously close to being ineffective.[223]

Moreover, the federal Privacy Commissioner would have a duty to protect at-risk documents. This could be achieved by physically preventing records from being disclosed, as was done by the Swiss government in Societe International.[224] In fact, this method was successfully implemented by the Canadian Ministry of Energy in a case where it confiscated records belonging to a Canadian company that received a grand jury's motion to compel disclosure. The motion was dropped.[225]

---

[222] 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).

[223] See for example, Michael Geist, "Weak enforcement undermines privacy laws", *The Toronto Star* (19 April 2004).

[224] *Societe Internationale, supra* note 219.

[225] *In re Uranium Antitrust Litigation* 480 F. Supp. 1138 (N.D. Ill. 1979).

As a blocking statute, a reformed *PIPEDA* would present a strong Canadian defence against disclosures to foreign law enforcement. *PIPEDA*'s purpose goes well beyond blocking access by U.S. law enforcement. Rather, like the Swiss financial privacy law, its objectives are oriented towards domestic use, with its international applications clearly a secondary purpose.

Further, unlike the new *FOIPP* amendments, *PIPEDA* goes beyond protecting government outsourcing by also protecting against outsourcing in the private sector. Private sector cross-border data transfers may be just as sensitive as those related to government data.

VI. Conclusion

British Columbia's quest to balance outsourcing opportunities with the protection of personal privacy has shone a spotlight on an issue that will likely grow in importance in the months ahead. The volatile combination of outsourcing, increased public sensitivity to privacy protection, and government commitments to security will prove exceptionally difficult to reconcile.

Although sceptics initially dismissed the B.C. case as little more than union labour protection, the outcome illustrates that the issue has struck a chord with the public and legislators alike. Global attention was focused on the issue, and provincial legislation was introduced to limit the disclosure of personal information.

Our analysis of U.S. and Canadian law suggests that arguments in the B.C. case contain elements of both fiction and reality. Claims that the enactment of the *USA Patriot Act* has dramatically altered the legal landscape are simply false. The U.S. law enforcement toolkit, which allows for the compelled, secret disclosure of personal information, pre-dates the *USA Patriot Act* by decades. Suggestions that the problem can be solved by keeping personal information from flowing outside the country are not realistic from a real-world, commercial perspective, where data is transferred and stored instantly on computer servers in other jurisdictions without regard for location.

However, claims that there is no threat to privacy are demonstrably false. The power of the U.S. legal system to compel disclosure extends to any organization – U.S. or Canadian – that falls subject to U.S. personal jurisdiction rules. Accordingly, data held in Canada by a Canadian multinational corporation that retains a U.S. presence is just as likely to be disclosed as data held by a U.S. company in the U.S. with a Canadian presence. This leads to conclusion that the legal situation is actually far more problematic than was initially feared.

While the *USA Patriot Act* may not be the devil it is portrayed to be, fears that Canadian data could be disclosed without warning are indeed well-founded. Given

the reluctance of U.S. courts to limit their jurisdictional reach, Canadian officials must respond to the potential encroachment on Canadian sovereign choices on privacy protections.

We believe that government officials have two alternatives. Canada, likely in partnership with other countries, could broker a diplomatic solution whereby U.S. law enforcement officials agree to a series of protocols that provide Canadians with some measure of privacy protection. Such an approach could mirror the current Canada-U.S. MLAT by requiring notice to government officials and other procedural safeguards.

We remain pessimistic about such an approach, however. Experience demonstrates that the U.S. is unlikely to compromise on matters involving national security. Accordingly, Canada may need to pursue an alternate approach that would lead to a stronger *PIPEDA*, backed by enforcement powers that rise to the level of a blocking statute. Although U.S. courts have been sceptical about blocking statutes in the past, a series of broadly applicable provisions designed to establish serious consequences for disclosure of personal information contrary to the law would force a U.S. court to carefully consider whether it could compel an organization to disclose the requested personal information.

Many Canadians point with justifiable pride to a privacy law framework that balances the interests of both individuals and business by fostering the use of personal information within a construct of fair information practices. The increasing popularity of global data outsourcing, combined with national security concerns, poses the toughest challenge yet for the long-term viability of the Canadian model. If Canadians are to retain confidence in their privacy laws, the country must find a way to outsource its data, and not its privacy.