Privacy and the USA Patriot Act

Implications for British Columbia Public Sector Outsourcing

October 2004

Information & Privacy Commissioner for British Columbia

REPORT SUMMARY

In the spring of 2004, the Office of the Information and Privacy Commissioner for British Columbia (OIPC) began receiving requests from government, the media, interest groups and members of the public for guidance about possible implications for the privacy of British Columbians of section 215 of the USA Patriot Act, a US federal law passed in October of 2001.[1] These requests for guidance related to initiatives for outsourcing British Columbia government functions to US companies or their Canadian subsidiaries.

Interest in the USA Patriot Act was triggered by the widely reported launch of a lawsuit in the British Columbia Supreme Court by the British Columbia Government and Service Employees' Union (BCGEU) to stop the British Columbia Ministry of Health Services from contracting out the administration of British Columbia's public health insurance program, the Medical Services Plan, to a US-linked private service provider. One of the BCGEU's claims was that the proposed outsourcing would contravene British Columbia's Freedom of Information and Protection of Privacy Act (FOIPPA) by making the personal health information of British Columbians accessible to US authorities under section 215 of the USA Patriot Act.

What We Asked

In May 2004, the Information and Privacy Commissioner initiated a public process seeking submissions on two questions:

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

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

What We Heard in Response

More than 500 submissions arrived from across Canada, the US and Europe. Those responding included individuals, governments, labour groups, information technology companies, health care providers, library associations, privacy advocacy organizations and other information and privacy

1 Section 215 concerns secret court orders enabling the FBI to obtain access to "any tangible thing" for foreign intelligence purposes or to protect against international terrorism or clandestine intelligence activities. USA Patriot Act stands for the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001.

commissioners.

There was general consensus that US authorities could, at least under some circumstances, use powers enacted by the USA Patriot Act to make orders for access to personal information located in Canada that is involved in outsourcing of public body functions to a US linked contractor. There was, however, a clear difference of opinion about whether the risk of access is unknown, low or of great concern, and what the implications might be for public body compliance with FOIPPA's privacy protection rules. Some information technology companies argued that there is no need for additional precautions to deal with any risk posed by the USA Patriot Act. Other submissions argued that the risk is so great that outsourcing to US-linked companies should be prohibited altogether. Others pressed the case for stiffer contractual provisions, legislative amendments or technological solutions.

The submissions consistently endorsed the value of privacy and raised larger questions about the place of privacy in an era of economic globalization, widespread fear of terrorism, and flows of data across borders. Several themes related to these issues emerged in the submissions:

- Many people feel that they are losing control over what happens to their personal information and worry that their privacy rights are being further displaced by economic and national security priorities.
- Disclosure of sensitive personal information, particularly that of a medical nature, can lead to discrimination against people with physical or mental disabilities—for example, people who are known to be HIV-positive can be turned away from the US border—and may jeopardize health care for patients who, fearing disclosure, withhold critical information from their doctors or simply avoid seeking treatment.
- Globalization of the information technology industry, enhanced by free trade and the ease of data transfer, produces economic opportunities but also raises concerns about national sovereignty and creates privacy challenges for businesses, governments, regulators and the public.
- Developments in information technology are fuelling governments' appetite for larger data banks and mining of data for national security and other purposes, and new laws are encouraging private sector disclosure to government authorities of customers' personal information for national security and law enforcement purposes.
- There are indications of a trend developing whereby personal information collected for national security purposes (including border and transportation security) may be used more frequently for ordinary law enforcement investigations. This leads to a blurring of the traditional division between the role of the state in protecting the public from domestic and foreign national security threats and its role in enforcing ordinary criminal and regulatory laws, which has significant implications for privacy and other civil rights.

The questions we posed cannot be considered in isolation from these broader and interrelated themes, which relate to the importance of privacy as a democratic right, expanding risks for privacy in an ever more interconnected world, and the risk and potential impacts of disclosure of personal information to US and other foreign authorities.

Protecting Personal Information: Old Rights and New Laws

Privacy is not an absolute right. If we accept the notion that trade-offs are sometimes necessary, whether for reasons of efficiency, economic benefits or national security and public safety, where and

how do we draw the line? To answer that question, and in doing so to answer the two questions that this report addresses, it is important to understand why democratic societies consider privacy a fundamental value and how they protect it.

The essence of liberty in a democratic society is the right of individuals to autonomy—to be free from state interference. The right to privacy has several components, including the right (with only limited and clearly justified exceptions) to control access to and the use of information about individuals. Although privacy is essential to individual autonomy, it is not just an individual right. A sphere of privacy enables us to fulfill our roles as community members and is ultimately essential to the health of our democracy.

The right to privacy was confirmed in the UN's 1948 Universal Declaration of Human Rights. Concerns about the impact of information technology on privacy, and about international data flows, triggered the first privacy laws, which were passed in several European countries starting in the early 1970s. Virtually every privacy law reflects several key internationally accepted principles that require governments and organizations to

- collect personal information directly from the person to whom it relates and explain why it is needed;
- only collect the information necessary for the intended purpose;
- use the information only for the purpose for which it was collected unless the person consents to other uses; and
- provide an opportunity for the person to see and to correct his or her personal information if it is inaccurate.

Canada's legislative privacy protections began in 1978 with the Canadian Human Rights Act. A year after the Canadian Charter of Rights and Freedoms came into effect in 1982, Canada's Privacy Act imposed privacy obligations on federal government departments and agencies. Several provinces followed suit and British Columbia's FOIPPA came into force in 1993. In January 2001, the federal government brought in new legislation extending privacy protections to the activities of private sector organizations (the Personal Information Protection and Electronic Documents Act). Similarly, on January 1, 2004, British Columbia's private sector privacy legislation, the Personal Information Protection Act, came into effect.

Due in part to its cultural and constitutional history, the US has followed a different route from Canada and Europe in the privacy field. No independent body was established to enforce the US federal Privacy Act and few US states have enacted laws regulating government use of personal information. Regarding commercial activities, the US has opted for sector-specific laws with an emphasis on self-regulation or enforcement by private litigation, rather than through independent oversight. There is ongoing tension between the US and Europe regarding the adequacy of US privacy laws. Canada's privacy laws are much more in tune with Europe's.

Much of the discomfort voiced about the implications of the USA Patriot Act for Canadians can be attributed to the disparity between the American and Canadian approaches to privacy. As a result of this disparity, Canadian personal information flowing across the border into the US does not always enjoy the same standards for protection that we have come to expect here.

Sharing Personal Information: Data in a Seamless Society

Technological advances and trade liberalization have increased the international flow of personal information in both the private and the public sectors. Data-management companies compete to offer public

sector clients technology and services for storing, organizing and accessing information. Governments in Canada and elsewhere have increasingly been following the lead of corporations in contracting out services formerly done in-house.

An ever more complex set of rules and agreements governs the international trade in goods and services. Canada must be careful when negotiating international trade obligations that relate to or may affect the delivery of public services to ensure that privacy protection is maintained in accordance with Canadian values.

Advanced technologies have created the ability to merge isolated databases into massive banks of information about identifiable individuals. This, in turn, enables data mining—the application of database technology and techniques to uncover patterns and relationships in data and to undertake the prediction of future results or behaviour. The hidden patterns and subtle relationships that data mining detects are recorded and become personal information about the individual whose characteristics or habits are being searched and analyzed. A recent audit by the US Government Accountability Office has studied the extent of data mining by US federal agencies. It confirmed that this practice is increasingly common and that many of the data mining efforts involve the use of personal information. The extent of data mining by governments in Canada has not been the subject of sufficient or transparent study and documentation and, in our view, since the privacy implications of data mining can be significant, this needs to be remedied.

These trends in data flows have had at least four effects:

1. As society cannot predict with accuracy where technology will take data management in the future, it needs to institute sufficient legal privacy protections today so that public policy will guide technology, not the reverse;
2. Once personal information crosses borders, regulating its use is at its best difficult and at its worst impossible;
3. Increasing private and public sector reliance on digitally stored, analyzed and accessed personal information increases the risk that inaccurate or limited snapshots of an individual will be misused, whether intentionally or not; and
4. The distinction between business and state uses of personal information is becoming blurred and will increase the risks to privacy and to other individual rights and interests.

State Surveillance: Privacy and National Security

Surveillance is a tool for intelligence gathering. Governments use a myriad of sources of information, both open and secret, to gather both foreign and domestic intelligence for national security purposes. Intelligence gathering produces undisclosed dossiers detailing individuals' lifestyles, acquaintances and activities—anything that can help shed light on threats they may pose either individually or through association with others. However, although intelligence gathering relies on a wide variety of sources, it may not provide a complete picture and may produce inaccurate information about individuals.

Since September 11, the US, Canada and other countries have increased the intensity and breadth of their foreign and domestic intelligence gathering activities in order to detect and deter terrorist activities. New technologies for gathering and analyzing data promise to increase the sophistication and the scope of surveillance for intelligence gathering purposes. These new technologies may outstrip the ability of society to set clear and continuously relevant rules for their use, creating the risk that technology will shape society rather than be controlled by it.

Canada and the US passed anti-terrorism laws with haste in 2001. Three years later it is time to take

stock and to consider the idea that privacy and security are not contradictory terms. For example, openness about the criteria used to compile information found in "no fly lists" and providing the opportunity to correct wrong personal information contained in those lists need not compromise security. In the long term, the security of a country depends as much on citizens' confidence in continued respect for civil rights as it does on their confidence in public safety.

Most people accept the need for state surveillance and intelligence gathering to deal with threats to public safety, whether from domestic criminal activities or from outside national borders. However, we must ensure that surveillance is subject to controls, including independent oversight of the circumstances in which it is undertaken and the way in which the information gathered is subsequently used. Real harm can result to individuals when their personal information is misused, even with the best of intentions.

More broadly, excessive surveillance in the name of national security and public safety can threaten the freedoms on which every successful democracy depends. Awareness of widespread surveillance makes people nervous about speaking their minds, engaging in political activities, or doing anything that might arouse ill-founded or vague suspicion. Excessive surveillance herds people toward conformity and discourages the diversity of ideas and beliefs that are indispensable to the flourishing of our communities.

Heightened fears about terrorism or other national security and public safety threats can impede the careful assessment of new technologies and state initiatives. Canadian governments should carefully assess existing and proposed surveillance activities, laws and technologies to ensure they do not improperly or unnecessarily diminish privacy and are subject to meaningful controls and independent oversight.

Anti-terrorism Laws in the US

The USA Patriot Act, enacted by the US Congress shortly after September 11, 2001, is anti-terrorism legislation that, among other things, expands the intelligence gathering and surveillance powers of law enforcement and national security agencies by amending the US Foreign Intelligence Surveillance Act (FISA). One of the intended effects of the USA Patriot Act was to tear down the "wall" that previously separated conventional law enforcement from national security intelligence gathering activities. USA Patriot Act provisions have been used in ordinary criminal investigations and have expedited surveillance in a myriad of circumstances, not all of which are terrorism related.

FISA, originally enacted in 1978, gives US authorities the power to gather intelligence on foreign agents in the US and abroad. The Foreign Intelligence Surveillance Court (FIS Court) issues secret orders under FISA allowing US authorities to gather information about individuals. Failure to comply with a FISA order, and to keep its existence secret, is an offence in the US.

Section 215 of the USA Patriot Act amended FISA to allow US authorities to, among other things, obtain records and other "tangible things" to protect against international terrorism and against clandestine intelligence activities. Section 218 of the USA Patriot Act amended FISA so that foreign intelligence gathering need only be "a significant purpose", rather than the only purpose, of FISA searches or surveillance in the US, leading some critics to suggest it could be used as a backdoor tool for enforcement of ordinary criminal and regulatory laws.

Section 505 of the USA Patriot Act expanded the circumstances under which the FBI can issue "national security letters" in the US to compel financial institutions, phone companies and Internet service providers secretly to disclose information about their

customers. The FBI is required only to establish that the information it seeks is relevant to an authorized intelligence investigation.

Anti-terrorism Laws in Canada

Other governments faced considerable pressure to strengthen national security and public safety laws after September 11. Like the USA Patriot Act, Canada's Anti-terrorism Act, enacted in December of 2001, amended several existing laws. Among other things, it created new terrorism offences under the Criminal Code and amended the definition of "threats to the security of Canada" in the Canadian Security Intelligence Service Act (CSIS Act). Even prior to the enactment of the Anti-terrorism Act, the CSIS Act provided for a generous mandate to collect information about people, whether in Canada or abroad, and the authority to disclose it where thought to be necessary.

In 2004, Parliament passed a new Public Safety Act, portions of which are not yet in force. The Act expanded police investigation powers and changed existing law to involve the private sector in the collection and disclosure of personal information for national and other security purposes. Amendments to the federal Personal Information Protection and Electronic Documents Act permit private sector organizations to collect and disclose personal information of customers or clients for certain law enforcement and national security purposes.

Among the Public Safety Act amendments to the Aeronautics Act that are in force are those requiring airlines to disclose personal information about passengers to the responsible minister or other designated authorities for transportation security purposes. The amendments that have not yet been brought into force will allow this data to be disclosed to CSIS and the RCMP. The data may be matched with other data and may be used to assist in executing certain outstanding warrants. When in force this new authority will effectively compel the private sector to assist the state, in the absence of a warrant or court order, in surveillance of all air travellers.

The balance between privacy and Canada's security and law enforcement interests is dynamic. In the ongoing quest for the right balance, it is vital that the broadening of the state's ability to take steps to satisfy our legitimate security needs does not blur into activities that are in reality the ordinary enforcement of laws. The need to deal with the threat of terrorism may appear much more immediate and easier to understand than the need to maintain the basic civil rights to which we have become accustomed. However, our measures for dealing with terrorism must be carefully guided to address real threats, instead of our fears, to ensure that we do not unnecessarily lose the safeguards of our liberties in law or in practice.

Privacy Rights under the Canadian Charter of Rights and Freedoms

All levels of government in Canada must ensure that their laws are consistent with the Canadian Charter of Rights and Freedoms and that their policies and actions do not offend Charter protections. Several submissions suggested that putting British Columbians' personal information at risk of seizure under the USA Patriot Act might conflict with privacy protection under the Charter. While we do not analyze this question, we acknowledge that Canadian courts require Charter values and rights to be considered in interpreting legislation such as BC's FOIPPA.

Charter protections include the right to be secure against unreasonable search and seizure (section 8) and the right to life, liberty and security of the person (section 7). The Supreme Court of Canada has determined that section 8 guarantees the right to

enjoy a reasonable expectation of privacy and protects individuals from arbitrary intrusion by government. This extends to the collection and use of personal information. The closer the information is to one's "biographical core"—such as information about one's health, genetic characteristics, sexual orientation, employment, social or religious views, friendships and associations—the greater is the obligation on government to respect and protect the individual's privacy. We have accounted for these Charter values and rights in interpreting FOIPPA for the purposes of this report.

Protecting Privacy in British Columbia: FOIPPA Requirements

FOIPPA, because it deals with access to information and the protection of personal privacy, is considered to be legislation of special or fundamental importance. Its subject matter, particularly informational privacy, receives significant constitutional protection under the Charter. FOIPPA applies to over 2,000 provincial government ministries and other public bodies in British Columbia. It imposes restrictions on the collection, use and disclosure of personal information.

Section 30 of FOIPPA, which is at the heart of this report, reads:

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

Outsourcing of public body functions to private contractors is not inconsistent with FOIPPA. A public body cannot, however, outsource functions in a manner that would result in non-compliance with FOIPPA. The steps that public bodies must take to protect personal information in outsourcing arrangements depend on the meaning of this section, especially the words "reasonable" and "unauthorized".

In assessing what constitutes "reasonable" security arrangements, the nature of the personal information involved and the seriousness of the consequences of its unauthorized disclosure need to be taken into account. It is clear, however, that security arrangements to protect against unauthorized disclosure of personal information are always necessary, regardless of its sensitivity.

We have also concluded that disclosure of personal information in response to a foreign law or order is "unauthorized" under section 30 of FOIPPA because a foreign law does not apply in British Columbia.

Section 33 spells out circumstances where public bodies may disclose personal information—for example, in accordance with treaties or to law enforcement agencies in certain cases—but we have concluded that none of these applies to allow disclosure in direct response to court orders made in the US under FISA or to national security letters issued by the FBI.

Some submissions suggested that unauthorized disclosure of personal information in British Columbia in response to a FISA order (or a national security letter) is of little concern because extensive transnational information transfer mechanisms that are recognized by FOIPPA would make an extraterritorial foreign order unnecessary. We concluded that it is unlikely that US authorities engaged in intelligence gathering would use the Canada-US treaty for mutual legal assistance in criminal matters (MLAT) for practical and legal reasons. We also concluded that it is not clear that US authorities would have available, or necessarily use, other information transfer methods—such as information sharing agreements—that are recognized in MLAT and in section 33 of FOIPPA. This raises important parallel issues regarding government transfers of personal information about

people in Canada to other countries that warrant rigorous study.

The British Columbia government's commitments not to send sensitive personal information to the US, to prohibit contractors from disclosing personal information unless permitted by FOIPPA, and to require them to notify the British Columbia government of US requests for disclosure, are positive steps.

We conclude that section 30 requires reasonable, but not absolute, security. There is a reasonable possibility of unauthorized disclosure of British Columbians' personal information pursuant to an extraterritorial US order or national security letter. That reasonable possibility is not sufficiently, or practically, dealt with by a ban on outsourcing. Our recommended solution is to put in place rigorous other measures (legislative, contractual and practical) to mitigate against illegal and surreptitious access.

Potential Use of the USA Patriot Act in Canada

There is general consensus in the submissions to us that the FIS Court could, under FISA, order a US-located corporation to produce records held in Canada that are under the US corporation's control. US courts have, in fact, been willing over the years to order disclosure, for the purpose of US proceedings, of records held outside the US, as long as a person or corporation subject to the US court's jurisdiction has legal or practical ability to access those records.

This requires us to consider whether control over records can be avoided through practical or contractual arrangements between public bodies and service providers. Some US courts have found that, under US law, control of records exists whenever there is a US parent-Canadian subsidiary corporate relationship, regardless of the contractual or practical arrangements between a British Columbia public body and the service provider or its US parent. Other US cases suggest, however, that contractual or practical arrangements may influence a US court's findings regarding control.

Even if control over Canadian records is found, it is not known whether the FIS Court would order disclosure if our law prohibited it. Submissions to us discussed whether a statutory provision in British Columbia that prohibits compliance with such an order would be effective. We cannot ignore the fact that US courts have upheld subpoenas ordering corporations to disclose records located outside the US, even where a foreign law prohibits the disclosure. We nonetheless conclude, however, that the FIS Court might decline to order disclosure in the face of a clear and strong British Columbia law prohibiting disclosure. The benefit of such statutory provision is not limited to its persuasive value to a US court; its compliance and deterrence effect within British Columbia is of even greater significance.

We do not exclude the possibility that policy or procedural safeguards exist in respect of FISA applications for disclosure of records located outside the US. In the absence of evidence of such safeguards, however, it is prudent to assume that US authorities are unfettered in their ability to seek such an order, that they may do so in circumstances that are not consistent with Canadian law and policy, and that the FIS Court might issue a FISA order for records located in Canada.

Recommendations

Provincial actions alone are not sufficient to address risks posed by transfers of personal information across national borders, whether as a result of FISA orders or of other information-sharing mechanisms. National dialogue and action are

required. Our recommendations reflect this reality as well as the fact that the risk of USA Patriot Act access is not just an issue for the public sector or this country. It is also an issue for the private sector and will have to be addressed by all jurisdictions across Canada and at an international level.

The final chapter of this report details our reasons for the recommendations listed below. The OIPC will monitor progress in implementation of these recommendations and will report publicly on progress within 12 months of the release of this report.

Amendments to FOIPPA

Recommendation 1

The government of British Columbia should amend the Freedom of Information and Protection of Privacy Act (FOIPPA) to:

(a) pending nation-to-nation agreement, as contemplated by Recommendation 16, 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 and from being accessed outside Canada;

(b) expressly provide that a public body may only disclose personal information in response to a subpoena, warrant, order, demand or request by a court or other authority if it is a Canadian court, or other Canadian authority, that has jurisdiction to compel the disclosure;

(c) impose direct responsibility on a contractor to a public body to ensure that personal information provided to the contractor by the public body, or collected or generated by the contractor on behalf of the public body, is used and disclosed only in accordance with FOIPPA;

(d) 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 to which FOIPPA applies;

(e) require a contractor to a public body to notify the public body of any unauthorized disclosure of personal information under FOIPPA;

(f) ensure that the Information and Privacy Commissioner has the powers necessary to fully and effectively investigate contractors' compliance with FOIPPA and to require compliance with FOIPPA by contractors to public bodies, including powers to enter contractor premises, obtain and copy records, and order compliance; and

(g) make it an offence under FOIPPA 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, punishable by a fine of up to $1 million or a significant term of imprisonment, or both.

Provincial litigation policy

Recommendation 2

The government of British Columbia should create a published litigation policy under which it would, as necessary, participate in or commence legal proceedings in Canada or abroad to resist a subpoena, warrant, order, demand or request made by a foreign court or other foreign authority for disclosure of personal information in British Columbia that is in the custody or under the control of a public body.

Further protection of personal information in BC from FISA orders

Recommendation 3

The government of British Columbia, in conjunction with the government of Canada as appropriate and

necessary, should seek assurances from relevant US government authorities that they will not seek a FISA order or issue a national security letter for access to personal information records in British Columbia.

Outsourcing contract privacy protection measures

Recommendation 4

All public bodies should ensure that they commit, for the duration of all relevant contracts, the financial and other resources necessary to actively and diligently monitor contract performance, punish any breaches, and detect and defend against actual or potential disclosure of personal information to a foreign court or other foreign authority.

Recommendation 5

Recognizing that it is not enough to rely on contractors to self-report their breaches, a public body that has entered into an outsourcing contract should create and implement a program of regular, thorough compliance audits. Such audits should be performed by a third party auditor, selected by the public body, that has the necessary expertise to perform the audit and recommend any necessary changes and mitigation measures. Consideration should be given to providing that the contractor must pay for any audit that uncovers material noncompliance with the contract.

Recommendation 6

Treasury Board should direct all ministries, agencies and organizations covered by the Budget Transparency and Accountability Act to include the activities in Recommendations 4 and 5 in their annual service plans and to ensure that service plans include all financial resources necessary to perform these functions. The government of British Columbia should consider also requiring all public bodies to plan and budget for such financial resources.

Federal protection of personal information from foreign orders

Recommendation 7

The government of Canada should consider whether federal legislation protects adequately the personal information of Canadians that is in the custody or under the control of the government of Canada or its agencies (directly or through contractors) from disclosure in response to a subpoena, warrant, order demand or request made by a foreign court or other foreign authority. This should include a thorough review of the federal Privacy Act, as earlier urged by the Privacy Commissioner of Canada, with particular attention to the fact that the federal statute contains no equivalent to the reasonable security requirement in section 30 of FOIPPA.

Recommendation 8

The government of Canada should review British Columbia's Freedom of Information and Protection of Privacy Amendment Act, 2004 (Bill 73) and consider enacting provisions to protect personal information in Canada from disclosure in response to a subpoena, warrant, order, demand or request made by a foreign court or other foreign authority.

Audits of information sharing agreements and data mining activities

Recommendation 9

The government of British Columbia should:

(a) undertake a comprehensive and independent audit of interprovincial, national and transnational information sharing agreements affecting all public bodies in British Columbia;

(b) use the audit to identify and describe operational and planned information sharing activities, including in each case: the kinds of personal information involved, the purposes for which it

is shared, the authority for sharing it, the public bodies or private sector organizations involved, and the conditions in place to control the use and security of the information shared;

(c) publicly release the audit report (including timely posting on a readily accessible government of British Columbia website);

(d) act on deficiencies or other problems indicated by the audit;

(e) conduct and publish periodic follow-up audits and reports to ensure ongoing transparency and accountability in this area; and

(f) require information sharing agreements entered into by all public bodies to be generally available to the public (including timely consolidated posting on a readily accessible government of British Columbia website).

Recommendation 10

The government of British Columbia should:

(a) undertake a comprehensive and independent audit of data mining efforts by all public bodies;

(b) use the audit to identify and describe operational and planned data mining activities, including in each case: the kinds of personal information involved, the purposes of the data mining, and the authority and conditions for doing so;

(c) ensure that the audit report also proposes an effective legislated mechanism to regulate data mining activities by public bodies and effective guidelines for the application of fair information practices to data mining by public bodies; and

(d) publicly release the audit report (including timely posting on a readily accessible government of British Columbia website).

Recommendation 11

The government of Canada should implement Recommendations 9 and 10 at the federal level.

Section 69 of FOIPPA

Recommendation 12

The government of British Columbia should:

(a) ensure that, within 60 days after the date of release of this report, all ministries are fully compliant with the reporting requirements of section 69 of FOIPPA;

(b) make the section 69 reporting requirements regarding information sharing agreements applicable to all public bodies (this can be done under section 69(7) by the minister responsible for FOIPPA); and

(c) in conjunction with Recommendations 9 and 10, review the utility of section 69 in its present form, noting our view that section 69 needs to be amended to require more complete, transparent, ongoing and effective reporting about the information sharing agreements and data mining activities of all public bodies.

Private sector issues

Recommendation 13

The government of British Columbia and the government of Canada should consider and address the implications of the USA Patriot Act for the security of personal information that is entrusted to private sector custody or control in British Columbia or elsewhere in Canada.

Trends in personal information collection and access for state purposes

Recommendation 14

The Parliamentary review of the Anti-terrorism Act provides an important opportunity for the government of Canada to renew its commitment to ensure that human rights and freedoms are not unnecessarily infringed by national security and

law enforcement measures. As part of this renewed commitment, we recommend that the public be permitted to participate in the review in a meaningful way.

International trade and investment agreements

Recommendation 15

The government of Canada should, in consultation with the provincial and territorial governments, negotiate with foreign trade partners (including members of the World Trade Organization) to ensure that trade agreements and other treaties do not impair the ability of Canadian provinces, territories and the federal government to maintain and enhance personal information protections in accordance with Canadian values.

Other international agreements

Recommendation 16

In moving towards a North American trade, energy, immigration and security zone, the government of Canada should, in consultation with the provincial and territorial governments, advocate to the US and Mexico for comprehensive transnational data protection standards and for multilateral agreements respecting continental control and oversight of transnational information sharing for government purposes, including national security and public safety purposes.