

The USA Patriot Act & Personal Privacy—Implications for Government Contracting

Cyber Security for Government Conference
Canadian Institute
Ottawa
September 28 & 29, 2005

David Loukidelis
Acting Information & Privacy Commissioner for British Columbia

INTRODUCTION

We live in an increasingly seamless world, one in which personal information flits around the world in the ordinary course of business. Our personal data wing their way around the world whenever we use the Internet, email someone or buy something online. But in the last few years especially, our personal information finds its way around the globe through the off-shoring of data processing by businesses seeking to protect their bottom lines and, increasingly, through the government outsourcing of functions traditionally done in-house.

At the same time, we live in a world in which there are different attitudes to privacy, where different values are placed on privacy and privacy is protected to different degrees if at all. The question, then, is how, in an increasingly interconnected world, we can protect our personal information wherever it may be found. What institutions can we possibly create to address data protection in the international era? This is not a new challenge, of course. The 1980 *OECD Guidelines on the Protection of Privacy and*

*Transborder Flows of Data*¹ are only one example of long-standing efforts to address the international dimensions of commerce and its impact on personal privacy. This issue also complicates laudable initiatives such as the APEC Privacy Framework for privacy protection in Asia-Pacific economies, adopted by APEC leaders late last year.²

Where privacy laws do exist, their limits are stretched by developments other than the globalization of data flows. The template for Canada's privacy laws, like those in Europe, is now more than a generation old. New ways of doing business, and providing public services, combine with new technologies to challenge existing laws, the capacity of which to deal with new demands is questioned by some.

The ability of our laws to meet these new demands is put in play by initiatives to outsource public sector services and information processing. And extra-territorial challenges to privacy protection in Canada add complexity to the mix. This paper examines a specific challenge in the context of British Columbia's *Freedom of Information and Protection of Privacy Act* (FIPPA) and offers suggestions for addressing similar risks under Canadian public sector privacy laws similar to FIPPA.³ To a fair

¹ www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

² The APEC Privacy Framework was approved November 20, 2004 by APEC leaders. Work continues on international implementation mechanisms. See the following link:

www.apec.org/apec/news_media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.html.

³ This paper contains general information only regarding the situation in British Columbia under British Columbia law. It is not intended to address the situation in any other jurisdiction. Nor does this paper offer legal or other advice. Readers should seek legal advice in arranging their affairs. The views expressed in this paper do not bind the author or the OIPC and do not fetter the discretion or judgement of the author or the OIPC in relation to any complaint, investigation or inquiry that may be made to or held by the author or the OIPC, as to which an open mind exists.

extent, as well, the suggestions found in this paper will—bearing in mind the author’s focus on British Columbia—be relevant to privacy compliance issues more generally in the context of public sector outsourcing arrangements.

THE USA PATRIOT ACT & PUBLIC SECTOR OUTSOURCING

International challenges to privacy protection came to the fore in 2004 in British Columbia. The British Columbia government’s policy of alternative service delivery, under which private sector companies perform public services that used to be done in-house led to concerns about outsourcing to companies with US links and possible implications under the USA Patriot Act.⁴ Specifically, in early 2004, the British Columbia government made public its intention to outsource the administration of British Columbia’s public health insurance scheme, the Medical Services Plan. Soon after 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 Patriot Act implications for the privacy of British Columbians where personal information is part of an outsourcing arrangement.

One of the Patriot Act’s main objectives was to expand the intelligence gathering and surveillance powers of US law enforcement and national security agencies. It increased

⁴ The formal name of this US federal law is the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001*, Pub. L. No. 107-56, 115 Stat. 272 (2001), referred to below to this Act as the “Patriot Act”. This law came into force October 26, 2001.

US authorities' ability to obtain orders from a secret court—the Foreign Intelligence Surveillance Court—requiring any company under US jurisdiction to hand over information in its control, with stiff penalties for any company that reveals it has been ordered to do so. The Patriot Act also expanded the ability of the FBI to issue on its own—without prior judicial authorization—secret administrative subpoenas compelling organizations to turn over personal information of identified individuals to the FBI.

In light of numerous, ongoing requests for guidance from a variety of quarters, in May 2004, the author announced that the OIPC would conduct a public consultative process to provide general guidance and recommendations to public bodies and the public on two questions relating to the Patriot Act. The goal of this was to assess any Patriot Act privacy implications and recommend practical and effective measures to meet any risks that were identified. These are the two questions the OIPC posed:

1. Does the 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 FIPPA? What measures can be suggested to eliminate or appropriately mitigate privacy risks affecting compliance with FIPPA?

In response to a public invitation for submissions on these questions, the OIPC received more than 500 submissions from across Canada, the US and Europe. We heard from individuals, governments (both domestic and foreign), labour groups, information technology companies and groups, health care providers, library associations, privacy advocacy organizations and privacy commissioners (including the Privacy Commissioner of Canada).

Many of these submissions addressed the questions posed about Patriot Act implications for outsourcing, but a great number of them raised far broader issues. A number of themes ran throughout the submissions. Although they are not directly relevant to this paper's topic, four of them warrant mention because they touch on far wider themes that may affect government activities and programs, including in relation to cyber security:⁵

- Many people clearly fear 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.
- Globalization of the information technology industry, enhanced by free trade and the technical ease of data transfer, produces economic opportunities, but also raises

⁵ Some of these themes are echoed in a recent opinion poll conducted for the Office of the Privacy Commissioner of Canada by EKOS Research Associates, specifically in relation to national security and counter-terrorism laws and powers (a copy of the report on this poll can be found at: http://www.privcom.gc.ca/information/survey/ekos_e.asp).

concerns about national sovereignty and creates privacy challenges for businesses, governments, regulators and the public.

- Many believe that developments in information technology are fuelling the appetite of governments for larger data banks and the mining of personal information for national security and other purposes, while new laws since September 11 are encouraging the private sector to share personal information with government authorities 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 can blur 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, a blurring of roles that could have significant implications for privacy and other civil rights.⁶

Having waded through the roughly 500 submissions, it became clear that the two questions posed about the Patriot Act could not be isolated from these broader and

⁶ There are many examples of this blurring of roles and the legal powers associated with them. In the US, the Patriot Act itself, and policy changes implemented in the wake of 9/11, have—to use the US Department of Justice’s own words—broken down the walls between national security and law enforcement in the US. Closer to home, Customs Act and also amendments to the Aeronautics Act have enabled compulsory collection, without warrant, of personal information in the name of national security, while allowing disclosure and use for ordinary law enforcement purposes.

interrelated themes. These themes all relate to the importance of privacy as a democratic right, to expanding risks for privacy in a more and more interconnected world, and to the risk—and potential impact—of disclosure of personal information to foreign authorities or jurisdictions without there necessarily being any meaningful privacy protection after disclosure abroad. To a significant extent, therefore, the OIPC’s October 2004 report, *Privacy & the USA Patriot Act—Implications for British Columbia Public Sector Outsourcing*,⁷ examined the wider questions arising out of these themes and offered recommendations to address them.

As for the questions about Patriot Act implications for privacy in British Columbia, the Patriot Act report agreed with the general, though not universal, consensus in the submissions that a court order could be made under the Patriot Act to require disclosure to the FBI in the US of personal information located in British Columbia but in the hands of a service provider with links to a corporation under the jurisdiction of the US courts.⁸

This conclusion was reached after extensive analysis of 50 years of US case law.⁹ Specifically, we concluded that the Foreign Intelligence Surveillance Court technically

⁷ www.oipc.bc.ca/sector_public/usa_patriot_act/pdfs/report/privacy-final.pdf (referred to below at the “Patriot Act report”).

⁸ It bears emphasis that the conclusion was solely that surreptitious access to personal information located *inside* Canada might occur under US processes, not that access to personal information would occur if it were located *outside* Canada. Information located outside Canada will all but inevitably be subject to foreign law.

⁹ For at least 50 years, US courts have, under a wide variety of laws, quite routinely issued orders, warrants or subpoenas that are extra-territorially effective, *i.e.*, process issued in the US but compelling compliance outside the US. Our research revealed no analogous practices on the part of the courts of European or Canadian courts.

could, the *Foreign Intelligence Surveillance Act* as amended by the Patriot Act, issue an order to a person subject to the court's jurisdiction compelling that person to obtain records or other things located outside the US court but under the control of that person, and deliver them to US authorities in the US. This would involve the US court's order reaching beyond the US and having a direct extraterritorial effect, without the intervention of Canadian law or constitutional principles, much less Canadian courts or other authorities.¹⁰

As for the risk that such an order might be issued, the Patriot Act report concluded—again, after careful study and analysis—that there is a reasonable possibility such an order could be made and that, contrary to several submissions, there is no reason to believe that other (existing) mechanisms for access to personal information would be used instead. It concluded that the risk of Patriot Act access was not, as some had contended, “incremental” or “vanishingly small” on any of the grounds on which these contentions were based.¹¹ None of these arguments overcame our conclusion, ultimately, that the risk of Patriot Act access required legislative and other meaningful responses in British Columbia if we are to ensure that our values and laws apply in Canada to protect our information.

¹⁰ We also concluded that the FBI could, by issuing a national security letter to itself, compel production of personal information in secret and that US courts would, as a default position, enforce compliance with such an instrument.

¹¹ These grounds ranged from the argument that US authorities would never care about personal information of British Columbia residents to the contention that other avenues for access exist that are more likely to be used. (The Canada-US Mutual Legal Assistance Treaty was mentioned in several submissions on this last point, but MLAT applies only to criminal matters and not national security intelligence gathering.)

The analysis and conclusions in the OIPC's report have been criticized by some in Canada and the US. Representatives of the Information Technology Association of Canada (ITAC), for example, have publicly argued that the report's conclusions are flawed.¹² The report speaks for itself. Further, public bodies in British Columbia must comply with the requirements of Bill 73 and otherwise take measures to meet their privacy obligations under British Columbia law.

MITIGATING PRIVACY RISKS IN OUTSOURCING

The OIPC did not recommend a ban on outsourcing of government services to private sector contractors. The Patriot Act report readily concluded that, as many submissions recognized, an outright ban on outsourcing would be neither necessary nor practicable. Nor did it recommend that corporations with links to the US sufficient to place them at risk of a Patriot Act order should be discriminated against in competing for outsourcing work.¹³

The Patriot Act report recommended, instead, that British Columbia's *Freedom of Information and Protection of Privacy Act* (FIPPA)—which governs the privacy practices of public bodies in the province—should be amended to prohibit disclosure of personal

¹² Also see ITAC's July 2005 position paper on the USA Patriot Act, *The USA Patriot Act & the Privacy of Canadians* (referred to below as the "ITAC paper"). The ITAC paper comes up below in the later discussion of its recommendations for risk assessment and risk mitigation.

¹³ The report does not, contrary to claims later made by others, single out companies incorporated in the US. It may be that many of the outsourcing service providers ultimately have US parents, but the report's analysis extends to any company, wherever incorporated (including Canada), with sufficient business presence in or ties to the US to subject them to the personal jurisdiction of US courts and authorities.

information located in British Columbia in response to a foreign court order, warrant or subpoena.¹⁴ The OIPC concluded that the recommendation for a statutory ‘blocking measure’ promised to be effective because of clear indications in US court decisions that an American court may well give effect to a legislative prohibition in and, as a result, not order production of personal information from abroad in the first place.¹⁵

For present purposes, the most significant of the Patriot Act report’s 16 recommendations is that contractual arrangements should be implemented in any British Columbia outsourcing initiative involving personal information to ensure that persons subject to US court jurisdiction do not have legal or practical control over personal information located in British Columbia. The British Columbia government promised to follow this recommendation at the provincial level and has since said that the several outsourcing, or “alternative service delivery”, arrangements into which it has entered to date contain contractual protections for personal information.

¹⁴ This prohibition would apply regardless of whether the order were issued by a US court, a British court or a Chinese court. The occasion for the report’s analysis and recommendations was the Patriot Act, but other foreign laws could conceivably present similar concerns. An example of a blocking statute is already on the federal statute books, the *Foreign Extra-territorial Measures Act* (Canada), which blocks operation in Canada of the Helms-Burton Act, which targets foreigners who do business in Cuba.

¹⁵ This same recommendation was made in a number of submissions. It was also endorsed—as was the rest of the report—by the OIPC’s special counsel, the Hon. Gerard La Forest, a retired justice of the Supreme Court of Canada and leading privacy expert and international lawyer. Consistent with this recommendation, but before the OIPC’s report was released, the British Columbia government introduced and brought into force amendments to FIPPA to address Patriot Act risks. See the *Freedom of Information and Protection of Privacy Act Amendment Act 2004*, S.B.C. 2004, c. 64 (referred to below as “Bill 73”). This paper does not suggest that other governments in Canada should enact legislation or otherwise act to address privacy risks. Each jurisdiction must undertake its own assessment of the nature and extent of any Patriot Act privacy risks in the context of its personal information-related outsourcing initiatives and, in that light, decide what if any statutory mitigating measures are desirable.

It should be kept in mind that the contractual measures discussed below will not be relevant or applicable in each and every case. The circumstances of each outsourcing will dictate what measures should be taken and what form they should have. Nor is the following discussion exhaustive, since further measures may be necessary or desirable in particular cases.

A place for risk assessment?

Some comment about risk assessment is in order before discussing what privacy protections could be built into outsourcing contracts. The Bill 73 amendments prohibit disclosure of personal information by public bodies *and* service providers in response to foreign compulsion. They also significantly limit the ability of public bodies in British Columbia to permit personal information, of any kind or sensitivity, to be located or accessed from outside Canada. This latter prohibition has been the focus of concern for ITAC and others, who are undoubtedly concerned that the globalization of outsourcing services, among other things, will be hindered by barriers to trans-border data flows.

It has been suggested by some that, in order to limit interference with efficient outsourcing of services, mitigating measures relating to Patriot Act concerns should proceed only after a risk assessment. The ITAC paper, for example, argues for a “pragmatic framework for identifying and responding to any identified privacy risks”

and contends that the response to identified privacy risks must be “proportionate”.¹⁶

ITAC then suggests the following criteria for identifying risks:¹⁷

Identifying actual risks to privacy requires an assessment of the following factors:

- the amount of the information in the custody of or accessible to the service provider;
- the amount of control by the service provider over the information;
- the sensitivity of the information;
- the usefulness of the information to US law enforcement;
- the ability of US law enforcement to target specific information; and
- the likelihood of US law enforcement obtaining the information through Canadian authorities.¹⁸

ITAC also contends that risk assessment will disclose that “only in the rarest of cases” will the risk “justify geographic restrictions, over and above typical safeguards to protect the confidentiality and security of information regardless of location.”¹⁹

Public statements by government officials indicate that risk assessment is part of the British Columbia government’s approach to Patriot Act issues. This is clear from their

¹⁶ ITAC paper, p. 9.

¹⁷ ITAC paper, p. 9.

¹⁸ The ability of a public body to apply the last three criteria is open to doubt depending on the circumstances. For example, a public body could determine the “usefulness of the information to US law enforcement” in many cases. But this assessment will in others be at best speculative—how is a public body to know what will be useful to “US law enforcement”? Nor is it clear how, in many cases, a public body could realistically assess the “likelihood of US law enforcement obtaining the information through Canadian authorities”. Still, the ITAC criteria will help agencies assess privacy risks in many cases.

¹⁹ ITAC paper, p. 9. ITAC’s observation reflects the difficult but necessary balancing act between globalization and privacy protection alluded to in the introduction to this paper and in the Patriot Act report.

mention of privacy impact assessments (“PIA”) being used as a risk assessment tool.

PIAs may be useful in this context for at least two important reasons:²⁰

- A threshold, and obvious, issue that a PIA can address is whether personal information²¹ is involved at all in a proposed outsourcing. If it is not, then no privacy risks or obligations arise.
- A related point is that a PIA might identify personal information, but also reveal an opportunity to manipulate the personal information, for the purposes of the outsourcing arrangement, so that it is no longer personal information in the service provider’s hands and is therefore not subject to the ordinary legal requirements. (A public body would, of course, have to be careful to ensure that the information is, assessed objectively and reasonably, truly no longer personal information.)²²

As regards risk assessment, the author acknowledges that a Canadian government might decide that contractual mitigating measures are needed only where a service provider has custody or control of material amounts of personal information or the outsourced

²⁰ A sample PIA tool can be found here: http://www.oipc.bc.ca/sector_public/resources/pia.htm. The utility of the PIA process in addressing security risks in outsourcing is acknowledged in the OIPC’s Guideline 01-02, *Guidelines for Data Services Contracts* (first published in 2001 and referred to below as the “OIPC outsourcing guidelines”): www.oipc.bc.ca/advice/Guidelines-Data_services.pdf. This paper draws on the OIPC outsourcing guidelines in a number of respects.

²¹ FIPPA defines “personal information” as “recorded information about an identifiable individual”. This definition is very similar, and in some cases identical, to definitions in other Canadian privacy laws. The definition makes it clear that business and other organizations have no privacy rights under FIPPA. Nor will non-identifiable information be subject to FIPPA.

²² The de-identification assessment and process would have to address the risk of re-identification, including where the information may be combined with information available to the service provider or others to become, again, “personal information”.

personal information is sensitive in nature (*e.g.*, personal health information). If, for example, a service provider will only possess or be using name and address information that can be found, in most cases, in public directories, the government organization may decide that little if any privacy risks are involved. The outsourcing contract may in such a case do little more than require the service provider to not use or disclose the personal information other than for contract purposes or as required by law. Such an approach would be consistent with ITAC's argument for proportionality, which depends on a context-specific approach to privacy protections. The ITAC paper puts it this way (p. 9):

...safeguards which may be appropriate when a public body hires a service provider to store and maintain an entire database of personal information will often be much more restrictive (and costly) than would be appropriate if the service provider would have only incidental access to data stored and maintained by the public body.

The following discussion outlines some contractual measures that could be considered in order to address risks of access in Canada to personal information through operation of foreign law.

Contractual measures to address control over records

Where contractual measures are considered necessary, these measures should address control over records. Our review of US law told us that, in considering whether to order or enforce disclosure in the first instance, a US court must be satisfied that the person or corporation under the court's jurisdiction has legal or practical control over the foreign records, *i.e.*, the ability to obtain them. Because there is little sense or justice in ordering

someone to obtain records over which it has no control, US courts will generally refrain from even making such an order or enforcing it.²³

Our research also told us that the tests for what constitutes “control” over records vary. Some courts have taken the view that if a US-located corporation owns a foreign corporation, the US corporation is deemed to control the foreign company’s records. Other courts require more. They look for a legal right of some kind, or sometimes merely a practical ability, to obtain the foreign records. Ownership of the records or contents may be one factor—if someone owns records or has a legal right to use them, control seems pretty clear. The nature of the records may be another factor. If the records are ordinary-course business records of the foreign company and it is either part of the same corporate family as the corporation that the order would be issued against, or is jointly working as a partner or co-venturer with that corporation on a business or project, control may be easier to find.²⁴

All of this is to say that the concept of control over foreign records is important. The Patriot Act report, therefore, concluded that contractual measures can and should be put in place in outsourcing initiatives in order to decrease the chance that control over records exists as just described. This is not to say that it is possible to, by contract, guarantee that a court will find there is no control of record—one cannot contract out of the law—but contractual clauses may be persuasive to the court, notably where the

²³ See Patriot Act report, pp. 118-119.

²⁴ See Patriot Act report, pp. 118-120.

records are the government organization's and not business records of the service provider.

Accordingly, the outsourcing contract should provide that the contractor has no control over the records or their contents. The contract should specify that:

- the service provider has no legal right to the records (including ownership of their contents);
- that the contractor only possesses the records and information to do its work;
and
- that its possession of the records is incidental to the main objective of the service arrangement.

The contract should also state that the public body is only transferring *physical custody* of personal information to the contractor, not *control* of that information, and that authority over personal information use, disclosure, access, destruction and integrity remains with the public body. The contract also should state how the public body is able to exercise its control (*e.g.*, by giving a notice to the contractor that requires the contractor to do what is specified in the notice).

Some benefit might also be gained, wherever they are practicable, from contract clauses that require the service provider to keep the personal information separate from its other

data holdings.²⁵ If personal information is mixed in with the service provider's own data or business information, a court might be more inclined to conclude that the personal information is in the service provider's control. Where they are considered appropriate, such contract clauses could require the contractor to securely segregate the personal information from information of others (including the contractor), including by installing access barriers to prevent information elements from being associated (including compared or linked, based on similar characteristics) with other information, including by:

- having separate storage facilities for the public body's personal information;
- requiring senior contractor management (or even public body) authorization before a person is granted access to computers or media containing personal information or to facilities where such computers or media are located;
- encrypting personal information to prevent unauthorized disclosure or access;
and
- implementing best security practices to authenticate users (such as passwords and public key encryption/smart card/biometric technology where practicable) and otherwise prevent unauthorized access.²⁶

²⁵ This issue is also discussed below in relation to security and compliance measures.

²⁶ These recommendations will also be typical of many if not all outsourcing contracts quite apart from Patriot Act issues. See section 3.2 of the OIPC outsourcing guidelines for other security-related tips.

Obligation for service provider to comply with domestic privacy law

Bill 73 amended FIPPA so that many of its relevant provisions respecting disclosure under foreign law apply directly to service providers. Further, almost any outsourcing contract will, quite apart from Patriot Act issues, require a service provider to comply with all applicable laws, which obviously would encompass the jurisdiction's privacy legislation.

Nonetheless, a contractual risk-mitigation framework could include clauses creating and developing an obligation on the service provider's part to use and disclose personal information that it obtains under the contract only as permitted by law, only for the purpose of performing the services²⁷ or as otherwise permitted under the contract.²⁸

The contract could also require the service provider to comply with the relevant privacy law as if the service provider were the public body. This would implicitly include the FIPPA prohibition against disclosure of personal information under foreign laws or processes, but consideration could be given to expressly stating this in the contract.

The point, of course, is to give the public body direct contractual rights and remedies if the service provider wrongfully uses or discloses personal information.

²⁷ Again, such a clause will in any case be a typical provision in such contracts, quite apart from Patriot Act or similar risks, in order to adequately deal with ordinary privacy compliance purposes. See, for example, section 3.1 of the OIPC outsourcing guidelines.

²⁸ Other permitted disclosures or uses might include cases where a service provider has to allow its subcontractors (ideally permitted only with the public body's prior authorization) to have access to the personal information to perform their sub-contract. Another example might be access to personal information for audit purposes. Permitted access to third parties should be conditioned on confidentiality agreements between the service provider and third parties. See sections 3.1.5 and 3.1.6 of the OIPC outsourcing guidelines.

Consideration should be given to a clause requiring the contractor to immediately notify the public body if any attempt is made to compel disclosure of personal information under foreign law (and perhaps also domestic law, for general privacy protection reasons, where particularly sensitive personal information is involved, *e.g.*, sensitive mental health information about a child in state care). Again, Bill 73 amendments have, in British Columbia, directly placed a duty to blow the whistle in this way, but contract clauses to mirror this place more control in the public body's hands to directly sanction failure to comply.

The contract could also require the service provider to either take the lead, or co-operate with the public body, in litigating any attempt to gain access other than under Canadian laws. It could include a prohibition against compliance with foreign law unless the public body is first notified and, ideally, has had a reasonable opportunity to initiate legal proceedings to contest the requirement.

Service provider strategy for privacy compliance

Another obvious but critical component of a contractual privacy compliance framework is an obligation for the service provider to create and implement a strategy or plan for privacy compliance. As with many of the above suggestions, this is desirable from the perspective of privacy compliance generally—it is by no means merely a Patriot Act

issue. Elements of a contractor privacy compliance strategy or plan are, for example, found throughout the OIPC outsourcing guidelines.²⁹

Among other things, the strategy or plan should specifically stipulate who is responsible for Patriot Act and other privacy compliance issues, lay out processes for identifying and promptly remedying privacy breaches and specify what steps are to be taken and by whom in reporting to the public body (and applicable authorities) any breach of privacy (including a Patriot Act breach).

Of course, the service provider should be required to have employees sign agreements to abide by contractual and statutory privacy requirements as a condition of employment, subject to discipline for breach.³⁰ Another component of a compliance plan should be employee education, with the contractor being required to educate employees on hiring, and periodically after that, about privacy compliance responsibilities and roles.³¹ (This should not, ideally, be seen to absolve the contractor of any liability for employee negligence or wrongdoing—the service provider should be on the hook for both intentional and inadvertent breaches.)³²

²⁹ See, for example, sections 3.2 and 3.3.

³⁰ See section 3.3.2 of the OIPC outsourcing guidelines.

³¹ See section 3.4.2 of the OIPC outsourcing guidelines.

³² See section 3.3.2 of the OIPC outsourcing guidelines.

The service provider should be required, as part of its compliance plan, to create and implement a security policy. The policy could, for example, require the contractor to:³³

- (a) take a physical inventory, at least annually, of all records containing personal information, to identify any losses;
- (b) ensure that records are not removed from storage premises without appropriate written authorization;
- (c) use physically secure areas for the storage of records and restrict access to authorized personnel;
- (d) ensure that access to documentation about computer systems that contain personal information is restricted to authorized personnel;
- (e) ensure that users of a system or network that processes personal information are uniquely identified and that, before a user is given access to the system or personal information, their identification is authenticated each time;
- (f) implement procedures for *identification* and *authentication*, which include:
 - (i) controls for the issue, change, cancellation and audit-processing of user identifiers and authentication mechanisms;
 - (ii) ensuring that authentication codes or passwords:
 - (A) are generated, controlled and distributed so as to maintain the confidentiality and availability of the authentication code;

³³ These are taken from the OIPC outsourcing guidelines, section 3.2.

- (B) are known only to the authorized user of the account;
 - (C) are pseudo-random in nature or vetted through a verification technique designed to counter triviality and repetition;
 - (D) are no fewer than 6 characters in length;
 - (E) are one-way encrypted;
 - (F) are excluded from unprotected automatic log-on processes; and
 - (G) are changed at irregular and frequent intervals at least semiannually;
- (g) maintain and implement formal procedures for terminated employees who have access to personal information, with prompts to ensure revocation or retrieval of identity badges, keys, passwords and access rights;
- (h) position system display units and hardcopy documents, or equip them with protective material, so that any personal information being displayed or processed cannot be viewed by unauthorized persons;
- (i) implement automated or manual controls to prevent unauthorized copying, transmission or printing of personal information;
- (j) design and implement a public body-approved automated, always-on auditing system, that is available to the public body for monitoring access to and the use of personal information in the custody of, or managed by, the contractor;

- (k) ensure that, bearing in mind the OIPC's *Guidelines for Audits of Automated Personal Information* OIPC Guideline 01-01,³⁴ the audit system referred to in (j) creates audit trails that automatically:
- (i) record the identity of anyone who accesses, views, alters, deletes or uses a record containing personal information for any purpose, or attempts to do any of those things, and records the date and time of any such actions; and
 - (ii) flag accesses, or access attempts, that fall outside of set criteria (*e.g.*, access outside regular working hours); and
- (l) implement control procedures to ensure the integrity of the personal information being stored, notably its accuracy and completeness.³⁵

Auditing of service provider performance

The Patriot Act report recommended that all public bodies should ensure that they commit, for the duration of all relevant outsourcing contracts, the financial and other resources necessary to actively and diligently monitor contract performance, to meaningfully punish any breaches and to detect and defend against actual or potential disclosure of personal information to a foreign court or other foreign authority. Of course, it is important for public bodies to have the contractual right, and practical ability and commitment, to monitor and enforce such contractual provisions and, more

³⁴ See <http://www.oipc.bc.ca/publications/advice/audit-3.pdf>.

³⁵ Other standards can, of course, be used. The OIPC outsourcing guidelines are, again, dated 2001. See, for example, ISOL IEC 17799 (Revision published June 2005. <http://www.iso.org/iso/en/commcentre/pressreleases/2005/Ref963.html>.)

generally, service provider performance. This is another suggestion that goes beyond Patriot Act compliance issues alone.

As the Patriot Act report recommended, public bodies should not simply rely on contractors to self-report breaches of the law or the service contract. At the very least, the public body should have a contractual right to enter the service provider's business premises (with or without prior notice) and inspect facilities, equipment and records for the purpose of monitoring contract performance. The contract should spell out the consequences of any detected non-compliance (*e.g.*, should the service provider have the right to cure the default, perhaps within a specified time; or are some defaults so serious that cure is not permitted and contract sanctions (including termination) can be triggered by the public body?)

As an alternative, or supplement, to the above suggestion, a public body could require the service provider to submit to regular, and thorough, compliance audits performed by a third-party auditor, selected by the public body (perhaps in agreement with the service provider in some cases). The auditor should have the necessary expertise to perform the audit and to recommend any necessary changes and mitigation measures. Consideration could be given to providing that the contractor must pay for any audit that uncovers material non-compliance with the contract. Further, as the Patriot Act report recommended, all provincial government ministries, at least, should be required to budget properly for the costs of contract-monitoring activities.

Whatever auditing or monitoring approach is adopted, public bodies should, if the contract does not set its own standards, refer to current good or best practices for auditing of security and privacy of personal information. The OIPC's 2001 *Guidelines for Audits of Automated Personal Information Systems*³⁶ may be of assistance, bearing in mind that they are almost four years old and that others resources are readily available.

OTHER PATRIOT ACT REPORT RECOMMENDATIONS

The Patriot Act report went beyond contractual measures, and even the narrow issues relating to the Patriot Act, and made more general recommendations about important national security and law enforcement privacy issues. The rest of this paper discusses some of these more general recommendations in the Patriot Act report in case they are of interest, recognizing that they are beyond the scope of this paper.

First, the Patriot Act report recommended that the British Columbia government—in conjunction with the government of Canada as necessary—should seek assurances from US authorities such as the FBI that they will not seek Patriot Act orders for access to personal information records in BC. Canada and the US are committed to a common security policy and, as part of negotiation of that policy, a good faith commitment on the part of US authorities to not seek such orders is desirable and workable. The Patriot Act report also recommended that, for the longer term, the government of Canada, in consultation with provincial and territorial governments, should advocate to the US and

³⁶ www.oipc.bc.ca/pdfs/public/GuidelinesforAudits.pdf.

Mexico for trans-national data protection standards and multilateral agreements respecting continental control and oversight of trans-national information sharing for government purposes, including national security and public safety.

Second, the Patriot Act report recommended that the British Columbia government should commission a comprehensive, independent, audit of interprovincial, national and transnational information-sharing agreements involving or affecting British Columbia public bodies. The government should, the Patriot Act report recommended, use the audit to identify both existing and planned information sharing activities, with a focus on the kinds of personal information involved, the purpose and authority for sharing information, the public bodies and private sector organizations involved, and conditions in place to control the use and security of the shared information. The audit should be the first step towards meaningful legislative measures to appropriately control information sharing.

In this regard, the Patriot Act report also recommended that the provincial government should ensure that s. 69 of FIPPA, which for almost three years has required ministries to publicly list their information-sharing agreements, is complied with. The provincial government has not done this to date, though it has committed to doing so as soon as practicable.

The third recommendation that merits mention here is that the federal and British Columbia governments each should commission independent audits of information sharing and data mining activities to reduce the risk that personal information will be secretly misused, sometimes with grave and lasting effects for innocent people. These audits should be a first step towards meaningful privacy controls that are independently overseen.

The Patriot Act report made these and other broader recommendations because, as indicated above, the submissions to us forced us to do so. They left no choice but to go beyond privacy risks presented by the Patriot Act. The Patriot Act report was compelled to address risks and challenges raised by other laws, practices and technologies.

These risks and challenges relate to a right that is of fundamental importance to our way of life, both before and after September 11. Privacy is essential to individual autonomy, but it's not just an individual right. Privacy enables us, we've got to remember, to fulfill our roles as community members—privacy is ultimately essential to the health of our democracy.

No right is absolute, of course, and, while opinion polls over the last 30 years have consistently affirmed that Canadians take privacy seriously, Canadians accept—as does the OIPC—the need for trade-offs where necessary, including for national security reasons. There are, however, new challenges in identifying the risks and assessing the

benefits as we move forward with national security and law enforcement initiatives, both legislative and operational. 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 and governments in Canada, like elsewhere, have increasingly been following the lead of corporations in contracting out services formerly done in-house.

Meanwhile, new technologies have created the ability to merge isolated databases into massive banks of information about identifiable individuals, facilitating the sharing and linking of personal information globally. These technologies include data mining—the use of software programs to find patterns that can help predict future results or the behaviour of individuals—a practice that is likely to grow in scope and sophistication, but also perhaps in the risk it presents for personal privacy and freedoms.

At the same time as these new technologies are advancing in scope and sophistication, the US, Canada and other countries have—quite understandably since September 11—increased the intensity and breadth of their foreign and domestic intelligence gathering activities in order to detect and deter terrorist activities. We have to confront and manage, in the context of fear about terrorism, the risk that new technologies may outstrip the ability of society to set clear and continuously relevant rules for their use.

In other words, we have to struggle, on an ongoing basis, against the risk that technology will shape society rather than be controlled by it.

In Canada, unlike some other countries, we are blessed with comprehensive federal and provincial privacy laws—some more modern and effective than others—that require adherence to internationally recognized fair information practices to protect personal information, but in order to keep those laws effective we need to keep up with the times and address new threats as they occur—whether from legislation or new computer technologies—and we need to lead rather than follow.

The response to the process set in motion in British Columbia last year suggests that other jurisdictions are looking to British Columbia to see what we do about the Patriot Act. Our report's 16 recommendations, based on careful consideration of hundreds of thoughtful submissions and detailed analysis of legal and policy options, are designed to provide practical solutions to address Patriot Act implications in British Columbia. The report also continues the dialogue about these matters, a dialogue that will continue for years.

* * *