PROVINCIAL CANADIAN GEOGRAPHIC RESTRICTIONS ON PERSONAL DATA IN THE PUBLIC SECTOR

Submitted to the
Trilateral Committee on
Transborder Data Flows

Fred H. Cate

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

The Centre for Information Policy Leadership develops initiatives that encourage responsible information governance in today's digital society. The Centre is a member-driven organization that operates within the privacy and information management practice at Hunton & Williams LLP. Through collaboration with industry leaders, consumer organizations and government representatives, the Centre provides leadership in developing policy to help ensure privacy and information security while balancing economic and societal needs and interests in today's global information age.

Fred H. Cate is a Distinguished Professor, C. Ben Dutton Professor of Law, and director of the Center for Applied Cybersecurity Research at Indiana University. A senior policy advisor to the Centre for Information Policy Leadership at Hunton & Williams LLP, he is a member of Microsoft's Trustworthy Computing Academic Advisory Board and of the National Academy of Sciences Committee on Information for Terrorism Prevention.

The author gratefully acknowledges the assistance provided by members of the Centre for Information Policy Leadership in the preparation of this paper. The views expressed herein are those of the author alone and should not be attributed to any other person or organization.

www.informationpolicycentre.com

Executive Summary

Section 215 of the U.S. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act") expanded on existing law to authorize senior FBI officials to apply for a secret court order requiring the recipient to produce "any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities."[1] Section 215 provoked significant controversy among many privacy advocates and from some Canadian provincial government officials who worried that the provision might be used to obtain data on Canadian citizens, without their knowledge or consent.

The British Columbia Legislative Assembly responded by adopting Bill 73—the Freedom of Information and Protection of Privacy Amendment Act, 2004. The law requires public bodies to ensure that "personal information in its custody or under its control is stored only in Canada and accessed only in Canada."[2] It also requires public bodies and their service providers to notify "the minister responsible for this Act" if it receives "a foreign demand" for personal information.[3]

Nova Scotia followed British Columbia in 2006 with its Personal Information International Disclosure Protection Act, which includes similar requirements. In 2006 Québec amended its Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information to require public bodies to ensure that information receives protection "equivalent" to that afforded under provincial law before "releasing personal information outside Québec or entrusting a person or a body outside Québec with the task of holding, using or releasing such information on its behalf."[4] Alberta's Freedom of Information and Protection of Privacy Act permits the disclosure of personal information controlled by a public body in response to a "subpoena, warrant or order" only if issued by a court with "jurisdiction in Alberta."[5]

The USA PATRIOT Act poses little risk to Canadians' personal information held by public bodies and stored in, or accessible from, the United States. The U.S. government would seem far more likely to access the data it needs for counterterrorism and law enforcement purposes through its direct surveillance programs, some operated in partnership with Canada, or by simply asking Canadian officials, who exercise powers similar to those of their U.S.

counterparts, for the required data. The likelihood of the government resorting to searches of personal data from provincial Canadian public sector authorities held by, or accessible through, service providers in the United States as a reliable law enforcement or counterterrorism tool is "vanishingly small."[6]

Against that minimal risk must be measured the demonstrated harms caused by the broad provincial geographic restrictions. Those include fewer services available to Canadian public bodies and residents, increased bureaucracy and significantly reduced efficiency, higher financial costs, the threat of tangible harms to health and safety, and the undermining of competition for public bodies' business and of Canada's burgeoning services industry. Taken together, these are a high price to pay to guard against the "utterly implausible" access by U.S. officials.[7]

The federal government in Canada has adopted a pragmatic response to the issue of foreign government access to personal data. This more balanced approach demonstrates that the high price of rigid geographic restrictions on transborder data flows is unnecessary. A comparable level of privacy protection can be achieved through rational analysis of the sensitivity of the information, the expectations of individuals whose data are involved, and the probability and gravity of those individuals being harmed by foreign governments accessing their data. Such a thoughtful approach, matched with a proportional response, promises effective privacy protection without compromising other important values.

Introduction

Following the terrorist attacks of September 11, 2001, the United States enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act"),[8] which enhanced the federal government's authority to collect data to enhance national security. Section 215 of that act expanded on a 1978 statute to authorize senior FBI officials to apply to the Foreign Intelligence Surveillance Court for a secret order that would require the recipient to produce "any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities."[9]

Section 215 provoked significant controversy among many privacy advocates, especially librarians, and from some provincial Canadian data protection authorities who anticipated that the provision might be used to obtain data on Canadian citizens.

Geographic Restrictions in Canadian Law

British Columbia

In October 2004, the Information and Privacy Commissioner of British Columbia issued a report, *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing,*[10] which concluded that there is a "reasonable possibility" that the U.S. government would use section 215 to obtain access to personal health data about British Columbia residents if those data were outsourced to "US-linked" companies in Canada.[11] The report therefore recommended that the provincial legislature:

- "prohibit personal information in the custody or under the control of a public body from being temporarily or permanently sent outside Canada for management, storage or safekeeping";
- "prohibit personal information in the custody or under the control of a public body from being ... accessed outside Canada";

- "require a contractor to a public body to notify the public body of any subpoena, warrant, order, demand or request made by a foreign court or other foreign authority for the disclosure of personal information" about British Columbians, even if doing so violates the national law to which the contractor is subject; and
- "make it an offense under FOIPPA [the British Columbia Freedom of Information and Protection of Privacy Act] for a public body or a contractor to a public body to use or disclose personal information, or send it outside Canada, in contravention of FOIPPA"—even if in response to "a subpoena, warrant, order, demand, or request by a court or other authority," unless "it is a Canadian court, or other Canadian authority"—"punishable by a fine of up to $1 million or a significant term of imprisonment, or both."[12]

The British Columbia Legislative Assembly anticipated these recommendations by adopting Bill 73—the Freedom of Information and Protection of Privacy Amendment Act, 2004—which substantially enacted them into law before the commissioner's report was published.[13] The law requires each public body to ensure that "personal information in its custody or under its control is stored only in Canada and accessed only in Canada."[14] "Personal information" is defined broadly to include "recorded information about an *identifiable* individual other than contact information."[15] This includes data that do not by themselves identify a specific individual, but that have the potential for doing so when combined with other data.

The law provides only two exceptions to the prohibition on storing or accessing personal information from outside Canada. Personal information may be exported or accessed from outside of Canada with the consent of the data subject or "for the purpose of disclosure allowed under [FOIPPA]."[16] The disclosures allowed under FOIPPA include:

- those required or authorized by other British Columbian or Canadian laws;
- those required or authorized by "treaty, arrangement or agreement";
- to government officials and bodies for specified uses;
- to satisfy a debt owed to or by the government;
- "for the purposes of licensing, registration, insurance, investigation or discipline of persons regulated inside or outside Canada by governing bodies of professions and occupations";

- if "compelling circumstances exist that affect anyone's health or safety"; and
- "to a law enforcement agency in a foreign country under an arrangement, a written agreement, a treaty or provincial or Canadian legislative authority."[17]

The British Columbia law allows the "minister responsible for this Act" to "by order, allow disclosure outside Canada [by law enforcement agencies] … in specific cases or specified circumstances, subject to any restrictions or conditions that the minister considers advisable."[18]

An additional exception was added in 2006, to permit disclosures outside Canada "necessary for" "installing, implementing, maintaining, repairing, trouble shooting or upgrading an electronic system" and for "data recovery that is being undertaken following failure of an electronic system."[19] Such disclosures are limited to "temporary access and storage for the minimum time necessary for that purpose," and, in the case of data recovery, are limited to "access and storage only after the system failure has occurred."[20]

Another exception that was amended in 2006 allows public bodies to disclose personal information to their employees and the employees of their service providers if "the information is necessary for the performance of the[ir] duties" and occurs "because the individual is temporarily travelling outside Canada."[21]

The 2004 law requires a public body or its service provider to notify "the minister responsible for this Act" if it receives "a foreign demand" for personal information, if it receives a request for disclosure that "it has reason to suspect" is for disclosure outside Canada, or if it "has reason to suspect that unauthorized disclosure of personal information has occurred in response to a foreign demand for disclosure."[22]

Finally, the 2004 British Columbia amendments explicitly apply the provisions of FOIPPA restricting disclosure of personal information to service providers and their employees.[23]

Nova Scotia

Nova Scotia followed British Columbia in 2006 with its Personal Information International Disclosure Protection Act, which includes similar prohibitions. As in British Columbia, the act requires that a public body ensure that "personal information in its custody or

under its control … is stored only in Canada and accessed only in Canada."[24] The act applies directly to "a service provider or associate of a service provider" as well.[25] This includes officers, directors, employees, affiliates, and subcontractors.[26]

Exceptions are permitted only with individual data subject consent, when necessary for the purpose of disclosure otherwise allowed under the act, or with the authorization of the "head" of a public body.[27] Heads of public bodies may provide such authorization if "the storage or access is to meet the necessary requirements of the public body's operation," and the head must report annually "to the Minister all such decisions made during the year, together with the reasons therefor."[28] This provision is broader than British Columbia's, which applies only to law enforcement.

If, under any of these exceptions, storage or disclosure of, or access to, personal information takes place outside Canada, "a service provider shall only collect and use such personal information that is necessary to fulfill its obligation as a service provider, and shall at all times make reasonable security arrangements to protect any personal information that it collects or uses by or on behalf of a public body."[29]

As in British Columbia, a public body, service provider, or associate must notify "the Minister" if it receives or "has reason to suspect" that it has received a foreign demand for disclosure, or if it "has reason to suspect that unauthorized disclosure of personal information has occurred in response to a foreign demand for disclosure."[30]

Disclosure of personal information is prohibited, except for specified purposes that are similar to those in the British Columbia law. The Nova Scotia law does not include an exception for "installing, implementing, maintaining, repairing, trouble shooting or upgrading an electronic system" or for related "data recovery," but it does include an exception allowing a "director, officer or employee" of a public body, but not of a service provider or associate, to carry personal data out of Canada in "a computer, a cell phone or another mobile electronic device," but only if "the head considers it is necessary for the performance" of the individual's duties.[31]

The law includes statutory protection for employees of service providers and their associates, but interestingly not of public bodies, who act as whistleblowers and report past or planned violations of the law.[32] Penalties for violating the Nova Scotia act range from $2,000 for individual employees to $500,000 for corporations.[33]

Other provincial responses have been less dramatic, but two nevertheless pose issues for transferring personal data held by a public authority to, or accessing them from, outside Canada.

Québec

In 2006 Québec amended its Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information to require that before "releasing personal information outside Québec or entrusting a person or a body outside Québec with the task of holding, using or releasing such information on its behalf," public bodies must ensure that the information receives protection *"equivalent"* to that afforded under provincial law.[34]

Under the amended act, "[i]f the public body considers that the information … will not receive protection equivalent to that afforded under this Act, it must refuse to release the information or refuse to entrust a person or a body outside Québec with the task of holding, using or releasing it on its behalf."[35] The text and timing of the amendment suggest that it may have been intended to prohibit the export of personal data to other countries, or even to other Canadian provinces, that lack "equivalent" protection to that provided by Québec law.

In addition, Québec's Act Respecting the Protection of Personal Information in the Private Sector provides that an organization doing business in Québec that entrusts a person outside Québec with "holding, using or communicating such information on its behalf" must take "all reasonable steps to ensure" that the information will be used only for the purposes for which consent was obtained and will not be "communicated to third parties" without such consent.[36]

If the organization considers that the information "will not receive the protection" required under the act, it "must refuse to communicate the information or refuse to entrust a person or a body outside Québec with the task of holding, using or communicating it" on its behalf.[37]

Alberta

Finally, Alberta's Freedom of Information and Protection of Privacy Act, like the federal Privacy Act, permits the disclosure of personal information controlled by a public body in response to a "subpoena, warrant or order" issued by a court.[38] However, unlike the federal law, Alberta's act imposes the additional requirement that the court have "jurisdiction in Alberta."[39] It

would therefore violate the act for a public body or its service provider to provide covered information in response to a "subpoena, warrant or order" issued by a court in another province or in another country.

While this provision does not explicitly prohibit the export of public-sector personal information from Alberta or restrict provincial government bodies from using non-Alberta service providers, it could have both effects if those steps were thought necessary to protect the information from being subject to a "subpoena, warrant or order" issued by a non-Alberta court. Moreover, service providers with data centers outside Alberta might simply avoid bidding on provincial contracts to avoid the risk, however remote, of being caught in the middle of a conflict between a non-Alberta court ordering production of specified information and the Alberta statute prohibiting it.

The "Minimal" Risk Addressed by Geographic Restrictions

What is the likelihood that the U.S. government would use its powers under the USA PATRIOT Act to access data on Canadians from public-sector records that happened to be stored in, or accessible from, the United States? During the inquiry by British Columbia's Information and Privacy Commissioner into the risks posed to personal data by the USA PATRIOT Act, the Attorney General of British Columbia and other legal authorities all opined that there was little if any possibility of those data being accessed under that act. Attorney General Geoff Plant characterized the "risk of access to Canadian information under the Patriot Act" as "minimal."[40] Martin Kratz, head of the technology law practice of the Canadian law firm of Bennett Jones LLP, provided an opinion letter describing such access as "highly unlikely."[41] Stewart Baker, former general counsel of the U.S. National Security Agency (NSA) and now the assistant secretary for policy of the U.S. Department of Homeland Security, concluded that U.S. law "effectively prevents U.S. authorities from obtaining the personal information of British Columbians without the consent of Canadian authorities or in violation of Canadian law and policy."[42] The possibility of such access, Baker concluded, is "vanishingly small" and "utterly implausible."[43]

These conclusions reflect three separate considerations.

Direct Surveillance

The first consideration is that the U.S. government may have direct access to the data it needs to investigate international terrorism and other serious criminal activity through its existing surveillance programs, often operated in collaboration with Canadian authorities. For example:

- The U.S. Transportation Security Administration's Automated Targeting System assesses the risk of passengers, vehicles, and cargo entering or leaving the United States by analyzing extensive personal data provided by transportation carriers, booking agents, exporters, importers, and passengers.[44] Many of these data must be provided to Customs and Border Protection under the Advance Passenger Information System electronic data system.[45]

- The U.S. government is requiring an increasing volume of data on non-U.S. citizens seeking to enter the United States, including ten fingerprints and sufficient other identifying information to facilitate a security background check. For example, the NEXUS program allows Canadian and U.S. border protection officials to jointly gather and share information, including fingerprints, and conduct bi-national security screening on Canadian and U.S. travelers.[46] The Free and Secure Trade (FAST) program requires commercial drivers from Canada and Mexico to provide ten fingerprints, identification and immigration documents, and a digital photograph to obtain a FAST Commercial Drive Identification Card.[47]

- In an effort to fight terrorism the Terrorist Surveillance Program allows interception of telephone communications in which at least one party is located inside the United States.[48] Administration officials have acknowledged that this is only one of a "number of intelligence activities."[49]

- Beginning shortly after September 11, 2001, the Office of Foreign Assets Control in the U.S. Department of the Treasury began issuing administrative subpoenas for the data held in the U.S. operations center of the Society for Worldwide Interbank Financial Telecommunication (SWIFT). By the end of 2006, SWIFT had received 65 subpoenas, each of which required it to provide the government with potentially millions of international bank transfer records "relevant to terrorism investigations."[50]

- The NSA has publicly acknowledged collecting more than 650 million electronic communications intercepts every day.[51] "Project Echelon" intercepts, analyzes, and shares signals intelligence gathered from communications transmitted via satellite, microwave, or radio around the globe. The Canadian federal government is reportedly a partner in Echelon surveillance.

These and similar programs are likely to provide U.S. officials with predictable, systematic access to the type of information they are most likely to need for law enforcement and counterterrorism investigations.

Request to Canadian Officials

The second reason that the U.S. government is unlikely to access personal information held by Canadian provincial governmental bodies through service providers is that it would be far simpler and more reliable simply to request the data from Canadian officials. Canada and the United States have for years sought personal information from each other's territories, shared information across their borders, and negotiated when efforts to obtain that information conflicted with the values of either nation. In the words of Canada's Privacy Commissioner, "There are longstanding formal bilateral agreements between the U.S. and Canadian government agencies that provide for mutual cooperation and for the exchange of relevant information."[52]

The most prominent is the Mutual Legal Assistance Treaty, which governs the transborder collection of information between Canada and the United States.[53] The countries signed the treaty in 1985 largely in response to concerns about the use of U.S. subpoenas to obtain access to data in Canada. Under the treaty, as the British Columbia Attorney General has stressed, "U.S. authorities *must* first try to obtain records located in Canada through the assistance of Canadian authorities."[54] Article IV states that "[a] Party seeking to obtain documents, records or other articles known to be located in the territory of the other Party *shall* request assistance pursuant to the provisions of this Treaty," except when the parties otherwise agree.[55] The United States understood and acknowledged this requirement in the Senate report that accompanied the treaty when it was ratified: "a Party needing documents, records, or articles located in the territory of the other and not available under any cooperative agreement or arrangement must use the treaty to obtain them."[56] The use of the USA PATRIOT Act or any other provision of U.S. law to obtain records located in Canada without first seeking access through the treaty is prohibited.[57]

There are other agreements in place that facilitate the sharing of sensitive data between Canada and the United States (as well as other countries). In addition to the Mutual Legal Assistance Treaty, for example, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) has a memorandum of understanding with the U.S. Financial Crimes Enforcement Network (FinCEN), as well as authorities in 44 other countries, that facilitates the sharing of financial transaction information. The U.S.-Canada Treaty on Mutual Assistance in Criminal Matters governs the sharing of data between the U.S. Department of Justice and the Canadian Department of Justice.[58] Under the Shared Border Accord and Smart Border Declaration, Canada and the United States operate the NEXUS program, which allows the Canadian Border Services Agency and U.S. Customs and Border Protection to jointly gather and share information and to conduct bi-national security screening on Canadian and U.S. travelers.[59]

Canadian law provides Canadian law enforcement and antiterrorism officials with power to access personal data similar to those in U.S. law, as the Privacy Commissioner of Canada has noted repeatedly:

> The risk of personal information being disclosed to government authorities is not a risk unique to U.S. organizations. In the national security and anti-terrorism context, Canadian organizations are subject to similar types of orders to disclose personal information held in Canada to Canadian authorities.[60]

Like the United States, Canada amended its federal laws post-September 11, 2001, to expand the power of the government to collect and disclose information about its citizens.[61] In fact, Michael Geist, Canada Research Chair in Internet and E-Commerce Law at the University of Ottawa Faculty of Law, has noted that section 21 of the Canadian Security Intelligence Services Act is remarkably similar to section 215 of the USA PATRIOT Act. Both provide for warrants to be issued in secret by federal courts empowering law enforcement officials to seize tangible things.[62]

With such a long and enduring relationship between Canada and the United States, U.S. government officials would likely just ask their Canadian counterparts for what they need for their counterterrorism and law enforcement efforts, as they are required to do under the Mutual Legal Assistance Treaty.

Impracticality

The third reason for skepticism is the sheer impracticality of U.S. law enforcement or counterterrorism officials relying on searches of personal data from provincial Canadian public sector authorities held by, or accessible through, service providers in the United States. As written, the Canadian provincial laws are not limited to outsourcing large data sets outside Canada. The scope of the restrictions in at least two provinces includes using networks and services that involve "access from" another country, processing through a central data center located in another country transactional data involving public employees or services, servicing equipment containing personal data remotely from outside of Canada, Canadian public universities' using collaborative servers with non-Canadian partners, sending and routing through another nation emails containing personal data from the public sector, and even placing telephone calls from or to a location outside Canada in which any personal data from the public sector is communicated. The fact that in only two provinces were limited exceptions crafted to deal with some of these situations suggests the true scope of the geographic limitations being involved.

It is not credible to think that the U.S. government would rely on such improbable sources of data for important purposes such as protecting national security. How would the government even know when a diagnostic technician in the United States would be accessing remotely an imaging device in a Canadian hospital, or that this specific device contained images of a suspect in an investigation? How would it know when a Canadian public sector employee's call about a malfunctioning computer to a customer service center located in the United States would involve providing the service representative with remote access to the machine that happened to contain data about a suspected terrorist? How would law enforcement officials obtain the necessary authorization to conduct such serendipitous surveillance, given that the average time needed to process a section 215 order authorizing a search was 147 days in 2004 and 2005, and 169 days in 2006?[63] Why would the government rely on such happenstance, when far more powerful and predictable tools are available to it to obtain the information it needs?

The Impact of Geographic Restrictions on Data Flows

Against the "minimal," "highly unlikely," and "utterly implausible" likelihood that Canadians' public-sector records would be accessed by the U.S. government through a service

provider must be balanced the cost of geographic restrictions to Canadian residents, industry, governments, and society.

To assess these costs, the Centre for Information Policy Leadership invited its members who conduct business in Canada to provide examples (which would be used without identifying the company involved) of the impact of the provincial restrictions on their customers, employees, and operations. Their responses, combined with information from press reports and documents published by Canadian industry groups, provide practical examples of the costs of provincial geographic restrictions.

The provincial geographic restrictions are already having a measurable impact on individuals and institutions alike, in public and private sectors, and in Canada and elsewhere. The scope of this impact reflects the breadth of the provincial legal provisions, including the definition of "personal information," which includes both data that *do* and data that *could* identify a specific individual. The broad impact also reflects the wide range of services—including health care; primary, secondary, and college education; university research; and the delivery of government-owned utility services—provided by the public sector in Canada, about one-third of the Canadian economy. The Information Technology Association of Canada (ITAC) describes the British Columbia law in particular as "the most stringent public sector privacy laws in the world—creating an invisible wall beyond which personal information cannot be moved."[64] ITAC goes on to note that "[t]hese geographic restrictions apply 'across-the-board' to virtually all personal information controlled by public bodies …."[65]

The provincial laws extend to the following common activities *if they involve personal information from the public sector*:

- Networks and services that involve "access from" another country are prohibited when public-sector personal information is implicated. These include the remote diagnostic tools used by computer manufacturers located in other countries, and software-debugging and problem-reporting tools, which are standard in many operating systems and other programs that transfer corrupted files back to servers located outside Canada. Simon Fraser University in British Columbia has reported "headaches when U.S.-based software companies need to provide remote support for their programs."[66]

- 24/7/365 customer service and information access provided through non-Canadian call centers and internet service providers are not allowed because those services may

result in foreign operations having access to personal data. Increasingly commonplace services, such as allowing patients to access test results or employees to access benefits information by calling 800 numbers or visiting secure websites, are prohibited if the service is provided—or accessible—from outside Canada.

- Many convenient and cost-effective communications services, such as offshore storage of voicemail, or even accessing voicemail from outside Canada, are restricted or prohibited in some provinces. Similarly, sending emails, documents, images, or Voice Over Internet Protocol conversations that contain personal information is not permitted outside Canada, nor within Canada either since internet communications in North America are likely to be routed through the United States and it is impossible to know for certain.

- Scanning, transcription, or other processing of customer or employee records outside Canada is prohibited. Statistics Canada signed a $43.3 million contract with Lockheed Martin Canada, Inc., to provide the scanning system to convert paper census forms into digital data. After a public outcry in 2003 that the U.S. government might have access to the scanned information through the contractor's parent company, the contract was altered to eliminate Lockheed Martin Canada's access to the scanned data.[67] This meant that the company was not permitted to fine tune, service, or repair the scanning system as it was used to digitize 13 million forms, nor is it able to innovate based on the experience from that process. For its part, Statistics Canada had to employ separate firms, unconnected with the development of the system, to run it, maintain it, and respond to inevitable issues that arose when it was used. This outcome—the result of public controversy in 2003—today could be mandated by recent provincial laws if the contract involved personal information held by a provincial public body.

- Processing transactional data, such as insurance claims, travel reimbursements, or credit card transactions, through a data center located in another country is forbidden, as is storing backup tapes or using disaster recovery facilities outside Canada. One of the world's largest issuers of affinity credit cards has been told that it can no longer service cards provided to support public sector institutions in British Columbia, from outside Canada.

- Remote servicing of imaging or recording equipment or other machines that may hold personal data from outside Canada is proscribed. Manufacturers of medical

imaging and other diagnostic equipment report that they can no longer provide remote service because such service inevitably involves the technician temporarily accessing patient information. British Columbia law was amended in 2006 to permit remote servicing and document recovery in certain circumstances.[68] No other province has adopted a similar exception, and the exception would not permit, for example, the remote viewing of radiological images or other personal information from outside Canada for the purpose of medical consultation.

- The auditing and fraud detection tools that public credit unions and utilities routinely use elsewhere are blocked by these laws because those tools require checking customer or applicant information against databases located outside Canada. Antifraud networks, for example, collect data on millions of transactions and both individuals and addresses in an effort to fight fraudulent credit applications, account takeover, and other forms of identity fraud. Provincial restrictions on data flows do not allow these services to be used, since they require transferring applicant data to U.S.-based servers.

- Unless specifically exempted from the provincial law, provincial government officials or employees of the businesses that support them may not travel outside Canada with any covered data on a laptop or PDA, irrespective of intent or purpose. Some Canadian universities, for example, have "prevented professors from carrying laptops containing student information across the border."[69] Nova Scotia's act contains an exemption allowing public sector employees to carry personal data across borders if they are incidentally found on a laptop or PDA, but not the employees of service providers to those public bodies.[70]

- "Groupware," wikis, social networks, and other software tools that help people collaborate together on common objectives are not allowed if they involve participants, systems, or servers located outside Canada. The University of Alberta, Memorial University of Newfoundland, and Dalhousie University have been unable to subscribe to plagiarism detection software and to RefWorks, a "popular U.S.-based Internet tool that allows academics and students to create personal accounts and store research information."[71] The schools ultimately funded a duplicate server, based at the University of Toronto, for which they must pay both RefWorks and the university to offset the costs of maintaining it. "What it's done is added an additional layer of bureaucracy for us," according to a spokesperson for Dalhousie University in Halifax, "and people aren't happy with that, obviously, but it's something that we're

> obliged to do."[72] Dalhousie had to spend more than $15,000 to move to Canada the servers that run a New York-based service that creates "virtual classrooms."[73] The university argues that the geographic restrictions could "adversely affect cross-border research."[74]

All these are prohibited by one or more of the provincial laws if they involve personal data from the public sector, or, at least in Québec, perhaps from the private sector as well. The scope of the examples reflects the breadth of the restrictions. Some of the legal changes have only recently come into effect, which, combined with lack of compliance or lack of enforcement, means that we do not yet have evidence of all these restrictions having materialized in practice. But the broad sweep of the laws, and the documented impact they have had on valuable services, means that public bodies and service providers alike have grown wary, new contracts have been delayed, services have been reduced, and the costs of both providing those services and trying to ensure compliance with the law are increasing.

The results of provincial geographic restrictions are all too apparent.

Reduced Service

With access only to provincial or national resources it is impossible to provide the same level of service as is available in other nations with access to global resources. Remote support, 24-hour customer service through call centers around the globe, speedy responses to service calls, efficient fraud detection, and hundreds of other services depend on access to a multinational array of people and data. It is not possible to cut off those resources and still receive the same level of service at either the organizational or individual level.

Increased Bureaucracy and Less Efficient Operation

Geographic restrictions on data flows inevitably lead to greater bureaucracy and less efficient operations. This is true for both service providers and public bodies. The controversy that gave rise to the British Columbia law provides a stark example. That controversy was provoked by a decision to award a health benefits administration contract to a U.S. company, MAXIMUS Inc. After the Information and Privacy Commissioner's report, adoption of a new law, and an unsuccessful court challenge, the contract was still awarded to MAXIMUS Inc., but through a maze of subsidiaries that had to be created for the purpose. MAXIMUS BC Health Benefits Operations Inc. was created as a wholly owned subsidiary of MAXIMUS BC Health,

which in turn is owned by MAXIMUS Canada Inc., which is owned by MAXIMUS Inc.[75] Even these four levels of separation were not sufficient. The government required that the stock of MAXIMUS BC Health be placed in a trust, with instructions that the shares be handed over to the government if MAXIMUS BC Health failed to abide by the terms of the service contract. In addition, MAXIMUS agreed to pay a stipulated $35 million penalty if it breached the confidentiality provisions in the contract.[76] This complicated structure not only added inefficiency and expense to the deal, but also reduced the ability of the parent company to oversee its subsidiaries effectively.

The government faces a similar increase in bureaucracy, while having to deal with the realities of fewer competitive bidders for its work. As ITAC noted in the context of British Columbia, the reliance on geographic restrictions has "led to more complex and time-consuming procurements, fewer service providers bidding on government business, and increased costs in delivering services to governments," while "the government is devoting more time and resources to procuring goods and services, while facing increased costs in delivering services to British Columbians."[77]

Higher Costs

Higher costs inevitably result from increases in bureaucracy and reductions in efficiency, not to mention the inability to access cost-saving services, and to take advantage of centralized facilities, data, and personnel. When servers must be duplicated—one for Canada, one for the rest of the world—costs go up. When technicians have to travel to Canada, rather than take advantage of remote diagnostic and repair tools, costs go up. As ITAC noted, "[e]conomies of scale cannot be created if a service provider has to duplicate its technology and communications infrastructure and cannot draw on human resources at its service centres in other jurisdictions."[78]

Geographic restrictions pose special challenges for multinational organizations, which can no longer take advantage of the efficiencies of their size and structure to provide centralized computer support, payroll processing, hiring and promotion evaluation, risk management, or even internal audit if personal information from the public sector would be involved. Higher costs are incurred by everyone: service providers, public bodies, and ultimately Canadian taxpayers and consumers who must cover the increased costs.

Harm to the Public

Reduced service at a higher price, delays, inefficiency, and bureaucracy all affect the public. But geographic restrictions on data flows may harm the public in more significant ways. That injury can be felt in many ways: an individual who is victimized by identity fraud because the public authority could not access the appropriate fraud detection or identity verification tool, or a researcher who cannot collaborate with colleagues in other countries. Cross-border data-matching serves many valuable purposes, such as enhancing the accuracy of records, locating criminals, enhancing security, limiting the spread of infectious diseases. The inability to move public sector data outside Canada greatly restricts the ability of service providers to achieve those benefits.

Competitive Disadvantage

The ability to compete globally has been a hallmark of Canadian service and high-technology industries. In 2004, the United Nations Conference on Trade and Development recognized Canada as one of the countries, along with Ireland, India and Israel, that has gained the most so far from offshoring.[79] In its 2005 report, *Offshore Outsourcing: Opportunities and Challenges for the Canadian Economy*, the Canadian Chamber of Commerce wrote that

> [o]utsourcing, whether at home, or offshore, is a permanent part of today's economic landscape. Indeed the practice should be seen as a fundamental structural economic adjustment to an internationalized economy where international mobility of capital—including labour—is increasingly possible.[80]

When provincial governments prohibit offshore outsourcing by service providers, they undercut one of Canada's great competitive strengths. In the words of the Chamber of Commerce report, "In Canada, where firms face a small domestic consumer market, looking beyond Canada for business opportunities has long been a norm, especially for firms in the technology sector."[81] This "turning back the clock on the flow of information across borders" threatens Canadian business and the people who benefit from it.[82]

The provincial restrictions also hurt multinational businesses that wish to compete in Canada. And they do so unfairly by allowing Canadian businesses to rely on their existing servers, data centers, personnel, affiliates, and other resources to serve customers around the world, while requiring non-Canadian businesses to create provincial affiliates with provincial data

centers and other provincial resources to service public sector customers in Canada. Canadian service providers are thus allowed the efficiencies and other benefits of centralized operations, while non-Canadian firms are not.

In addition, the requirement that service providers notify the provincial government if any non-Canadian government agency seeks access to data creates a real dilemma for affected businesses. For example, a Canadian company that receives a subpoena under either Canadian or U.S. law is likely to be prohibited by the terms of subpoena from disclosing its existence to anyone other than its counsel. However, if that subpoena concerns personal information that has been obtained from, or is being processed for, a public body in British Columbia or Nova Scotia, provincial law requires that the company disclose the existence of the subpoena or face stiff civil and even criminal penalties for failing to do so. The conflict of laws is inescapable.

The anticompetitive impact is already experienced by some Canadian industries with affiliates located outside Canada. They are already prohibited from using their centralized data systems to house Canadian public sector personal data, because those data would be accessible from their non-Canadian affiliates. But the anticompetitive impact will spread throughout the burgeoning Canadian services industry if the provincial restrictions become the model for other nations. Already, other Canadian service providers are threatened in Québec and Alberta by laws that draw lines between those provinces and the rest of Canada. But as other governments follow the approach of British Columbia, Nova Scotia, Québec , and Alberta and adopt laws restricting the export of, or access to, personal data in the public sector outside their national or provincial boundaries, Canada's services industry, which accounts for 80 percent of new Canadian jobs between 1992 and 2005, and the people it supports will suffer.[83]

Thinking Ahead

The risks to individuals, businesses, and public bodies created by provincial restrictions seem unjustified in light of the limited likelihood of the event—access by the U.S. government to public sector personal data through a service provider—occurring. But those risks are *unnecessary* as well. The geographic restrictions approach to protecting privacy ignores the concepts of reasonableness, balance, and respect for national sovereignty recognized in Canadian law.

In its decision rejecting the union's suit against outsourcing administration of British Columbia's public sector health services, the provincial Supreme Court stressed the importance of the reasonableness requirement.

> The importance of the right to privacy … cannot be minimized. Those fundamental rights are contained in the Charter for the benefit of all Canadians. However, those rights, as previously stated, are not absolute. There is a *reasonable* expectation of privacy and the language [of the Charter] emphasizes that individuals should be secure against *unreasonable* search and seizure. In the case at bar …. [t]he *reasonable* expectations of privacy are satisfied by statute and by contract …. A *reasonable* expectation of privacy is protected.[84]

The geographic prohibitions also undervalue the important competing values that may conflict with information privacy. David Flaherty, the previous British Columbia Information and Privacy Commissioner and a leading scholar of privacy law, has stressed the need for balance in privacy protection in many of his writings, including a 1998 report on the British Columbia Cancer Agency: "[F]air information practices need to be consciously fashioned, by written policies, to the needs of public bodies and their clientele to deliver services effectively. Privacy protection is all about balancing competing interests."[85]

One of the competing values at stake is national sovereignty. To require a business providing services to a Canadian public body to violate the laws of other nations in which it operates by refusing to comply with lawful government demands for information is contrary to the fundamental respect for national sovereignty embodied in Canadian law. As the Privacy Commissioner of Canada concluded,

> Canada must respect the legal frameworks of other countries. The [Personal Information Protection and Electronic Documents] Act cannot prevent foreign authorities from lawfully accessing the personal information of Canadians held by organizations within their jurisdiction. Likewise, the Act cannot force Canadian companies to stop outsourcing to foreign-based service providers (or service providers that operate in several jurisdictions).[86]

Following disclosure of the SWIFT subpoenas, the federal Privacy Commissioner of Canada conducted an investigation into whether SWIFT's compliance with the Treasury subpoenas violated Canadian law. She concluded that it did not.

> Multi-national organizations must comply with the laws of those jurisdictions in which they operate. Thus, while they operate in Canada, they obviously must comply with Canadian law. However, to ask the organization to ignore the legitimate laws of other jurisdictions in which they operate is unrealistic and unworkable. Moreover, it has the potential of being interpreted as an infringement by Canada on that nation's sovereignty. It is for this reason that, in my opinion, the [Personal Information Protection and Electronic Documents] Act acknowledges that an organization that is subject to the Act and that has legitimately moved personal information outside the country for business reasons may be required at times to disclose it to the legitimate authorities of that country.[87]

Fortunately, as this decision suggests, Canadian federal law provides a more flexible and practical way forward. That path is described not only in the Privacy Commissioner's opinions, but also in a guidance document, *Taking Privacy Into Account Before Making Contracting Decisions*, prepared by the Treasury Board of Canada Secretariat.[88] Rather than rely on across-the-board geographic restrictions on data, the Treasury Board's approach requires public bodies when contracting for services to apply a context-specific "invasion-of-privacy test." Under that test, agencies evaluate:

- the sensitivity of the personal information, including whether the information is detailed or highly personal (e.g., health information), and the context in which the information was collected;
- the expectations of the individuals to whom the personal information relates (including the assurance that their information will be shared only on a need-to-know basis); and
- the potential injury if personal information is wrongfully disclosed or misused, including the potential for identity theft or access by foreign governments.[89]

As the board writes, "[t]he above privacy considerations will assist institutions in identifying potential risks with respect to the proposed program delivery instrument that should be mitigated as part of the contracting process."[90]

On the specific issue of the likelihood of access by foreign governments, the board offers a four-level approach, as shown in Figure 1.

No Risk	Databases maintained and processed on a Government of Canada site only, or databases located or maintained off-site and processing conducted by a Canadian company that operates in Canada only. Records storage/archival and disposal handled on a Government of Canada site only or by a Canadian company operating in Canada only.
Low Risk	Databases located or maintained off-site and processed by a company in Canada, with potential access by a foreign subcontractor or potential access by foreign parent company or affiliate (with risk mitigation strategies in place). Records storage/archival and disposal handled off-site by a company in Canada, with potential access by a foreign subcontractor or potential access by foreign parent company or affiliate (with risk mitigation strategies in place).
Medium Risk	Database maintained and processing conducted by a foreign-based company in a foreign jurisdiction (with risk mitigation strategies in place).
High Risk	Database maintained and processing conducted by a foreign-based company in a foreign jurisdiction (with no risk mitigation strategies in place). Records storage/archival and disposal handled by foreign-based company in foreign jurisdiction.[91]

Figure 1

Under this approach, most of the everyday services that would be prohibited by the geographic restrictions in the provincial laws, would be considered only low or medium risk, and would likely be permitted, especially if they did not involve sensitive information or if the likelihood of access by a foreign government was limited.

The hallmark of the Canadian Treasury Board approach and of the opinions of the federal Privacy Commissioner is their sensitivity to the specific risks and opportunities presented in each situation. This allows them explicitly to take into account competing values—for example, the need for the personal information—and it focuses the attention and resources of public bodies and private-sector service providers on where the risks are greatest.

Conclusion

The USA PATRIOT Act poses little risk to Canadians' personal information held by public bodies, which is stored in, or accessible from, the United States. The U.S. government would seem far more likely to access the data it needs for counterterrorism and law enforcement purposes through existing surveillance programs, some operated in partnership with Canada, or by simply asking Canadian officials, who exercise powers similar to those of their U.S. counterparts, for the required data. The likelihood of the government resorting to searches of personal data from provincial Canadian public sector authorities held by, or accessible through, service providers in the United States as a reliable law enforcement or counterterrorism tool is "vanishingly small."[92]

Against that minimal risk must be measured the demonstrated harms caused by the provincial geographic restrictions. Those include fewer services available to Canadian public bodies and residents, increased bureaucracy and significantly reduced efficiency, higher financial costs, the real threat of tangible harms to health and safety, and the undermining of competition for public bodies' business and of Canada's burgeoning services industry. Taken together, these harms are a high price to pay to guard against the "utterly implausible" access by U.S. officials.[93]

The more pragmatic and balanced approach of the federal Canadian government to the issue of foreign government access to personal data in the public sector demonstrates that the high price of the geographic ban is also unnecessary. A comparable level of protection can be provided through a more rational analysis of the sensitivity of the information, the expectations of individuals whose data are involved, and the probability and gravity of the potential harm. Such a thoughtful approach, matched with a proportional response, promises effective privacy protection without compromising other important values.

Notes

[1] 50 U.S.C. § 1861.

[2] British Columbia Bill 73—the Freedom of Information and Protection of Privacy Amendment Act, 2004, § 30.1.

[3] Id. § 30.2(2).

[4] Québec Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information, § 70.1 (added by 2006, c. 22, s. 47).

[5] Alberta Personal Information Protection and Electronic Documents Act, § 40(1)(g); Canada Privacy Act, § 8(2)(c).

[6] Ross Breckon, Vice President of EDS Canada Inc., EDS Canada Submission on the USA Patriot Act at 29 (2004) (letter from Stewart A. Baker, Steptoe & Johnson, LLP, to Ross Breckon, July 19, 2004).

[7] Id.

[8] Pub. L. 107-56, 115 Stat. 272 (2001).

[9] 50 U.S.C. § 1861.

[10] Information and Privacy Commissioner of British Columbia, *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing* (Oct. 2004).

[11] Id. at 18.

[12] Id. at 134-135.

[13] Bill 73—the Freedom of Information and Protection of Privacy Amendment Act, 2004.

[14] British Columbia Freedom of Information and Protection of Privacy Act § 30.1.

[15] Id. Schedule 1 (emphasis added).

[16] Id. § 30.1.

[17] Id. §§ 33.1(1)-(2).

[18] Id. § 33.1(3).

[19] Id. § 33.1(1)(p)(i) (added by the Miscellaneous Statutes Amendment Act (no.2) SBC 2006 c.24,2006-24-10(b)).

[20] FOIPPA, supra § 33.1(1)(p)(ii).

[21] Id. § 33.1(1)(e)-(e.1).

[22] Id. § 30.2(2).

[23] Id. § 30.4.

[24] Bill No. 19—the Nova Scotia Personal Information International Disclosure Protection Act, 2006, § 5(1).

[25] Id.

[26] Id. § 2(1)(b).

[27] Id. § 5(1).

[28] Id. §§ 5(2)-(3).

[29] Id. § 5(4).

[30] Id. § 6(1).

[31] Id. § 9(4).

[32] Id. § 7(1).

[33] Id. §§ 13(3)-(4).

[34] Québec Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information, § 70.1 (added by 2006, c. 22, s. 47) (emphasis added).

[35] Québec Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information, supra § 70.1

[36] Québec's Act Respecting the Protection of Personal Information in the Private Sector, § 17.

[37] Id.

[38] Alberta Personal Information Protection and Electronic Documents Act, § 40(1)(g); Canada Privacy Act, § 8(2)(c).

[39] Alberta Personal Information Protection and Electronic Documents Act, § 40(1)(g).

[40] The Hon. Geoff Plant, Attorney General of the Province of British Columbia, Submission to the Information and Privacy Commissioner for British Columbia ¶ 4.08 (2004).

[41] Ross Breckon, Vice President of EDS Canada Inc., EDS Canada Submission on the USA Patriot Act at 21 (2004) (letter from Martin Kratz, Bennett Jones LLP, to Ross Breckon, July 19, 2004).

[42] Id. at 24 (letter from Stewart A. Baker).

[43] Id. at 29, 35 (letter from Stewart A. Baker).

[44] Privacy Act of 1974; U.S. Customs and Border Protection, Automated Targeting System, System of Records, 72 Federal Register 43650 (2007) (DHS, system of records notice).

[45] Advance Electronic Transmission of Passenger and Crew Member Manifests for Commercial Aircraft and Vessels, 72 Federal Register 48320 (2007) (CPB, final rule).

[46] Documents Required for Travelers Departing From or Arriving in the United States at Sea and Land Ports-of-Entry From Within the Western Hemisphere, 72 Federal Register 35088, 35093 (2007) (DHS, Dept. of State, proposed rule).

[47] Id. at 35093-35094.

[48] James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, Dec. 16, 2005, at A1.

[49] Letter from J.M. McConnell, Director of National Intelligence, to Senator Arlen Specter, Ranking Member of the Senate Judiciary Committee (July 31, 2007).

[50] Office of the Privacy Commissioner of Canada, *Commissioner's Findings* ¶ 30 (Apr. 2, 2007), http://www.privcom.gc.ca/cf-dc/2007/swift_rep_070402_e.asp.

[51] U.S. Department of Defense, Technology and Privacy Advisory Committee, *Safeguarding Privacy in the Fight Against Terrorism* 48 (2004).

[52] *Bank's Notification to Customers Triggers PATRIOT Act Concerns*, supra.

[53] Mutual Legal Assistance Treaty Between United States and Canada, reprinted in S. Treaty Doc. 100-14, 100th Cong., 2d Sess. (1988).

[54] The Hon. Geoff Plant, supra ¶ 2.07.

[55] Mutual Legal Assistance Treaty, supra art. iv.

[56] Senate Report, Treaty with Canada on Mutual Legal Assistance in Criminal Matters, reprinted in S. Treaty Doc. 100-14, 100th Cong., 2d Sess. (1988).

[57] The British Columbia report argues that because the treaty only applies to requests for assistance in relation to the investigation or prosecution of an "offence," it would not apply to "intelligence gathering or surveillance where no investigation or prosecution of an 'offence' is involved." *Privacy and the USA Patriot Act*, supra at 102. Under U.S. law, section 215 orders can only be issued as part of "an investigation to protect against international terrorism or clandestine intelligence activities," both of which constitute offenses under U.S. and Canadian law. Pub. L. No. 107-56, § 215. It therefore seems unlikely that U.S. authorities would be able to invoke section 215 without also triggering the Mutual Legal Assistance Treaty.

[58] See *Report of Findings*, Apr. 2, 2007, supra.

[59] Documents Required for Travelers Departing From or Arriving in the United States at Sea and Land Ports-of-Entry From Within the Western Hemisphere, supra at 35093.

[60] Office of the Privacy Commissioner of Canada, *Bank's Notification to Customers Triggers PATRIOT Act Concerns* (PIPEDA Case Summary #313), Oct. 19, 2005, http://www.privcom.gc.ca/cf-dc/2005/313_20051019_e.asp; see also Office of the Privacy Commissioner of Canada, *Report of Findings in Files 6100-02681, 6100-02682, 6100-02683,* ¶ 37 (Aug. 7, 2008).

[61] See, e.g., An Act to amend certain Acts of Canada, and to enact measures for implementing the Biological and Toxic Weapons Convention, in order to enhance public safety, SC 2004, C.15.

[62] Michael Geist and Milana Homsi, *The Long Arm of the USA Patriot Act: A Threat to Canadian Privacy?* 24 (2004).

[63] Statement of Glenn A. Fine, Inspector General, U.S. Department of Justice, before the Senate Committee on the Judiciary concerning "The FBI's Use of National Security Letters and Section 215 Requests for Business Records," Mar. 21, 2007, at 11, http://www.usdoj.gov/oig/testimony/0703a/final.pdf; Statement of Glenn A. Fine, Inspector General, U.S. Department of Justice, before the House Committee on the Judiciary Subcommittee on the Constitution, Civil Rights, and Civil Liberties concerning "The FBI's Use of National Security Letters and Section 215 Requests for Business Records," Apr. 15, 2008, at 9, http://www.usdoj.gov/oig/testimony/t0804/final.pdf.

[64] Information Technology Association of Canada, *The USA Patriot Act and the Privacy of Canadians* 4 (July 2005).

[65] Id.

[66] "Universities Find Ways to Keep Info Out of U.S. Hands," *The Record* (Kitchener-Waterloo, Ontario), Sep. 24, 2007, at D2.

[67] Dean Beeby, "Census Includes Same-Sex Marriage Question," *Globe & Mail*, Apr. 18, 2005, at A9.

[68] British Columbia Freedom of Information and Protection of Privacy Act § 33.1(1)(p)(i) (added by the Miscellaneous Statutes Amendment Act (no.2) SBC 2006 c.24,2006-24-10(b)).

[69] "Universities Find Ways to Keep Info Out of U.S. Hands," supra at D2.

[70] Bill No. 19—the Nova Scotia Personal Information International Disclosure Protection Act, 2006, § 9(4).

[71] Caroline Alphonso, "Universities Move to Hide from U.S. Eyes," *Globe & Mail*, Nov. 11, 2006, at A15.

[72] "Universities Find Ways to Keep Info Out of U.S. Hands," supra at D2.

[73] Id.

[74] Id.

[75] *British Columbia Government & Service Employees' Union v. The Minister of Health Services & The Medical Services Commission*, 2005 British Columbia Supreme Court 446 ¶¶ 68-70.

[76] Id.

[77] Information Technology Association of Canada, supra at 5.

[78] Id.

[79] Id. at 7.

[80] Canadian Chamber of Commerce, *Offshore Outsourcing: Opportunities and Challenges for the Canadian Economy* 3 (2005), http://www.chamber.ca/cmslib/general/outsourcing050113.pdf.

[81] Id.

[82] Information Technology Association of Canada, supra at 7.

[83] Canadian Services Coalition & Canadian Chamber of Commerce, *Canadian Services Sector: A New Success Story* 3 (2006), http://www.canadianservicescoalition.com/CanadianServicesSectorANewSuccessStory.pdf.

[84] *British Columbia Government & Service Employees' Union v. The Minister of Health Services & The Medical Services Commission*, 2005 British Columbia Supreme Court 446 ¶¶ 68-70 (emphasis added).

[85] Information and Privacy Commissioner of British Columbia, *The British Columbia Cancer Agency: The Results of a Privacy Check-Up* (1998).

[86] Office of the Privacy Commissioner of Canada, *Responsibility of Canadian financial institutions in SWIFT's disclosure of personal information to US authorities considered* (PIPEDA Case Summary #365), Apr. 2, 2007, http://www.privcom.gc.ca/cf-dc/2007/365_20070402_e.asp.

[87] Office of the Privacy Commissioner of Canada, *Report of Findings*, Apr. 2, 2007, http://www.privcom.gc.ca/cf-dc/2007/swift_rep_070402_e.asp.

[88] Treasury Board of Canada Secretariat, *Guidance Document: Taking Privacy Into Account Before Making Contracting Decisions* (2006), http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/gd-do/gd-do_e.asp.

[89] Id. at 7.

[90] Id.

[91] Id. at 21.

[92] Ross Breckon, supra at 29 (2004) (letter from Stewart A. Baker).

[93] Id.

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP