The following document was received by the DHS Privacy Office on behalf of the DHS Data Privacy and Integrity Advisory Committee.

Trevor Shaw
Director General, Audit and Review Branch
Office of the Privacy Commissioner, Canada
Background Materials:
Privacy and the USA Patriot Act: Implications For British Columbia Public Sector Outsourcing

For more information please visit: www.dhs.gov/privacy or email the DHS Privacy Office: privacy@dhs.gov or the DHS Data Privacy and Integrity Advisory Committee: privacycommittee@dhs.gov.

Additional Contact Information:

Data Privacy and Integrity Advisory Committee
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Telephone: 571-227-3813
Fax: 571-227-4171

Privacy and the USA Patriot Act

Implications for British Columbia Public Sector Outsourcing

October 2004

Information & Privacy Commissioner for British Columbia

Library and Archives Canada Cataloguing in Publication Data

British Columbia. Office of the Information and Privacy Commissioner.

Privacy and the USA Patriot Act:
Implications for British Columbia Public Sector Outsourcing

ISBN 0-7726-5236-8

1. Privacy, Right of - British Columbia. 2. Government information - Access control - British Columbia. 3. Public records - Access control - British Columbia. 4. Terrorism - United States - Prevention. 5. United States. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. I. Title.

JC596.2.C3B74 2004 323.44'8'09711 C2004-960135-0

Contents

PREFACE

This report continues the public dialogue about privacy that was triggered earlier this year by a British Columbia Government and Service Employees' Union (BCGEU) lawsuit aimed at halting the British Columbia government's plan to retain a US-linked contractor to run the province's public health insurance program, the Medical Services Plan. The BCGEU brought to light the concern that has been gradually emerging in other provinces, and indeed other countries, that contractors who possess sensitive personal information could be secretly compelled under the USA Patriot Act to turn it over to US authorities. This report's scope and detail speak to the breadth of the issues that figure in that debate, which has often been intense and passionate.

Our review of the USA Patriot Act and the outsourcing of public services in British Columbia has caused us to confront the most challenging and important privacy issues my office has faced since I took this job just over five years ago. The September 11, 2001, terrorist attacks triggered a dramatic shift in public policy in Canada and elsewhere—a policy shift that is likely to continue for the foreseeable future. A central theme of this report is that we cannot wait for historians to tell us whether or how much the shift towards a national security focus has imperilled our hard-won rights and liberties. We have to do our best now, not tomorrow, to ensure that the laws and practices introduced right after September 11 are consistent with our democratic tradition and our civil rights.

This perspective runs through many of the more than 500 submissions we received. Most of them were from individuals deeply concerned about their privacy and often eloquent in expressing their concerns. I am grateful to everyone who took the time to share their thoughts and their often very personal reasons for valuing their privacy so highly.

At the risk of singling out only a few who made submissions, I am grateful to the BCGEU for its commitment to this process and for its thoughtful submission. The BC government also has my thanks for its commitment to this process and for its comprehensive submission. The Honourable Joyce Murray, Minister of Management Services, and the Honourable Geoff Plant, Q.C., Attorney General for British Columbia, deserve particular thanks.

This report is unusual because it examines the impact of foreign law on British Columbia residents living in British Columbia, not abroad. Because the USA Patriot Act is a US law, I felt very strongly that American officials should be asked for their views and extended invitations to the US government. We received submissions from the Federal Bureau of Investigation, which plays a central and critical role in counterterrorism activities in the US, and from the Department of Homeland Security, which has an equally vital role to play in protecting the US against terrorism. I thank them both for sharing their thoughtful perspectives.

My sincere thanks also go to the many civil society groups and private sector organizations from Canada, the US and Europe that took the time to make their views known to us. Their submissions presented us with a broad array of perspectives on some very tough issues and their input was important.

I am also very grateful for the support of a number of Canadian colleagues. I thank Jennifer Stoddart (Privacy Commissioner of Canada), Karen Rose (Information and Privacy Commissioner for Prince Edward Island)

and Bernard Richard (Ombudsman of New Brunswick) for their excellent submissions to us. We also received valuable advice on the report, for which I am sincerely thankful, from Frank Work, Q.C. (Information and Privacy Commissioner for Alberta), Hank Moorlag (Information and Privacy Commissioner for Yukon), Peter Bower (Director, Access & Privacy Division, Office of the Ombudsman for Manitoba) and, again, Jennifer Stoddart. As always, Ann Cavoukian, the Information and Privacy Commissioner of Ontario, was both supportive and encouraging.

From Europe, I sincerely thank Jacob Kohnstamm, President of the Dutch Data Protection Authority, and Attila Peterfalvi, the Hungarian Data Protection Commissioner, for their advice and input. My appreciation also goes to Alex Türk, President of the Commission Nationale de l'Informatique et des Libertés, the French data protection authority, for the interest he and his colleagues have shown in this report.

Closer to home, several people have worked on this report and deserve thanks. I am, first, deeply grateful for the advice of our special counsel, the Honourable Gérard V. La Forest, C.C., Q.C., counsel with the Atlantic Canadian law firm Stewart McKelvey Stirling Scales. His deep knowledge of privacy issues goes back more than thirty years to his work as a member of the government of Canada's Task Force on Privacy and Computers, whose groundbreaking 1972 report remains highly relevant today. As a member of the Supreme Court of Canada, his eloquent judgments laid an enduring foundation for the constitutional protection of Canadians' privacy under the Canadian Charter of Rights and Freedoms. Our report benefited greatly from his wisdom and counsel, especially in relation to privacy under the Charter and the implications of US law for compliance with British Columbia's Freedom of Information and Protection of Privacy Act. I am sincerely grateful to him.

It would be difficult to overstate the contributions to this report of Susan E. Ross, who has been one of our legal advisers and counsel for over a decade. As always, she applied her considerable abilities with tireless and selfless energy and focus in researching a wide array of legal issues and in contributing a very great deal to the writing of this report. I am greatly in her debt.

I am also indebted to David Greer, who was equally tireless and selfless in his significant contribution to the research and writing of this report. David also handled the report's publishing and production arrangements with consummate professionalism, and his calm manner and intelligent humour helped enormously during late nights and early mornings.

I am also indebted, once again, to my colleagues in the Office of the Information and Privacy Commissioner and they have my sincere thanks for their contributions. Special thanks go to Bill Trott and Mary Carlson for their comments on several drafts of the report and to Justine Austin-Olsen for her comments on the draft and her careful accuracy check. I thank Celia Francis for her editorial work and also thank her, Errol Nadeau, Judy Durrance, Barbara Haupthoff, Morag Wilmut, Brenda Guiltner, Elizabeth Keay, James Burrows, Jay Fedorak and Michael Skinner for their insightful advice and comments on the draft report. My thanks go to Maria Dupuis and Kathie Baker for organizing the hundreds of submissions as they came in and for their work on the report's production, with Dan Kerr and Krista Cain also deserving thanks for their relief work in the report's preparation.

Any errors or omissions in this report are, of course, my sole responsibility.

October 20, 2004
Victoria BC

David Loukidelis
Information and Privacy Commissioner for British Columbia

In the Information Age, an increasing amount of personal information is contained in records maintained by Internet Service providers (ISPs), phone companies, cable companies, merchants, bookstores, websites, hotels, landlords, employers and private sector entities. Many private sector entities are beginning to aggregate the information in these records to create extensive digital dossiers.

The data in these digital dossiers increasingly flows from the private sector to the government, particularly for law enforcement use. Law enforcement agencies have long sought personal information about individuals from various third parties to investigate fraud, white-collar crime, drug trafficking, computer crime, child pornography, and other types of criminal activity. In the aftermath of the terrorist attacks of September 11, 2001, the impetus for the government to gather personal information has greatly increased, since such data can be useful to track down terrorists and to profile airline passengers for more thorough searches. Detailed records of an individual's reading materials, purchases, diseases, and website activity enable the government to assemble a profile of an individual's finances, health, psychology, beliefs, politics, interests, and lifestyle. This data can unveil a person's anonymous speech and personal associations.

The increasing amount of personal information flowing to the government poses significant problems with far-reaching social effects. Inadequately constrained government information-gathering can lead to at least three types of harms. First, it can result in the slow creep toward a totalitarian state. Second, it can chill democratic activities and interfere with individual self-determination. Third, it can lead to the danger of harms arising in bureaucratic settings. Individuals, especially in times of crisis, are vulnerable to abuse from government misuse of personal information. Once government entities have collected personal information, there are few regulations of how it can be used and how long it can be kept. The bureaucratic nature of modern law enforcement institutions can enable sweeping searches, the misuse of personal data, improper exercises of discretion, unjustified interrogation and arrests, roundups of disfavored individuals, and discriminatory profiling. These types of harms often do not result from malicious intent or the desire for domination. Justice Brandeis was prescient when he observed that people "are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in the insidious encroachment by men of zeal, well-meaning but without understanding."

Daniel J. Solove[1]

[1] Daniel J. Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy", (2002) 75 S. Cal. L. Rev. 1083

List of Abbreviations

ASD	alternative service delivery
BCGEU	British Columbia Government & Service Employees' Union
CAPPS	Computer Assisted Passenger Prescreening System (US)
CSE	Communications Security Establishment (Canada)
CSIS	Canadian Security Intelligence Service
DHS	Department of Homeland Security (US)
EU	European Union
FISA	Foreign Intelligence Surveillance Act (US)
FIS Court	Foreign Intelligence Surveillance Court (US)
GAO	Government Accountability Office (US)
GATT	General Agreement on Tariffs and Trade
GATS	General Agreement on Trade in Services
FOIPPA	Freedom of Information and Protection of Privacy Act (BC)
HIV	human immunodeficiency virus
IPC	Information and Privacy Commissioner for British Columbia
ITAC	Information Technology Association of Canada
MLACMA	Mutual Legal Assistance in Criminal Matters Act (Canada)
MLAT	Mutual Legal Assistance Treaty (Canada-US)
NAFTA	North American Free Trade Agreement
OECD	Organization for Economic Co-operation and Development
OIA	Office of International Affairs, Department of Justice (US)
OIPC	Office of the Information and Privacy Commissioner (BC)
PIA	privacy impact assessment
PIPA	Personal Information Protection Act (BC)
PIPEDA	Personal Information Protection and Electronic Documents Act (Canada)
PNR	Passenger Name Registry
USA Patriot Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001
WTO	World Trade Organization

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.

1 WHY AND HOW WE PREPARED THIS REPORT

Interest in the USA Patriot Act

The USA Patriot Act is a US federal law. Enacted in quick response to the September 11, 2001, terrorist attacks in the US, its name stands for the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001.[1] Its effect was to amend and extend a number of US laws and rules dealing with intelligence and counter-intelligence activities, information sharing and terrorism.

Earlier this year, 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 of section 215 of the USA Patriot Act for the privacy of British Columbians. These requests for guidance related to initiatives for outsourcing government functions to US companies or their Canadian subsidiaries. Section 215 concerns secret orders that may be issued by the US Foreign Intelligence Surveillance Court to enable the FBI to obtain access to "any tangible thing" for foreign intelligence purposes or to protect against international terrorism or clandestine intelligence activities.

Section 215 of the USA Patriot Act amended section 501 (and two other sections) of the US Foreign Intelligence Surveillance Act (FISA).[2] The orders that are the main focus of this report are therefore actually issued under FISA, not the USA Patriot Act. Public discussion and the submissions we received have nonetheless generally referred to section 215 of the USA Patriot Act as the relevant statutory foundation for these orders. In this report, we refer to these orders with reference to section 215 of the USA Patriot Act or simply as 'FISA orders'.[3]

Interest in British Columbia in the privacy implications of the USA Patriot Act was triggered by the widely reported launch of a lawsuit in the British Columbia Supreme Court[4] 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

1 USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

2 FISA has been officially codified in Title 50 of the United States Code. Section 501 of FISA is 50 USC §1861 and is reproduced in Chapter 6 of this report.

3 This report also refers to US administrative orders called national security letters, which require an organization to disclose information about its customers. The authority to issue national security letters is found in various US statutes and was amended by section 505 of the USA Patriot Act, which is discussed in Chapter 6 of this report.

4 British Columbia Government & Service Employees' Union (petitioner) v. The Minister of Health Services and The Medical Services Commission (respondents) B.C.S.C., Victoria Registry No. 04-0879. Copies of the BCGEU petition and supporting affidavits are at: www.bcgeu.ca.

the proposed outsourcing would contravene British Columbia's Freedom of Information and Protection of Privacy Act (FOIPPA)[5] by making the personal health information of British Columbians accessible to US authorities under section 215 of the USA Patriot Act.

Mandate of the Information and Privacy Commissioner

The OIPC is an independent agency under the direction of the Information and Privacy Commissioner. Its responsibilities include monitoring the administration of FOIPPA and enforcing compliance with the Act. FOIPPA protects the privacy rights of British Columbians in their dealings with a wide variety of public bodies, including ministries of the provincial government. It does this by restricting the collection, use and disclosure of personal information by public bodies and by requiring personal information in the hands of public bodies to be protected by reasonable security arrangements. Personal information, defined in FOIPPA as "recorded information about an identifiable individual", includes not only basic identifying details (such as name, address, phone number, ID numbers, blood or other body tissue type), but also information related to a person's life history (such as medical or educational information, employment information, political beliefs or religious associations).

Request for Submissions

The Information and Privacy Commissioner decided to respond to widespread public interest and concern by initiating a short-term and open process for assessing possible implications of the USA Patriot Act for compliance with FOIPPA. In May 2004, he published a Request for Submissions, framed around these 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?[6]

The Information and Privacy Commissioner's objective was to elicit the views of governments, members of the public, businesses, labour organizations and other interest groups and then, in a short space of time and following as open a process as possible, issue an advisory report that would be a point of departure for further discussion and action.

This report is the result. It offers such reasoned and practical commentary and solutions as we have been able to identify, within a limited framework, respecting section 215 of the USA Patriot Act and public sector outsourcing initiatives generally in British Columbia.

Two features of the report require special emphasis.

This report is not binding and does not determine rights. It pursues the objective of interpreting and discussing the implications of FOIPPA, other relevant Canadian laws and legal mechanisms and relevant US laws and legal mechanisms. The process was not amenable to considering or making findings about

5 Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165.

6 The Appendix to this report lists the governments, government agencies, organizations and academics that made submissions. These submissions will remain posted on our website for 12 months following the issuance of this report.

specific situations and fact patterns and this report does not do that.

Many submissions were critical of the impact of the USA Patriot Act on civil liberties in the US, but this report is not a judgment on the wisdom of laws in the US. It is up to American lawmakers to enact laws that address circumstances in the US and for Americans to decide whether or not those laws are appropriate. This report assesses the implications of the USA Patriot Act in the context of compliance with FOIPPA when British Columbia public bodies enter into outsourcing arrangements with US-linked service providers, including US companies and their Canadian subsidiaries—a matter of direct interest and concern to British Columbians and the Information and Privacy Commissioner.

Responses to the Request for Submissions

The Request for Submissions generated over 500 written responses. While most individuals who made submissions live in British Columbia, we heard from governments, organizations and individuals from across Canada and from the US and Europe. The responses covered a range of views about whether outsourcing to a British Columbian or Canadian private service provider with US links poses a risk of disclosure under the USA Patriot Act that contravenes FOIPPA and, if so, whether the nature or magnitide of the risk is a concern. Many submissions were brief, but a significant number provided comprehensive analyses of the questions posed and of wider, yet intertwined, issues.

The intensity and complexity of the submissions were remarkable. Clearly, the issues struck sensitive nerves. But why so much interest from so many people?

With the collapse of many trade barriers and the explosion of information technology, the outsourcing of functions involving information management has become a significant factor in the global economy, with a worldwide impact on the way businesses and governments operate, handle information and deliver services. Information technology has at the same time also made it more and more possible, and easier, for businesses and governments to collect and organize information about people. The importance of respecting the privacy of personal information resonates in the submissions, including those from outsource service providers, but raises the issue of how much privacy counts in an age of global data flows and national security imperatives.

The prospect of another country's intelligence and anti-terrorism legislation being applied to personal information entrusted to public bodies in British Columbia elicited strong reactions. The possibility of this occurring crosses a boundary for many people in terms of both personal privacy and national identity. It makes them really consider the value of their personal privacy and democratic traditions in relation to the easy movement of personal information around the globe. It also makes them question whether values relating to personal privacy and national identity, among others, are merely obstacles that get in the way of economic efficiencies, including efficient outsourcing, or whether they are benefits of a civil and democratic society that must not be compromised. We are also driven to ask, in any case, what options are available regarding this issue.

The following commentary in the submission of Jennifer Stoddart, the Privacy Commissioner of Canada, eloquently captures the connections between outsourcing and broader issues relating to globalization and privacy:

> The concerns raised about the impact of the *USA Patriot Act* on the privacy of personal information about Canadians are really part of a much broader issue — the extent to which Canada and other countries share personal information about their citizens with each

> other, and the extent to which information that has been transferred abroad for commercial purposes may be accessible to foreign governments. The enactment of the *USA Patriot Act* may simply have served as the catalyst that brought these issues to the fore. In Canada, citizens increasingly recognize the vital importance of personal information management for good government and sound corporate practices….
>
> No one seriously questions that governments and private sector organizations must collect, use and disclose personal information to do business, run programs and ensure adequate public security. However, Canadians are increasingly concerned about the extent to which their governments claim to require personal information about individuals to fight crime and protect national security. Canadians are also concerned about how and when personal information about them is shared with foreign governments and agencies, including police and security agencies. Their concern centers on the balance between law enforcement and public security on the one hand, and respect for fundamental human rights such as privacy on the other.
>
> The transfer of personal information across borders is a fact of contemporary governance — a product of "globalized" economies, interdependent private and public sectors and increased international cooperation on criminal justice and public security issues. The flow of personal information transcends national and organization boundaries…[7]

Many other submissions, including that of the British Columbia government, also touch on and explore these broader issues. Because of this, we concluded that, in order to respect the thrust of the submissions to us and the results of our own research into the issues, we needed to examine the implications of section 215 of the USA Patriot Act within the larger context of globalization, national security, law enforcement and privacy.

Structure of This Report

The report is organized into chapters that canvass the necessarily wider landscape, analyze the issues raised, answer the questions in the Request for Submissions and offer options for action:

- Chapter 2 provides a thematic summary of the submissions we received.
- Chapters 3 and 4 provide an overview of privacy laws in Canada, Europe and the US and of the privacy protection challenges created by trends in outsourcing and information technology.
- Chapter 5 discusses the privacy implications of increasing levels of state surveillance for national security purposes following the attacks of September 11, 2001.
- Chapters 6 and 7 describe section 215 of the USA Patriot Act in the context of legislative developments in the US and Canada respecting foreign intelligence gathering and international terrorism and the implications of those developments for privacy protection.
- Chapters 8 to 10 analyze privacy protections under the Canadian Charter of Rights and Freedoms, the responsibilities of public bodies under FOIPPA for protecting personal information, how the FOIPPA framework would relate to an order of the US Foreign Intelligence Surveillance Court to enable US authorities to obtain access to personal information in British Columbia and whether a US court could or would make such an order.
- Chapter 11 discusses strategies to mitigate against the risk of disclosure of British Columbians' personal information to US authorities and presents our conclusions and recommendations.

7 Submission of the Privacy Commissioner of Canada (12 August 2004) pp.2-3.

2 WHAT WE HEARD

As noted in Chapter 1, the hundreds of submissions we received reflect a remarkable intensity and complexity. The importance of protecting privacy consistently resonates throughout the submissions from individual citizens, businesses, governments, labour groups and others. It is not surprising, therefore, that the possibility that US authorities might be able to gain access to personal information through outsourcing of services provoked very strong reactions, particularly in relation to health information.

Other themes clearly emerged from the submissions, however, and these have irresistibly shaped our approach to the questions posed in the Request for Submissions and to this report as a whole. Building on these themes, this chapter sets the stage for our treatment of the issues in the following chapters.

Privacy Is Important

In consistently endorsing the fundamental importance of privacy, the submissions raised questions about why we value privacy individually and as a community and about who we are as a civil society. Our treatment of compliance issues under BC's Freedom of Information and Protection of Privacy Act (FOIPPA) can, in this light, be meaningful only if we first address fundamental questions around privacy. What do we mean by 'privacy'? Why do individuals value it and why do we protect it legally? How is privacy protected in modern democracies?

We believe that discussing these basic questions is a necessary starting point for any attempt to assess USA Patriot Act implications for privacy compliance in BC. This is particularly true because, among other things, sensitive information can be implicated in outsourcing initiatives and disclosure of sensitive information such as health information can have serious consequences for individuals. To give only one example, the BC Medical Association, which represents BC physicians, believes the possibility of a breach of confidentiality can pose a threat to the physical and psychological well-being of individuals:

> Without confidence that privacy will be maintained, patients may refrain from disclosing critical information; may be reluctant to provide their consent to use their personal health information for research purposes; may lie about their health status or simply not seek treatment. A 1999 survey by the CMA found that 11% of the public held back information from a health care provider because they were concerned about whom it would be shared with, or for what purposes it would be used. A 1999 Ipsos-Reid survey also found that 76% of British Columbians believed it is very important that medical information be kept private.[1]

The BC Freedom of Information and Privacy Association (FIPA), BC Coalition of People with

1 Submission of the British Columbia Medical Association (12 July 2004) p. 1.

Disabilities and BC Persons With AIDS Society were all concerned that transfer of health-related information increases the risk of discrimination. As FIPA and the BC Coalition of People with Disabilities put it:

> People with disabilities, for example, are all too familiar with the stigma attached to many kinds of disability and the discrimination to which access to their medical information can give rise. Barriers to employment, housing, and travel are commonplace. Already people living with HIV/AIDS are barred from entering the United States. Questions of privacy and confidentiality are not abstractions for people with disabilities; they are concrete daily realities. The possibility, however slight, of their medical records being made available to a foreign agency without their knowledge or consent, and perhaps being further disclosed, is chilling.[2]

While privacy is a value widely appreciated in Canada, the US and Europe, how that value is translated into constitutional or legislative protections varies from place to place. The implications of US law—the USA Patriot Act—for privacy compliance in BC can only be assessed against the backdrop of the privacy rights and protections adopted at home and by our neighbours. There are also more direct, practical, reasons for our discussion of privacy protection elsewhere. By assessing legislative schemes found elsewhere we have learned lessons that shape the recommendations we make later in this report. We therefore provide a comparative analysis of various countries' laws on privacy protection in Chapter 3 and note differences between the US and Canadian approaches—differences that have a bearing on British Columbians' concerns about the treatment of personal information that crosses national borders.

Data Flows Around the Globe

Another important theme in the submissions is the global nature of data flows in the electronic age. Many of the submissions speak to the increasingly seamless world in which we live, with personal information flowing around the world like the jet stream. Submissions speak to both the benefits and risks of this wave of data globalization, with a number of them interlacing globalization of data with concerns around national sovereignty and control over privacy standards.

As the Information Technology Alliance of Canada (ITAC) points out, the information technology industry knows no borders and the knowledge trade has been described as 'The Third Wave of Globalization'. Bits and bytes have erased the need to fuss with limitations once imposed by geography and, to a large extent, time. Free trade has swept aside many regulatory barriers to data transfers. Cultural and political boundaries have little relevance to business and, in some respect, governments, except as challenges to be met.

The globalization of data flows creates privacy challenges for businesses, governments, regulators and the public. The possibility that outsourcing of services could involve internationally connected information systems and the storage of data outside Canada relates directly to the USA Patriot Act and its potential impact on the ability of the British Columbia government to protect privacy rights. For this reason, in Chapter 4 we sketch the broader trends in transborder data flows, particularly in the context of outsourcing of services in various parts of Canada.

Data Banks and Data Mining

Another current running through a number of submissions stems from awareness that governments around the world—including those in Canada and the US—have an increasing appetite for personal

2 Joint submission of the BC Freedom of Information and Privacy Association and BC Coalition of People with Disabilities (6 August 2004) p. 12.

information and for exploiting it for various purposes, including national security and law enforcement. The submissions also recognize that developments in information technology are making it easier for governments to amass, share, store and manipulate personal information in increasingly sophisticated ways.

Governments in the US, Canada and Europe are planning or implementing national security programs involving the collection of data from public and private sources. Canadian law has recently been amended to facilitate the private sector's secret collection and disclosure of personal information for national security purposes.

Discussion of USA Patriot Act implications for privacy compliance cannot ignore these important contextual developments. We therefore devote the final part of Chapter 4 to examining trends in data mining by governments as a backdrop to our discussion of USA Patriot Act implications in BC's public sector.

Blurring the Lines: Anti-terrorism and Ordinary Law Enforcement

Perhaps the most troubling theme to emerge from the submissions and from our analysis is the blurring of the lines that have traditionally separated the state's national security and law enforcement functions. This trend is striking in relation to the USA Patriot Act, but it has also been a feature of developments in Canada and Europe since September 11. These developments have been associated with a marked increase in the breadth and intensity of state surveillance, discussed in Chapter 5, and with the implementation of anti-terrorism laws.

We acknowledge that this trend may raise risks for privacy and other civil rights. A fundamental and universally acknowledged principle of privacy protection is that, with only very limited exceptions, personal information gathered for one purpose may only be used for that purpose. Where personal information is gathered for national security purposes—often under special, relaxed legal standards—its later use for law enforcement or other purposes raises troubling questions.

Once again, our analysis of USA Patriot Act implications for privacy compliance in BC cannot ignore the contextual reality of this blurring of functions in Canada and elsewhere and, arguably, degradation or evasion of traditional privacy protections. For this reason, after analyzing the USA Patriot Act in Chapter 6, we turn in Chapter 7 to an analysis of Canada's own post-September 11 anti-terrorism laws and measures, which are an important part of any assessment of USA Patriot Act implications in British Columbia. This discussion will set the stage for our discussion of privacy rights in British Columbia, government responsibilities to protect them and our analysis in Chapter 10 of the implications of the USA Patriot Act with respect to these rights and responsibilities.

3 PROTECTING PERSONAL INFORMATION: OLD RIGHTS AND NEW LAWS

Most people think about privacy and consider it important. That much is evident not only from the hundreds of individual submissions we received but also from public opinion polls showing, over many decades, that most people are concerned about protecting their privacy.[1]

Public awareness of the use and potential for misuse of personal information has heightened in recent years because information can so easily be transferred through computer databases. People quite properly demand the right to control the use of information they provide about themselves, whether to corporations, governments or any other organization. Consumer concern about corporate abuses, usually for marketing purposes, has been a major factor in the passage in Canada of strong new private sector privacy laws that aim to ensure that personal information is only used for the purposes for which it is provided and with the consent of the person it describes. Unlike private sector privacy laws, Canadian privacy laws that apply to governments have traditionally not required consent, but they otherwise generally contain the same principles as private sector privacy laws.

Citizens and consumers expect both governments and corporations to ensure that their personal information will not be put at risk. Some people feel that government should on no account outsource its services because that means transferring their information into other hands and, they feel, providing opportunities for inadvertent or deliberate misuse. Others acknowledge that it is reasonable for government to outsource services as long as it takes effective security measures to protect personal information from being disclosed or used for any other purpose than that for which it was initially collected. The powers provided by the USA Patriot Act are a source of particular concern to many because the security of information is jeopardized (information may be seized from US-linked companies using secret orders). Those powers also create concern about the potential impacts on individuals' lives of access to sensitive information by US authorities for purposes very different from those for which the personal information was provided in the first place. People worry, in other words, that different standards of privacy protection in the US may create a second level of risk by increasing the chance of misuse of personal information once it crosses the national border.

Some submissions we received argue that there is an equally great risk of personal information being accessed under Canadian anti-terrorism laws. Whether or not this is so (a question we discuss in

1 David Flaherty, in *Protecting Privacy in Surveillance Societies* (Chapel Hill: University of North Carolina Press, 1989) at 7 notes that annual Harris polls conducted in the US between 1976 and 1983 showed an increase from 47% to 76% in respondents who described themselves as very concerned or somewhat concerned about privacy, and cited a 1982 survey in London, Ontario, showing that 90% of respondents considered privacy important or very important. Harris polls have showed a steady increase in the numbers of people very concerned or somewhat concerned about privacy. The 2003 poll showed that almost two-thirds of people are often willing to allow others to have access to, and to use, their personal information where they understand the reasons for its use, where they see tangible benefits for so doing and when they believe care is taken to prevent the misuse of this information.

Chapter 7), many people consider the possibility of US access to British Columbians' information offensive to the notion of Canadian sovereignty. Do privacy rights give way when information is secretly accessed, whether by Canadian or US authorities, in the name of fighting terrorism? But what if "fighting terrorism"—in a perhaps never-ending "war on terrorism"—becomes a permanent preoccupation? We also live in a society where the rule of law is paramount, and that includes the protection of civil liberties.

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, 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.

This chapter, therefore, discusses the underlying principles of privacy protection and how they have been translated into law in Canada and other countries. This will set the stage for the discussion in Chapters 4 and 5 of the challenge of protecting privacy in a world in which data increasingly flows internationally and in which, both before and after September 11, governments have asserted the need for expanded surveillance for national security purposes.

What Is Privacy?

A simple and classic definition of privacy is the one provided in 1890 by Louis Brandeis, later a justice of the US Supreme Court: the right to be let alone. Brandeis contended that privacy has several dimensions. It includes the right to control access to your physical space, your body, your thoughts and, as discussed below, information about you.

People sometimes take privacy for granted. It has been said, "Privacy is like freedom: we do not recognize its importance until it is taken away."[2] People may willingly allow the invasion of some aspects of their privacy in order to obtain benefits like medical treatment (privacy of the body) or a driver's licence (informational privacy). They acknowledge the need for government to collect personal information for purposes such as tax collection or the administration of health care programs, as long as care is taken to ensure the information is used only for that purpose and is kept secure from unauthorized access. Society also recognizes the need to allow some invasions of privacy for law enforcement purposes and sets strict rules under which that can happen, for example, by setting rules covering search and seizure.

In some cases, a person's privacy may be violated without his or her acquiescence or even knowledge. Governments collect information about citizens without their knowledge when conducting surveillance for national security purposes but, even then, society imposes certain rules to protect against abuses of authority. Governments also gather intelligence about the activities of foreign agents or terrorist groups in other countries. Here, the rules become murkier because secrecy and opportunism are vital to the success of intelligence gathering.

Alan Westin, in his widely influential book *Privacy and Freedom*, described privacy as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others".[3] Ann Cavoukian and Don Tapscott, in *Who Knows: Safeguarding Your Privacy in a Networked World*, suggested adding the word "if" to "when, how and to what extent", because it is up to each individual to first decide *whether* to communicate information to

2 Ann Cavoukian & Don Tapscott, *Who Knows: Safeguarding Your Privacy in a Networked World* (Toronto: Vintage Canada, 1995) at 13.
3 Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967) at 7.

others.[4]

Almost everyone attaches great value to the protection of information about them from misuse. For that reason, society is careful to ensure that violations of privacy occur only in accordance with strict rules that recognize the importance of informational privacy. Today privacy faces many new threats that sorely test our ability to establish clear rules for the collection, use and disclosure of personal information. Why is it important that we do so? The answer to that lies, at least in part, in the relationship between privacy and other fundamental freedoms that are the bulwarks of democracy.

Why Privacy is Vital

The essence of liberty in a democratic society is the right of individuals to autonomy, to be generally free from state interference in their lives. The liberty interest in democratic societies—of which privacy is a part—has recently been described by the US Supreme Court in this way:

> Liberty protects the person from unwarranted government intrusions into a dwelling or other private places. In our tradition the State is not omnipresent in the home. And there are other spheres of our lives and existence, outside the home, where the State should not be a dominant presence. Freedom extends beyond spatial bounds. Liberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct.[5]

The Supreme Court of Canada has described privacy as an essential component of individual freedom: "An expression of an individual's unique personality or personhood, privacy is grounded on physical and moral autonomy—the freedom to engage in one's own thoughts, actions and decisions."[6] As David Flaherty has put it,

> The contribution of privacy to personal autonomy involves the protection of the inner core self, the ultimate resource of the individual. A person seeks protection from the manipulation and dominance of others in defence of his uniqueness and dignity as a person. The autonomy of the self depends upon the maintenance of wells of reserve. Under normal conditions the ultimate sanctuary of the personality is never breached. The last resource of the individual is that no one can force him to bare his personality and expose his naked self to the shame of total understanding.[7]

Individual autonomy is also essential for healthy communities. As Colin Bennett has put it, without "autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct", we cannot mature and flourish as thinking, responsible, caring persons. Without thinking, responsible, caring people, community withers and society declines. Claims to privacy rest on the recognition that civil society requires "relatively autonomous individuals who need a modicum of privacy in order to be able to fulfill the various roles of the citizen in a liberal democratic state."[8]

As Whitfield Diffie and Susan Landau noted in *Privacy on the Line*, freedom of expression and privacy are not entirely separate notions, but complement one another:

> Privacy is essential to political discourse. The fact is not immediately obvious, because the most familiar political discourse is public. History records political

4 Cavoukian & Tapscott, *supra* note 2 at 21.
5 Lawrence v. Texas, 539 U.S. 558 at 562 (2003). Also see Planned Parenthood of Southeastern Pa. v. Casey, 505 U. S. 833 at 851 (1992).
6 R. v. Dyment, [1988] 2 S.C.R. 417 at 427. Also see Joe Feinberg, "Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution?" (1982) 58 Notre Dame L. Rev. 445.
7 David Flaherty, *Privacy in Colonial New England* (Charlottesville: University Press of Virginia, 1967) at 3-4.
8 Colin J. Bennett & Charles D. Raab, *The Governance of Privacy* (Aldershot: Ashgate, 2003) at 14.

> speeches, broadsides, pamphlets and manifestos, not the quiet conversations among those who wrote them. Without the opportunity to discuss politics in private, however, the finished positions that appear in public might never be formulated.[9]

Alan Westin has noted that the freedom of citizens to choose what information they share with others is one of the fundamental differences between totalitarian states and free societies. The freedom to determine the appropriate balance between anonymity and public participation is, in Westin's words, "the core of the 'right of individual privacy'—the right of the individual to decide for himself, with only extraordinary exceptions in the interests of society, when and on what terms his acts should be revealed to the general public."[10]

Privacy as a Human Right

At the end of the Second World War, the community of nations formed the United Nations to help ensure that no country would ever again be able to start war, on its own people or other nations, without risking the most severe sanctions. One of the first major achievements of the United Nations was the 1948 Universal Declaration of Human Rights.[11] The right to life, liberty and personal security, recognized in Article 3, is the foundation for a broad range of political rights and civil liberties. The right to privacy is expressly guaranteed in Article 12:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

The rights recognized by the Universal Declaration were later codified in the International Convention on Economic, Social and Cultural Rights and the International Convention on Civil and Political Rights, which were adopted by the UN General Assembly in 1966 and came into force in 1976.[12] These two conventions, together with the Universal Declaration, are the main components of the International Bill of Human Rights, which set the standard for national constitutions or implementing laws, including the Canadian Charter of Rights and Freedoms,[13] which came into force in 1982.

Harmonizing Privacy Laws: The OECD's Fair Information Practices

The Universal Declaration's recognition that privacy is a human right might not have inspired quick action at the national level had it not been for growing concerns about the privacy impact of information technology and, more recently, international data flows. By the late 1960s, the growth of automatic data processing was beginning to embed large amounts of information about the details of people's lives in scattered databases with virtually no regulation of their use. The primary users of computer systems then were government agencies that could afford the mainframe computers needed for processing records for tax, social security and social assistance programs. Large banks and insurance companies soon followed suit.

Automatic data processing also developed to the point that the instantaneous transmission of large quantities of data across national boundaries was becoming a common practice. This raised widespread

9 Whitfield Diffie and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* (Cambridge, Massachusetts: The MIT Press, 1998) at 127.
10 Westin, *supra* note 3 at 42.
11 Universal Declaration of Human Rights, G.A. Res 217A(III), UNGAOR, 3d Sess. Supp. No. 13, UN DOC. A/810 (1948).
12 Available online at www.ohchr.org.
13 Constitution Act, 1982, being Schedule B, Part I to the Canada Act 1982 (U.K.), 1982, c. 11.

concerns about the unlawful storage of personal data, the storage of inaccurate personal data and misuse or unauthorized disclosure of personal data in other countries.

Beginning in the early 1970s, several European countries implemented national or state level privacy legislation. One of the first privacy laws was Sweden's Data Act of 1973, which influenced the development of similar laws in other Western European countries. That Act made it unlawful to start or maintain a database of personal information in machine-readable form without first obtaining a licence from the Swedish Data Inspection Board. Four years later, West Germany followed with its federal Data Protection Act, which applied to both the public and private sectors. France enacted its Law on Informatics, Data Banks and Freedoms in 1978.[14]

In 1981, the Council of Europe introduced the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.[15] Although the convention has had, and continues to have, some influence, it did not fully achieve its goal of promoting adoption of harmonized privacy laws throughout Europe. Concern by businesses and governments that differences among national laws might hamper the free flow of personal data across borders and hinder economic development triggered action by the Organisation for Economic Cooperation and Development (OECD).

In 1980, the OECD developed its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[16] The Guidelines contain what have commonly become known as "fair information practices". These practices have been well summarized by Ann Cavoukian and Don Tapscott:

- Only the information that is really needed should be collected.
- Where possible, it should be collected from the individual to whom it pertains (the data subject).
- The data subject should be told why the information is needed.
- The information should be used only for the intended purpose.
- The information should not be used for other (secondary) purposes without the data subject's consent.
- Data subjects should be given the opportunity to see their personal information and correct it if it's wrong.

These fair information practices have become the basis for virtually every privacy law passed since 1980.[17] They are at the heart of the 1995 data protection Directive of the European Union (EU),[18] which requires all EU member states to enact privacy legislation meeting the Directive's detailed requirements (EU Directive).[19] The intended, and desirable, harmony among privacy laws has nonetheless been hindered by gaps between privacy protection approaches in Europe, Canada and the US, gaps that have become a source of increasing tension as a result both of trade globalization and of the addition of anti-terrorism initiatives to the mix of privacy challenges.

Europe-US Tensions

Some assumed that the EU Directive would open a policy window leading to similar privacy laws in the United States and creation of the type of data protection agency that had become standard in Europe.

14 David H. Flaherty, *supra* note 1 at 21, 93, 165.
15 Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, CETS No.:108; opened for signature Strasbourg 28/1/1981.
16 Available online at www.oecd.org.
17 Cavoukian & Tapscott, *supra* note 2 at 25-26.
18 EC, European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] O.J.L. 281/31.
19 Colin Bennett & Rebecca Grant, eds., *Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999) at 12.

However, the US has neither established a specialist, central data protection authority nor strengthened its privacy legislation in response to the EU Directive.[20] Instead, the US Department of Commerce in the late 1990s proposed a voluntary "Safe Harbor" framework under which US private sector organizations provide "self-certification" of compliance with seven privacy principles endorsed by the Department.[21] EU approval of that proposal in 2000, while it eased the anxieties of transnational corporations, generated a new debate within the European community about whether the EU was lowering its privacy standards through compromises with American business and government.

Privacy Protection in Canada

Privacy in democratic countries is protected by a mix of laws enacted by elected representatives and, often but not always, constitutional guarantees interpreted by the courts.

The Canadian Charter of Rights and Freedoms

The Canadian Charter of Rights and Freedoms[22] guarantees certain civil liberties and protects them from government action. Charter rights can only be curtailed by such "reasonable limits" as are "demonstrably justified in a free and democratic society". All governments, ranging from the federal to local governments, must ensure that their laws are consistent with the Charter and that their policies and actions do not offend Charter protections.

Charter protections include the right to be secure against unreasonable search and seizure (in section 8) and the right to life, liberty and security of the person (in section 7). The Supreme Court of Canada has determined that the Charter guarantees to Canadians the right to enjoy a reasonable expectation of privacy from intrusion by government. This extends to the collection and use of personal information. The closer the information is to someone's "biographical core"—such as information about one's health, genetic characteristics, sexual orientation, employment, social or religious views, friendships and associations—the greater the government's obligation to respect and protect the individual's privacy.

Since the Charter came into force in 1982, cases brought before the courts have led to a gradual and increasingly detailed judicial interpretation of how the general principles enshrined in the Charter apply to the day-to-day lives of Canadians in their dealings with government. Chapter 8 of this report provides a detailed analysis, in light of this judicial elaboration of constitutional guarantees, of the relevance of the Charter to the two questions addressed by this report.

Public sector privacy laws

Canada's legislative privacy protections began in 1978, when the Canadian Human Rights Act came into force. The first comprehensive Canadian privacy law, the federal Privacy Act, came into force in 1983, a year after the Charter. It imposes privacy obligations on some 150 federal government departments and agencies by placing limits on their collection, use and disclosure of personal information.

All Canadian provinces and territories now have similar public sector privacy legislation. British Columbia's Freedom of Information and Protection

20 Priscilla Regan, "American Business and the European Data Protection Directive: Lobbying Strategies and Tactics" in Colin Bennett & Rebecca Grant, *ibid* at 200.

21 Maria Recalde, "Seeking Safe Harbor from European Union Privacy Laws" *New England InHouse, Lawyers Weekly USA* (July 2003) available online at www.lawyersweeklyusa.com.

22 Canadian Charter of Rights and Freedoms, *supra* note13.

of Privacy Act (FOIPPA) came into effect in 1993 at the provincial government level and in 1994 at the local public body level. FOIPPA requires over 2,000 British Columbia public bodies to follow its rules on collection, use and disclosure of personal information (defined as "recorded information about an identifiable individual"). Section 30 of FOIPPA requires public bodies such as government ministries and agencies to 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". Section 33 allows public bodies to disclose personal information without notice or consent in specified circumstances. We discuss the relevance of FOIPPA, notably sections 30 and 33, to the USA Patriot Act in Chapter 9.

As noted in a 2001 OIPC report on a FOIPPA privacy investigation, a public body must not enter into arrangements with third parties that have the effect of undermining the public body's ability to meet its obligations under FOIPPA, including section 30. A public body's legal right to have personal information is not an adequate safeguard for FOIPPA's purposes—there must also be assurance of functional protection for that information. Public bodies have a duty under FOIPPA to ensure that outsourcing does not compromise privacy rights under that law and to implement adequate safeguards to maintain control over use and disclosure of personal information.[23]

Private sector privacy laws

As already noted, privacy laws governing private sector activities originated in Europe starting in the early 1970s. The EU's 1995 Directive prohibits transfers of personal information to a country outside the EU unless that country provides what the EU considers, measured against the Directive, an "adequate" level of privacy protection. This has catalyzed legislative responses inside and outside the EU.

The Canadian response first came at the federal level, in the form of the Personal Information Protection and Electronic Documents Act (PIPEDA),[24] which came into force in stages, beginning in January of 2001. Since the start of 2004, PIPEDA has applied to provincially regulated private sector organizations that collect, use and disclose personal information in the course of a "commercial activity" and to federally regulated organizations. PIPEDA does not, however, apply to privacy practices in the course of commercial activity in provincially regulated sectors where the relevant province has, in the eyes of the federal Cabinet, enacted a "substantially similar" private sector privacy law. British Columbia's Personal Information Protection Act (PIPA),[25] which came into force on January 1, 2004, is substantially similar to PIPEDA, as are the laws enacted in Quebec and Alberta.[26]

Private sector privacy laws work by placing limits on private sector organizations' collection, use and disclosure of personal information. Generally speaking, organizations must get the consent, explicit or implicit, of any individual whose personal information they obtain and can only use that information for the purpose for which consent was given. These laws respond to clear public concerns about private sector privacy practices—concerns that show no signs of abating. These laws protect individuals' privacy in the private sector—notably by providing for independent oversight of compliance—but also create a level playing field for all private sector organizations.

23 BCOIPC Investigation Report 01-01, "Investigation into BC Nurses Union Complaint about Telus-VGH LastWord Contract" (5 October 2001).
24 Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5 .
25 Personal Information Protection Act, S.B.C. 2003, c. 63
26 Industry Canada has published its finding, under PIPEDA, that BC's PIPA and Alberta's PIPA are substantially similar to PIPEDA, but the federal Cabinet has yet to formalize this finding with the necessary Order-in-Council. Only Québec's private sector privacy law has obtained the necessary Order-in-Council under PIPEDA. Québec has since challenged the constitutionality of PIPEDA on division of power grounds. The case is pending.

The Ten Privacy Principles

The privacy principles outlined in Canada's PIPEDA and reflected in British Columbia's PIPA are based on the Canadian Standards Association's Model Code for the Protection of Personal Information, which in turn was based on the OECD Guidelines. The ten principles can be summarized as follows:

1. *Accountability*. Organizations are accountable for the protection of personal information under their control.
2. *Identifying purposes*. The purposes for which the personal information is being collected must be identified during or prior to the collection.
3. *Consent*. Information must be collected with the knowledge and consent of the individual and for a reasonable purpose.
4. *Limiting collection*. The collection of personal information is to be limited to what is necessary for the identified purposes and be collected by fair and lawful means.
5. *Limiting use, disclosure and retention*. Information can only be used and disclosed for the purpose for which it is collected and be retained only as long as it is necessary to fulfil the purpose.
6. *Accuracy*. Information must be as accurate, complete and up-to-date as possible.
7. *Safeguards*. Information must be protected by adequate safeguards.
8. *Openness*. Information about an organization's privacy policies and practices is to be readily available.
9. *Individual access*. Information must be accessible for review and correction by the individual whose personal information it is.
10. *Challenging compliance*. Organizations are to provide means to an individual to challenge an organization's compliance with the above principles.

The playing field is also broad. Some Canadian provinces have, it is true, enacted private sector privacy laws that apply only to the health sector, but the trend is apparently toward privacy laws covering the entire private sector, as opposed to dealing with privacy sector by sector.

Privacy Protection in the US

The US has taken a different approach from Europe and Canada to the protection of privacy.

Constitutional protections

Constitutional protection for the privacy rights of Americans is rooted in the US Bill of Rights, which created a series of amendments to the US Constitution. Although the US Bill of Rights, like the Canadian Charter of Rights and Freedoms, does not specifically identify privacy as a right, several amendments have been interpreted to do so by their language. The most relevant of these are the First Amendment (freedom of speech, press, assembly and religion), the Fourth Amendment (freedom against unreasonable search and seizure) and the Fifth Amendment (freedom from self-incrimination). These rights have also been codified in several state constitutions.

The drafting of the US Constitution owed much to the acceptance of a series of assumptions—drawn heavily from the philosophy of John Locke—that defined the context for privacy in a republican political system. These were the concepts of individualism, limited government and the central importance of

private property and its links with the individual's exercise of liberty. Each of these guiding ideas had a common purpose—to free citizens from the surveillance and control that had been exercised over "subjects" by the kings, lords, churches, guilds and municipalities of European society.

In later debates about the nature and extent of the rights of citizens to privacy, the Fourth Amendment proved particularly troublesome. In 1833, in his *Commentaries on the Constitution of the United States*, Justice Joseph Story wrote that the key to the meaning of the Fourth Amendment was its reasonableness clause, requiring that warrants only be issued on the basis of probable cause, be supported by oath or affirmation and describe specifically the place to be searched and the person or objects to be seized. In 1868, Judge Thomas Cooley's *Constitutional Limitations* placed the "citizen's immunity in his home against the prying eyes of the government" alongside protection from "arbitrary control of the person" as the two foundations of personal liberty.[27]

The interpretation of privacy rights of citizens has been an ongoing source of debate. During the past century, the primary sources of controversy have been the evolution of surveillance technologies and the interest of government in the affairs of individuals.

Technological developments have fundamentally altered the nature of communication, surveillance and the very meaning of privacy. With the invention of the telephone, microphone and camera in the latter half of the nineteenth century, the capacity for invading privacy extended into the informal areas of conversation and action. Alan Westin notes that it took several decades for the courts to come to grips with these technological challenges. In 1928, in *Olmstead v. United States*,[28] the US Supreme Court narrowly held that wiretapping was not a search and seizure under the Fourth Amendment. For years to come, the public perception that fighting crime and maintaining moral standards was more important than controlling state use of new technologies acted as a brake on judicial action to expand the notion of privacy to include freedom from electronic surveillance.

When, in 1963, the Supreme Court reconsidered the electronic eavesdropping question in *Lopez v. United States,*[29] a case involving the use of a radio transmitter concealed on the body of a federal official, the majority held that the person being recorded was speaking voluntarily and had no right to privacy protection. In the minority, Justice Brennan stated:

> [A]s soon as electronic surveillance comes into play, the risk changes crucially. There is no security from that kind of eavesdropping, no way of mitigating the risk, and so not even a residuum of true privacy. Electronic surveillance, in fact, makes the police omniscient; and police omniscience is one of the most effective tools of tyranny.

By the early 1960s, public opinion about the value of privacy was shifting again as a result of civil rights controversies and, almost certainly, changing moral attitudes. In *Griswold v. Connecticut*,[30] a 1965 case dealing with a law forbidding the dissemination of birth-control information, Justice Goldberg said that the right to privacy was a fundamental right that could be protected even though "it is not guaranteed in so many words by the first eight amendments". Justice Douglas spoke in the same case of the "zones of privacy" created by several different US Bill of Rights amendments. A survey of editorial reactions at the time showed that most Americans agreed that privacy was a right fundamental to their way of life.[31]

Although the US fairly soon afterwards acquired a federal Privacy Act, early in 2001 it was noted that some

27 Westin, *supra* note 3 at 330-32.
28 *Olmstead v. United States*, 277 U.S. 438 (1928).
29 *Lopez v. United States,* 373 U.S. 427 (1963).
30 *Griswold v. Connecticut,* 381 U.S. 479 (1965).
31 Westin, *supra* note 3 at 338-64, passim.

Contrarian Viewpoints on Privacy Laws

Not everyone agrees that comprehensive and stringently enforced privacy laws are the answer to discouraging violations of privacy. Jeffrey Rosen argues that social disapproval is a better deterrent, warning that

> when a state goes beyond the negative role of refraining from violating the dignity and privacy of its citizens, and uses its power to punish citizens for violating one another's dignity and privacy, it may encourage a degree of surveillance and exposure far greater than the indignities it seeks to avoid.[35]

David Brin, meanwhile, turns privacy on its head by arguing that the answer is not to be obsessed about protecting privacy but rather to eliminate secrecy in public interactions altogether—a "camera on every lamp-post" philosophy. "People of bad intent will be far more free to do harm in a world of secrets, masks and shrouds", he says, "than in a world where the light is growing all around, bit by steady bit".[36]

Both Rosen and Brin cite the lack of effectiveness of the jumble of state and federal privacy laws as giving weight to their positions. Canada has avoided this shortcoming through comprehensive federal and provincial privacy laws that are both largely harmonized with one another and enforced by independent commissioners.

What complicates matters for Rosen's argument, however, is the steady blurring of the lines between information in corporate hands and information in state hands. Social disapproval alone may not be enough to ensure fair play when wayward data pique the interest of intelligence authorities and when technology moves so quickly that public understanding of its uses may lag far behind its latest applications.

Amitai Etzioni takes a different tack in arguing against too great a reliance on privacy laws. His view is that the level and nature of privacy protection must take into account social circumstances that may vary over time. He suggests that the age of individualism that flourished in the United States after 1960 brought with it expectations about sacrosanct rights of privacy that do not always mesh with the best interests of society:

> The realms of rights, private choice, self-interest and entitlement were expanded and extended, but corollary social responsibilities and commitments to the common good were neglected, with negative consequences such as the deterioration of public safety and public health. The new sociohistorical context, as we see it, calls for greater dedication to the common good and less expansive privileging of individual rights.[37]

Etzioni concludes that a balanced approach to privacy protection requires an emphasis on community scrutiny, founded on strongly held social values, rather than the heavy hand of government enforcement. He calls for a "communitarian public philosophy of privacy" that recognizes a whole category of acts in which concerns for the common good take precedence over privacy.[38] Although *The Limits of Privacy* was written before the events of September 2001, surely Etzioni would agree that there could be no better example of an appropriate justification for the negation of privacy rights than society's need to combat terrorism.

The debate about alternative approaches to the protection of privacy is perhaps far more vigorous in the United States than in Canada—the writers quoted above are all American—because Canada already has comprehensive laws in place that appear to enjoy wide public support.

35 Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (New York: Vintage Books, 2001) at 219.
36 David Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* (Reading, Mass.: Addison-Wesley, 1998) at 334.
37 Amitai Etzioni, *The Limits of Privacy* (New York: Basic Books, 1999) at 195-96.
38 *Ibid*. at 214-15. *supra* note 33 at 219.

observers consider that the privacy rights recognized by *Griswold* had contracted rather than expanded in the previous quarter century.[32] Later that year, the US Supreme Court ruled in favour of a criminal defendant who claimed that the thermal imaging device used by police to detect his marijuana grow operation violated his Fourth Amendment rights. The court agreed that using the thermal imaging device constituted a search that violated the defendant's reasonable expectation of privacy.[33] One writer commented of the decision:

> It speaks in majestic tones about protecting privacy from the onslaught of technology, from a Court that has all but given up privacy in favour of crime control…. So what's going on here? Should liberals (or drug manufacturers) start looking to Justices Scalia and Thomas for protection of criminal defendants' rights? I'm afraid not. This is a rare instance of an alliance between liberals and libertarians, united here in support of the sanctity of the home. For Scalia and Thomas, at least, it comes down to property. Step outside, and you're fair game.[34]

Since September 2001, the debate in the US about constitutional guarantees to privacy has again come to the forefront, most notably with regard to the impact of the USA Patriot Act on privacy protection.

US legislative protections

As noted above, the US has followed a different route than Canada and Europe in protecting privacy legislatively. In the public sector, at the federal level, the Watergate scandal was one catalyst for the Privacy Act of 1974. Another was the already mentioned concern about widespread dissemination of personal information resulting from the expansion of computer databases. The Privacy Act, which applies to federal government agencies, was intended to make them disclose their activities in collecting, using and disclosing personal information and to enable citizens to learn about and correct their personal information held by those agencies. One of the key differences between the US Privacy Act and those of Europe and Canada is that it includes no provision for an oversight body (such as a privacy or data protection commission) to ensure compliance with the Act.

In the private sector, the US has, unlike Canada and the EU, taken a sector-by-sector approach to privacy protection, relying on a combination of regulation and self-regulation. Neither states nor the federal government have embarked on Canadian- or EU-style broad-scale privacy laws in the private sector. Privacy is, instead, protected by sector-specific laws such as the federal Children's Online Privacy Protection Act, Financial Services Modernization Act, Health Insurance Portability and Accountability Act, Video Privacy Protection Act and Driver's Privacy Protection Act.

US privacy laws are often, although not always, enforced by private litigation in the courts rather than by specialist privacy oversight agencies. The "Safe Harbor" accord between the US and the EU is a form of self-regulation in many respects, although the Federal Trade Commission prosecutes for deceptive trade practices any company that claims to abide by that accord, but does not.

The Canadian approach to privacy protection is rooted in different cultural norms and historical traditions than exist in the US. Canada, like Europe, has adopted comprehensive legislative protection of privacy rights, enforced through independent oversight. In the US, where suspicion of unnecessary government intervention remains strong, both federal and state administrations have opted for a more self-regulatory route. The result has been a patchwork of privacy laws emerging only in response

32 Craig Berrington, "Privacy, Insurance and the Transparent Society" *Privacy in Focus* (February 2001), available online at Wiley Rein & Fielding at www.wrf.com.
33 *Kyllo v. United States*, 533 U.S. 27 (2001).
34 David Cole, "Scalia's Kind of Privacy" *The Nation* (12 July 2001), available online at www.thenation.com.

to pressing circumstances—an approach that might be described as privacy where necessary, but not necessarily privacy.

Conclusion

Much of the discomfort voiced about the implications of the USA Patriot Act for Canadians can be attributed to the fact that there currently exists such disparity between the American and Canadian approaches to privacy. Moreover, regardless of which approach one favours—stringent laws or very little law at all—the rules must be clear and clearly understood. As a result of the disparity, Canadian personal information flowing across the border into the US does not always meet with the same standards for protection that we have come to expect here.

The risk of misuse of personal information conveyed outside Canada has increased in recent years as a result of advancements in information technology. The globalization of data processing that prompted the OECD into action a generation ago continues to bedevil attempts to provide meaningful privacy guarantees or redress for any harmful effects of data flows across borders. Coupled with the trend toward outsourcing of government services, the increasingly seamless world of data flows continues to challenge law-makers and regulators grappling with the need to protect citizens' privacy. We discuss these trends in the following chapter.

In subsequent chapters we will articulate our conclusion that the absence of clear rules regarding the protection (or lack of protection) of civil liberties under anti-terrorism laws, reflected in the lack of clear distinction between national security and law enforcement purposes, deserves consideration in both countries, in addition to being a matter of concern to British Columbians who could be affected by the reach of the USA Patriot Act.

4 SHARING PERSONAL INFORMATION: DATA IN A SEAMLESS SOCIETY

Data flows like water: what begins as a small stream may eventually run into a sea of information that cannot easily be protected. When data protection laws first came into place in the 1970s and 1980s, data banks were smaller, less sophisticated and more isolated than they are today. Later, advances in information technology enabled the merging of databases into massive banks of information. Especially in the US, access to data conglomerates may occur with little regulation and for multiple commercial and governmental purposes—including, increasingly, national security. In Canada, outsourcing by Canadian governments and corporations has steadily increased the flow of data among public and private sector organizations. This heightens the need for enhanced security measures to protect personal information from misuse, especially when there is a possibility of data transfers to US organizations.

Since September 11, 2001, anti-terrorism initiatives in the US have resulted in steadily increasing government surveillance of databases as well as the creation of specific powers providing for access to information considered necessary for the detection and deterrence of terrorist activities. The expanded reach of US national security laws is prompting changes in business practices in Canada, where many companies have US parents or subsidiaries. A pertinent example was provided in September 2004 by a Canadian Imperial Bank of Commerce mailing to its credit card holders. New provisions in the cardholder agreement included the following paragraph:

> I acknowledge that in the event that a Service Provider is located in the United States, my information may be processed and stored in the United States and that United States governments, courts or law enforcement agencies may be able to obtain disclosure of my information through the laws of the United States.[1]

In an article about the notice, *The National Post* noted that the USA Patriot Act is putting pressure on US financial institutions to monitor and disclose to law enforcement and other state agencies details of individuals' banking activities. It continued:

> A report this week by KPMG said banks worldwide are being called upon by regulators and governments to be the first line of defence in a crackdown on money laundering and terrorist fundraising… Many Canadian firms subcontract credit card operations to a Georgia-based company called Total System Services Inc.[2]

This report focuses on personal information collected by government. It is important to note, however, that the implications of the USA Patriot Act for the protection of personal information are not restricted to government-controlled information.

1 Canadian Imperial Bank of Commerce Notice, "Changes to the CIBC VISA Cardholder Agreement" (September 2004).
2 Barbara Schecter, "Visa Accounts Open to U.S. Law Enforcement Agencies, CIBC Warns" *The National Post* (24 September 2004) FP1.

The potential vulnerability of information to access by US government authorities is simply one factor contributing to increasing public concerns about the everyday flow of data from Canada to the US, often through the outsourcing of public services.

Outsourcing Trends

'Outsourcing' describes the contracting out of business functions to external suppliers, eliminating the need to maintain internal staff necessary to perform that function.[3] Governments have increasingly been following the lead of corporations in contracting out services formerly done in-house. Governments intent on balancing budgets may view outsourcing as an opportunity to pare costs of major programs. In addition, arrangements with contractors may provide the promise of increased efficiency in the delivery of services that require specialized knowledge or advanced technology.

Proposals for outsourcing of government functions sometimes lead to controversy, as the BC government's proposal to outsource the operation of the Medical Services Plan shows. Supporters describe the advantages to be gained from cost savings and improvements in service quality and may support outsourcing without any qualification as to where and to whom services should be outsourced. Some critics claim, on the other hand, that outsourcing has more to do with ideology than with cost-savings. They express concern that outsourcing decisions are not transparent enough and that government agencies, unlike corporations, should consider non-economic factors in deciding whether to outsource. Still others support outsourcing if jobs are not moved out of the province or country, but theirs is an uphill battle in an age when technology and free trade agreements have greatly reduced the relevance of geographical borders.

Information technology: globalization's 'Third Wave'

The business of government has grown increasingly complex and efficient management of information is essential. Data management companies compete to offer public sector clients technology and services for storing, organizing and accessing information. What distinguishes information technology outsourcing from other types of outsourcing is that such outsourcing arrangements often deal with personal information. Technological advances and trade liberalization have increased the flow of personal information in the course of data management services not only between Canada and the United States, but also, increasingly, to countries like India and China. More generally, the outsourcing of 'knowledge work' has been described as the third wave of globalization, following trade and manufacturing.[4]

In the US, transnational transfers of personal information as a result of outsourcing sparked concerns about the vulnerability of personal information sent outside the US, resulting in the recent introduction in the House of Representatives of a law designed to ensure that data protection laws in offshore jurisdictions meet stringent standards.[5] There is more than a little irony in this proposal, given the concern expressed by some other countries that US privacy standards are too lenient. Nevertheless, developing countries that hold a major stake in the outsourcing industry are now acting to respond to US concerns. India, for example, is taking the lead in implementing data protection safeguards and the

3 Public Policy Forum, and ITAC Round table, "IT Offshore Outsourcing Practices in Canada" (Ottawa, 20 May 2004).
4 *Ibid*. at 6.
5 US, Bill H.R. 4366, Personal Data Offshoring Protection Act of 2004, 108th Cong., 2004.

outsourcing industry in that country is reported to have implemented tough security measures that exceed North American norms.[6]

For a country like India, the stakes are high. In a recent article, Katherine Boo described how Chennai, the fourth largest city in India, has utilized electronic portals to develop a rapidly expanding niche doing the work of American companies like Verizon, Bank of America, Hewlett-Packard, Citibank, Visa, MasterCard and Electronic Data Systems. Boo explains that

> [t]he Americanization of Chennai has been so swift and … so quiet that many of its citizens do not yet grasp the change in their cultural and literal landscape. An animation company makes cartoons seen by American children on Saturday mornings. Radiologists read American MRIs, clerks adjudicate U.S. tax returns, and programmers automate Medicaid eligibility for an entire midwestern state. Chartered accountants complete U.S. tax returns while underwriters certify U.S. mortgages. And within Office Tiger's pink building aspiring financiers analyze American firms that are ripe for takeover in a place they call Wall Street East.[7]

Commenting on the expanding scope of outsourcing to India, Boo notes that a study by the University of California at Berkeley identifies fourteen million US jobs at risk to outsourcing in the near term.[8] Some of the same companies that provide outsourcing services to governments in North America send their own work offshore to developing countries.

Developing countries are not the only major recipients of corporate outsourcing contracts. A recent report by the UN Conference on Trade and Development notes that Canada runs a close second to India in attracting service work sent offshore, including call centres, information technology projects and regional headquarters.[9] All indications are that, in the globalized economy, outsourcing will continue to expand rapidly.

Outsourcing in British Columbia

The BC government has struggled for many years with how best to manage the flow of data needed to support its services. In 1978, the BC Systems Corporation (BCSC) was created to establish policies for the rationalization of data processing in government and to provide information technology services to government. After BCSC tried to extend its mandate to become a commercial Crown information technology service provider, private sector firms objected that the corporation was engaging in unfair competition[10] and called for its dissolution. BCSC was disbanded in the mid-1990s.

Since then, the BC government has continued to outsource an increasingly broad variety of information tasks. In the mid-1990s, IBM Canada began providing information technology services, including merging of databases, to support the operation of the Medical Services Plan and PharmaNet. In March 2004, the BC government selected Maximus to administer the Medical Services Plan. Based in Virginia, Maximus provides business operations and information technology services to governments, including health care enrolment services and child support enforcement operations in Canada and the US. Its wholly owned Canadian subsidiary, Themis, has its head office in Victoria. Contract negotiations were underway at the time of the writing of this report.

6 Simon Chester, "Outsourcing Threat to Privacy Overblown" *Financial Post* (16 August 2004).
7 Katherine Boo, "The Best Job in Town: The Americanization of Chennai" *The New Yorker* (5 July 2004) at 57.
8 *Ibid*. at 59.
9 Barrie McKenna, "Offshoring of Jobs Big Benefit for Canada" *The Globe and Mail* (23 September 2004) A-1.
10 D. Smith and B. Barnard, "Consultations on British Columbia's Information Structure" prepared for the BC Ministry of Employment and Investment (9 November 1994), available online at www.vcn.bc.ca.

In early 2002, the Information and Privacy Commissioner wrote to all Cabinet Ministers to provide guidance for the protection of privacy in the implementation of outsourcing plans:

> Alternative service delivery models can improve service delivery and yield cost-savings. The privacy risks should not, however, be underestimated where personal information is being collected, used, disclosed or managed by an outside service provider who is not familiar with legal privacy requirements. Such risks include use or disclosure of personal information by unauthorized personnel, compromised integrity of personal information, accidental disclosure of personal information and improper retention or secondary use of personal information.
>
> Ministries are, of course, subject to the privacy provisions of Part 3 of the Act, including when they adopt alternative service delivery methods such as contracting-out. On November 14, 2001, my Office issued *Guidelines for Data Services Contracts*, OIPC Guideline 01-02 ("OIPC Guidelines"). These are intended to pro-actively support any initiatives that involve the contracting-out of services involving personal information. A copy of the OIPC Guidelines is enclosed for your information. The OIPC Guidelines acknowledge that a public body cannot, through a service delivery agreement, contract out of its privacy obligations under Part 3 of the Act. I urge you to ensure that your Ministry, in contracting out or otherwise securing private sector provision of services to or for the public, includes appropriate privacy compliance provisions in all contracts involving personal information.
>
> As between any government-developed privacy compliance standard and the Act's requirements, the Act of course prevails. The OIPC will, in discharging its statutory role to enforce compliance with the privacy provisions of Part 3, refer to the OIPC Guidelines for general guidance. The OIPC's disposition of a particular matter will, of course, be determined in each case by the Act's requirements and by the relevant facts (including the nature of the personal information involved and the type of the services or relationship).
>
> In addition, this Office has for years urged public bodies to carry out a privacy impact assessment ("PIA") for each proposed policy, program or legislative amendment. A PIA tool for this purpose may be found on our Website, at www.oipcbc.org. This tool is designed to allow a ministry to identify, at the earliest stage of policy or program development, any privacy impacts that may be show-stoppers or that should influence design. It makes sense to perform a PIA as soon as possible in the process, as this is more cost-effective in identifying and addressing privacy impacts and ensuring compliance with Part 3 of the Act. I ask you to ensure that your Ministry carries out a PIA for each alternative service delivery proposal involving personal information.[11]

The Guidelines for Data Services Contracts and Privacy Impact Assessment tool have since been updated and are available on the Public Sector section of our website.

Outsourcing in other provinces

Many corporations operating in Canada are subsidiaries of multinationals or US companies headquartered in the US, which often centralize the storage and processing of information at the home office in the US or with a service provider in that country. Information may thus routinely flow from a Canadian subsidiary to a US parent.

Outsourcing to US companies is nothing new, nor is it unique to BC. Nova Scotia, for example, employs Electronic Data Systems to manage provincial government databases, including social assistance, payroll and motor vehicle registration (with control of the data base apparently remaining in Canada).[12] Saskatchewan has outsourced government services

11 Correspondence from David Loukidelis, Information and Privacy Commissioner for British Columbia, to all Cabinet Ministers, "Alternative Service Delivery—Privacy Issues" (21 January 2002).

12 Personal communication, Darce Fardy, Review Officer, Nova Scotia Freedom of Information and Protection of Privacy Review Office (5 July 2004).

to US companies over the years and Ontario has outsourced social assistance operations to Accenture, a company with significant US links. What is relatively new is public concern about the implications of transfer from governments to corporations of personal information about citizens from government to private enterprises.

Public concerns about personal information in outsourcing arrangements

After contracting with the Canadian subsidiary of Lockheed Martin to process the returns for the 2006 national census, Statistics Canada encountered an unexpected wave of public opposition and said it was cancelling the contract and that Statistics Canada staff would handle and process the census questionnaires. The agency noted that media reports had led to

> the incorrect perception that the confidentiality and privacy of the information provided to Statistics Canada may be compromised by the use of outside contractors. While this was never the case owing to the stringent security measures in place, the agency acknowledges and accepts that perceptions are important.[13]

In October 2004, however, Statistics Canada confirmed the signing of a new contract under which Lockheed Martin Canada would develop hardware and software to process the census forms. The director of the census program explained that there would be safeguards in place to ensure the private company cannot get access to the census information and that all questionnaires and data would be handled at Statistics Canada sites, with no external connection. This was intended to reassure critics who continued to express concerns about the USA Patriot Act.[14]

The public's response to the Statistics Canada proposal reveals a growing sensitivity about the use of sensitive personal information, especially when US companies are involved. It is not always easy to determine the reasons for such public concerns since a variety of factors may be involved. Some, such as concerns about the level of US involvement in the Canadian economy, may have nothing to do with privacy. Increased public and media awareness of privacy risks, and of privacy laws, may play a role. In addition, heightened concerns about the possibility of information leaks from insecure databases may contribute to public unease. These factors certainly figured prominently in the submissions we received from the public about outsourcing to US-linked companies.

Stories in the press about misuses of sensitive personal information in data banks undoubtedly contribute to public suspicion about the security of personal information held by corporations and governments. For example, in July 2004 the Winnipeg Free Press reported that the customer database of a Winnipeg Internet pharmacy had been stolen and that a Florida company was allegedly offering to sell the personal information on more than 32,000 patients to the highest bidder. In a letter sent to pharmacies and Internet pharmacies throughout Manitoba, the company offered to sell the database for US$130,400, claiming that a buyer could make millions using the database to target customers with a documented willingness to buy online.[15] Designers of security systems find themselves hard-pressed to keep pace with the technical ingenuity of those who, for monetary gain or other motives, covet the contents of databases.

13 Statistics Canada, "Role of Private Contractors in the Census" available online at www12.statcan.ca.
14 Canadian Press, "Census Deal with U.S. Firm Goes Through" *The Globe and Mail* (9 October 2004), available at www.theglobeandmail.com.
15 Leah Janzen, "Florida Firm Hawking Stolen St. B. Net Drug List" *Winnipeg Free Press* (5 August 2004).

International Trade and Investment Agreements

Proponents and critics of outsourcing both raise the fact that Canada is party to complex international trade and investment agreements[16] that may affect the outsourcing of government services and information services. They stress different aspects of these agreements, however.

The British Columbia government emphasizes the importance of considering whether the exclusion of contractors with US connections from bidding on an outsourcing contract would violate Canada's international trade obligations, which could potentially expose Canada to retaliatory action by the US. It also acknowledges that, at the present time, provincial governments are not subject to NAFTA and WTO government procurement obligations and that there are also certain exceptions from NAFTA and WTO obligations for services necessary to maintain public health and safety.[17]

The Final Report of the Commission on the Future of Health Care in Canada (Romanow Report) offered the following summary of the exceptions and reservations issue as it affects health care services in Canada:

> Each of the [various international trade] agreements has particular exceptions and "reservations". Under NAFTA "social services established or maintained for a public purpose" are exempted from the terms of the agreement. Successive Canadian governments have argued that this reservation protects the public health care system from the full force of NAFTA's provisions and means that services that existed prior to the agreement are protected. However, there is no clear definition of what constitutes a "social service" or what determines whether a service is established for a "public purpose" [reference omitted]. Similarly, many of Canada's obligations under the GATS apply only to those services or sectors that are explicitly made subject to the agreement. To date, Canada has chosen not to make hospital services and a whole array of health services subject to GATS or to open them to foreign private investment or delivery by foreign-based companies.[18]

The Canadian Union of Public Employees' submission emphasizes that, while it is debatable (or at least subject to case by case consideration) whether Canada's international trade obligations do not permit it to limit outsourcing to Canadian businesses, "it is certain that once a function has been outsourced to an American company, it will be difficult or impossible to bring that work back in house without attracting trade sanctions."[19] This was a concern also noted in the Romanow Report:

> Some have described this as a "one way valve" that, once opened, may not be able to be closed [reference omitted]. It is possible that, once foreign-based for-profit hospitals are allowed to operate, it would be very difficult to reverse course and subsequently preclude those hospitals from operating even if their services were of poorer quality, their costs were high, or their presence no longer reflected the policy goals of Canadians.[20]

Some organizations do not oppose outsourcing but do oppose the compromises to privacy that may result. As the British Columbia Civil Liberties Association's submission put it:

16 Submission of Government of British Columbia (23 July 2004), p. 41, refers to the North American Free Trade Agreement (NAFTA), the World Trade Organization (WTO) General Agreement on Trade in Services (GATS) and the WTO General Agreement on Tariffs and Trade 1994 (GATT 1994). It also observes that British Columbia is a party to the Canadian Interprovincial Agreement on Internal Trade.

17 Submission of Government of British Columbia (23 July 2004) pp. 42-43.

18 Final Report of the Commission on the Future of Health Care in Canada, *Building on Values: The Future of Health Care in Canada* Roy J. Romanow, Q.C., Commissioner (November 2002) at 236.

19 Submission of the Canadian Union of Public Employees (4 August 2004), pp. 16-17, citing a February 29, 2000 opinion by international trade lawyer Stephen Shrybman concerning the privatization of insured health care services in Alberta. This point is also made in the submission of the Council of Canadians (6 Aug 2004) p. 4.

20 Romanow Report, *supra* note 18 at 238.

> The BCCLA has no position on outsourcing generally. However, where the outsourcing involves risks to privacy, the Association does take issue. In the instant matter, there is risk of unauthorized access to highly sensitive personal information. Because there is no need to outsource to a foreign company, the risk is being assumed voluntarily. The policy laundering[21] argument that NAFTA-Made-Us-Do-It does not have any application to the facts; the government has a choice as to how to deliver these services….[22]

As stated in the United Nations Conference on Trade and Development's recent report on the globalization of service, countries need to be careful when negotiating international trade obligations related to public services, so that their own policy objectives—including, in the context of this report, privacy protection objectives—are served best.[23] The following observation in the Romanow Report is worth remembering in this respect:

> In the past, our relative size, especially in relation to the United States, has meant that Canada has been a "rule-taker" (i.e., a country that accepts the rules set down by more powerful countries) rather than a "rule-maker" (i.e., a country that acts with other like-minded countries to set the rules). But as the number of countries that are parties to international agreements grows and international trade organizations struggle to balance social policy interests of their members with the commitment to open up markets to trade, Canada is well placed to work with other like-minded countries to ensure that international trade agreements protect our social policies while not depriving us of the benefits of increased trade.[24]

Canada has a stake in ensuring that international trade obligations not only promote international trade but also protect the right of all countries to make independent policy choices. Canada needs to 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.

Gathering and Hunting: Data Banks and Data Mining

The expense of marketing combined with the falling cost of information technology gives businesses a strong incentive to gather information about consumers for purposes such as targeting potential customers and tailoring products to meet consumer demands. Unless carefully controlled, personal information collected by a company will leak into giant data banks that soak up information from a multitude of businesses.

Data banks

Whether collected by governments or corporations, personal information is increasingly likely to be accumulated in large data banks. Some multi-billion dollar companies exist only for the purpose of collecting, analyzing and sharing personal data with other companies for a variety of purposes. ChoicePoint, for example, provides information to the insurance industry to support underwriting and fraud prevention but also provides identity authentication services to employers and others, as well as information

21 Policy laundering is the process by which a government implements what would normally be a controversial policy at home claiming that its international obligations force it to do so, but where the government actually helped negotiate the same international obligations that supposedly force its hand. By first laundering the controversial policy through international mechanisms and agreements, the government is able to do something that would otherwise be controversial, citing its obligations as a member of the community of nations.

22 Submission of the British Columbia Civil Liberties Association (6 Aug 2004), p. 8.

23 United Nations Conference on Trade and Development, *World Investment Report 2004: The Shift Towards Services* (United Nations: New York and Geneva, 2004) at 234 (Box VI. 6. II).

24 Romanow Report, *supra* note 18 at 235.

Judging People by Their Digital Dossiers

As Jeffrey Rosen has pointed out, the Internet in one sense has strengthened privacy, by increasing the opportunity for anonymity, and in another sense has reduced privacy because every use of the Internet leaves electronic footprints behind. Electronic footprints can be collected and analyzed by strangers. Rosen warns about "the danger of being judged, fairly or unfairly, on the basis of isolated bits of personal information that are taken out of context". What holds true for the Internet applies to databases in general. The result is an incomplete picture in which information is mistaken for knowledge. As Rosen notes,

> In an age when disaggregated personal information is centrally collected, widely accessible, and permanently retrievable, private citizens run the risk of being treated like celebrities in the worst sense, vilified rather than celebrated on the basis of isolated characteristics.[25]

What makes the description of a person in today's global data world especially worrisome is that the portrait created is not a portrait of one's true self. Our digital selves, in other words, can hardly reflect our true selves. Analysis of data can create a caricature, but it does not create a person—and the essence of privacy is maintaining your personhood. This is of more than philosophical concern. The pooling of data streams and analysis of the data can have real and costly consequences for individuals.

Intimate information that people once might have shared only with their closest friends now has a way of gathering in secret places for the scrutiny of those with the money or the authority to examine the collective picture. As Charles Sykes has said,

> The very technology that was supposed to free us from mass society and the conformity of mass media has turned out to be as much a fishbowl as an information highway. In modern society, we have discovered that being free means also being naked. The same society that allows us to live anonymously relies on surveillance to keep track of us because we are a society of strangers.[26]

Ten years ago, the Australian privacy expert Roger Clarke coined the term "digital persona" to describe the model of an individual established through the collection, storage and analysis of data about that person. Clarke described the digital persona as a "potentially threatening, demeaning and perhaps socially dangerous phenomenon," especially given the propensity for organizations to employ data surveillance—or "dataveillance", as he called it—to exercise control over the behaviour of individuals and the societies they collectively form:

> If information technology continues unfettered, the use of the digital persona will inevitably result in impacts on individuals which are inequitable and oppressive, and in impacts on society which are repressive. European, North American and Australasian legal systems have been highly permissive of the development of inequitable, oppressive and repressive information technologies. Focussed research is needed to assess the extent to which regulation will be sufficient to prevent and/or cope with these threats. If the risks are manageable, then effective lobbying of legislatures will be necessary to ensure appropriate regulatory measures and mechanisms are imposed. If the risks are not manageable, then information technologists will be left contemplating a genie and an empty bottle.[27]

25 Jeffrey Rosen, *The Unwanted Gaze: the Destruction of Privacy in America* (New York: Vintage Books, 2001) at 200-202.
26 Charles J. Sykes, *The End of Privacy* (New York: St. Martin's Press, 1999) at 16.
27 Roger Clarke, "The Digital Persona and Its Application to Data Surveillance" *The Information Society* 10:2 (June 1994).

to support marketing campaigns.[28]

Privacy experts express concern that in the US, unlike Canada and Europe, the gathering, sharing, selling and use of personal and consumer information is largely unregulated outside the health care and banking sectors and that this lack of regulation makes it virtually impossible to protect privacy. One of the primary arguments for maintaining a free and unregulated flow of information is that doing so is essential for a healthy economy. Not everyone agrees with that premise, however. For example, Peter Swire suggests that the lack of privacy protection can discourage people from full participation in the economy. "When you consider what's contained in today's financial records, the record really of an entire way of life, it's easy to see how people would be afraid to engage in transactions that would lead to exposing sensitive information", he states. "You can make a strong case that privacy protections will help the functioning of our economy by reducing some of those fears of exposure."[29]

The economic argument, a central issue in the debate about privacy protection in US commerce, overlooks the fact that privacy is a basic civil liberty. In 1977, the US Privacy Protection Study Commission expressed grave concern about the consequences of automated record-keeping for protection of personal information:

> The real danger is the gradual erosion of individual liberties through the automation, integration and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable.[30]

While these sound like prophetic words, the Commission could hardly have foreseen the extent to which data banks would be integrated a quarter of a century later. Nor can we predict with any accuracy where technology will take information management in another twenty-five years.

Uncertainty about the future underscores the need to institute sufficient legal privacy protections today so that public policy will guide technology rather than blindly following it. The new Canadian privacy laws discussed in Chapter 3 cannot realistically stem the flow of personal information from Canada into data banks in the US or elsewhere. They do not, for example, provide clear means to retrieve and erase whatever personal information may have existed in those data banks before the new laws came into effect.

Probing information banks: data mining

Privacy advocates worry about the vulnerability of information held in data banks to theft, alteration or misuse and about the difficulty facing citizens attempting to correct inaccurate information once it has lodged in a bank whose custodians may lack the accountability and responsiveness of agencies or companies that originally collected the information. But they are also concerned about the possible implications of data mining—which may use software that applies undisclosed and unverifiable analytical criteria and assumptions—for people who may be inaccurately labelled or stigmatized as, for example, bad credit risks for reasons unrelated to their actual payment history.

Data mining uses various techniques to extract information from large volumes of data and subject it to analysis. As practised by federal government agencies

28 Christopher Brown, "Experts Debate Uses, Privacy Concerns Raised by Vast Databases of Personal Info" *Privacy and Security Law* 3:13 (2004).
29 *Ibid.*
30 US Privacy Protection Study Commission, *Personal Privacy in an Information Society* (July 1977), available online at www.epic.org. Similar warnings were sounded earlier in *Privacy and Computers*, the 1972 report of a task force established jointly by the Canadian Departments of Communications and Justice. Also see *Records, Computers and the Rights of Citizens,* the 1973 report of the Advisory Committee on Automated Personal Data Systems established by the US Secretary of Health, Education and Welfare, online: www.epic.org.

in the US, data mining has been described as "the application of database technology and techniques—such as statistical analysis and modeling—to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results".[31]

A key characteristic of data mining is that analysis of an individual's personal information creates new, secondary, information about that person.[32] The "hidden patterns and subtle relationships" that data mining detects are recorded and become personal information of the individual whose life is being scrutinized and analyzed. Information about an individual's credit history, credit card purchases, law enforcement record or interactions, travel habits and so on may be mined to derive the finding that she is a possible terrorist who should be put on a terrorist watch list and be kept under surveillance. This new personal information would become part of the swelling river of data whose channels are, in the private and public sectors, ever changing and difficult to follow, much less control. In this light, data mining raises concerns about the accuracy and use of derived personal information, not to mention the individual's right of access to and correction of such information.

Data mining has become an increasingly common practice in government agencies in the US. If agencies can increase their efficiency by not duplicating the collection of personal information, by collecting more of it, by adopting new technologies to monitor the behaviour of individuals more carefully or by compiling denser and more complete profiles of citizens, then they may feel compelled to do so.

Advances in database technology also simplify the process of searching out information that may be used to identify possible criminals or terrorists before a crime is committed—or to identify individuals of interest to government agencies or the private sector for other reasons.

In response to concerns raised by a subcommittee of the US Senate, the General Accounting Office (recently renamed the Government Accountability Office), an independent US government agency, recently studied the extent of data mining by US federal agencies. The GAO found that 52 of 128 US federal government departments and agencies included in the study use or plan to use data mining. The six most common uses included: improving service or performance; detecting fraud, waste and abuse; analyzing scientific research and information; managing human resources; detecting criminal activities or patterns; and analyzing intelligence and detecting terrorist patterns. The latter two uses accounted for six out of eight data mining incidents reported by the Department of Justice. The Department of Homeland Security was the only federal agency that declined to identify the specific purposes for which it used data mining.[33]

There is no doubt that, in principle, data mining activities may yield benefits in the form of improved services and greater efficiency. On the other hand, the easier it becomes to accumulate and analyze personal information on a massive scale, the greater the potential for intentional or unintentional misuse and error. As data banks and data mining grow in nature and extent, each person's life is becoming more of an open book, in which new details become visible with

31 US General Accounting Office, *Data Mining: Federal Efforts Cover a Wide Range of Uses* Report to the Ranking Minority Member, Subcommittee on Financial Management, the Budget, and International Security, Committee on Governmental Affairs, U.S. Senate, (May 2004) at 1 (available at the GAO website: www.gao.gov). The term 'knowledge discovery' is increasingly supplanting 'data mining', for various reasons, including perhaps because it sounds more productive and less threatening.

32 As noted by Colin J. Bennett, in *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1992) at 19, the ability to assemble information selectively or to correlate existing information "can be functionally equivalent to the ability to create new information". This is certainly the functional outcome of much if not all data mining. Also see Paul Sieghart, *Privacy and Computers* (London: Latimer, 1976) at 75-76.

33 US General Accounting Office, *supra* note 31 at 2, 8.

each new advance in data management technology.

The GAO's study was intended simply to assess the extent of data mining in the US government. Because privacy issues were such a prominent theme in interviewees' comments, however, the GAO intends next to examine such privacy implications of data mining as:

- quality and accuracy of mined data;
- use of data for other than the original purpose for which data were collected without consent of the individual;
- protection of the data against unauthorized access, modification and disclosure; and
- the right of individuals to know about the collection of personal information, how to access that information and how to request a correction of inaccurate information.

The 2005 fiscal year US Department of Homeland Security spending bill, unanimously passed by the US Senate, would require the Executive Branch to report to Congress on US federal government agencies' use of data mining technologies and the privacy impact of their activities.[34]

Merging government and private databases

Since September 2001, US government agencies have intensified their efforts to link government databases with industry databases. In 2003, the Pentagon acknowledged that it was funding research into a proposal to create a giant data base, from public and commercial sources, that would be used to identify possible terrorists through analysis of patterns in the data. Under the Total Information Awareness program, the U.S. government would combine large amounts of information collected from the private sector into a giant database that would identify patterns believed to be associated with planning terrorist attacks.

In response to public concerns, the Pentagon changed the name of the program to Terrorism Information Awareness, clearly to avoid unfortunate undertones, but the research project remained highly controversial and was finally scrapped.[35] Other proposals for data collection have included a US Department of Justice plan to access information collected by Internet service providers and a national identity card system, which could facilitate the collection and linking of public and private sector personal information.

Soon after September 11, a company called Seisint and several US states created the Multistate Anti-Terrorism Information Exchange (Matrix) by combining the company's own commercial databases with law enforcement records. Matrix records include personal information such as current and past addresses and phone numbers, arrest records, real estate information, photographs of neighbours and business associates, car make, model and colour, marriage and divorce records, voter registration records and hunting and fishing licences. Funded in part through contracts with the US Departments of Justice and Homeland Security, Seisint sells database access to several states.[36]

Personal information in such merged databases can include individuals' email records, health problems, credit history and credit card purchases, criminal records or interactions with the police, employment histories, telephone records, television shows watched, vacation destinations and website visits. One critic of the scope of such initiatives contends that "under the guise of national interest,

34 US, Bill H.R. 4567, Department of Homeland Security Appropriation Act, 2005, 108th Cong., 2004.
35 Arthur J. Cockfield, "The State of Privacy Laws and Privacy-encroaching Technologies after September 11: A Two-year Report Card on the Canadian Government" University of Ottawa Law and Technology Journal 1 (2003-2004) 327 at 337.
36 Madeleine Baron, "Welcome to the Matrix: Inside the Government's Secret, Corporate-run Mega-database" *The New Standard* (9 July 2004).

a government employee, without the knowledge of the individual in question, could scrutinize these merged databases."[37]

Conclusion

As Daniel Solove has observed, we have entered a new era of "pervasive recording of information" that differs in kind and degree from the information gathering activities of the past. The appetite of data banks is insatiable and digitally stored information is permanently encoded. Once personal information has escaped into the data universe, retrieving it or erasing it may be a virtual impossibility and correcting errors may be no easy task.

The increasing incidence of data mining by government agencies, at least in the US, has widened the spread of information and increased the potential for negative impacts on data subjects. We are not aware of studies of data mining by Canadian government agencies but assume that data mining technologies are as available to them as to their US counterparts. As the privacy impacts of data mining may be significant, in Chapter 11 we recommend audits of data mining practices by British Columbia and federal government agencies.

Canada needs to 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.

While new Canadian privacy laws will help to control the flow of data, limit the purposes for which it can be used and facilitate the correction of wrong information, they do not apply to personal information once it has crossed the border into the US. In the next chapter, we will discuss the implications that arise when data mining by government agencies overlaps with state surveillance for national security and law enforcement purposes.

37 Cockfield *supra* note 35 at 337.

5 STATE SURVEILLANCE: PRIVACY AND NATIONAL SECURITY

'Surveillance' is simply an official-sounding term for close observation.[1] It can be conducted openly (a visible video camera) or secretly (a wiretap). An individual can be the subject of surveillance and so can the general population. Surveillance may be conducted by government agencies for many purposes and frequently makes use of electronic tools such as data mining. For national security and law enforcement purposes, surveillance is increasingly being conducted anonymously and electronically—police may still watch crowds at demonstrations, but they seem increasingly likely to be found at computer screens.

High Technology Tools

Since 2001, both Canada and the United States have increased domestic surveillance. Intelligence and law enforcement agencies in both countries will naturally continue to take advantage of whatever technologies are legal and presumed effective. Some technologies can protect and enhance privacy, but new tools to facilitate surveillance are constantly emerging. For example, both Canada and the US have floated the notion of biometric national identity cards, which could be used to match people's 'tombstone information' (legal name and date of birth) to information in data banks, but neither has implemented them yet.[2] As another example, data from a facial-scanning program for visitors to the US is entered into a database that can be shared with law enforcement agencies and compared against a watch list for potential terrorists.

In Chapter 3, we discussed the essence of the right to privacy in democratic societies: it is up to each individual to decide what personal information to share with others. Still, almost everyone accepts the need for some level of government surveillance to detect and deter criminal activity and, more recently, terrorist activity. This acceptance carries with it an expectation that there will be clear rules to control the use of surveillance and ensure fair treatment of surveillance subjects. These rules are necessary because secrecy can provide the opportunity and temptation for abuse. And technology, no matter how sophisticated, magnifies the risk that erroneous information will be gathered and disseminated. Ordinarily, fair information practices provide for the right to know what information is being collected about oneself and ask for it to be corrected if it appears to be wrong. Secret surveillance, as an exception, denies people that opportunity.

1 In this chapter, we refer to surveillance for the purpose of national security and law enforcement rather than for public health and other public interest purposes.

2 In October 2004, however, the Canadian government approved the use of biometric facial data on passports. Glen McGregor, "Biometric Passports Approved" *Victoria Times-Colonist* (6 October 2004) A-1.

Fair Play and Power

Unfortunately, legal protections can lag behind technology. While anti-terrorism laws may have been evaluated before being passed, technological changes surrounding or proceeding independent of these policy changes are rarely subjected to the deliberation and review that govern legal changes. This creates an increased risk of unanticipated and adverse social outcomes.[3] The more complex technological systems become, the more likely they are to shape society rather than be shaped by it. The longer fear of terrorism persists, the easier it may become to forget the rules of fair play.

This is not to say that rules are frequently abused, but every breach that comes to light understandably contributes to public anxiety about lapses or misdeeds that may occur but never be revealed. This was illustrated recently by the findings of an internal RCMP investigation into the treatment of Canadian citizen Maher Arar. The Garvie report found that an RCMP-led intelligence unit had cut corners, ignored rules and lacked the expertise to deal with complex national security cases. The report concluded that the RCMP had provided US authorities with unreliable information that appears to have resulted in Arar's deportation to Syria and imprisonment in a military intelligence prison.[4]

Meaningful, independent, oversight of surveillance activities is therefore needed to ensure that government agencies' desire to know is carefully balanced against individual rights to privacy. Independent oversight is one thing that distinguishes free societies from their totalitarian counterparts. Oversight cannot prevent errors from occurring, of course, but it can at least set reasonable limits on the circumstances and manner in which surveillance is conducted.

Setting limits on surveillance for national security purposes is vital in light of what one expert has suggested is, historically, the irresistible temptation to use the tools of surveillance and control for internal, and often political, purposes:

> National security, or national *in*security to be more precise, is an anxiety that afflicts states across the ideological spectrum. Intelligence in the service of domestic political policing has been used by governments of all persuasions, and every type of state has relied at least from time to time on secret or political police against the perceived threat of subversion, if not revolution.… [H]owever different the texture of domestic Intelligence in different regimes, it is the universality of the phenomenon in the twentieth century that is most arresting. The tools for internal surveillance and control being available, no state has resisted the temptation to use them, and few have not attempted to refine the tools yet further. States with many external and internal enemies, real and potential, have often used these tools recklessly and brutally; states with higher degrees of domestic consensus have most often used the tools with greater restraint, discretion, and skill, usually during periodic bouts of national or state insecurity. Such relative restraint, however, has served to mask the negative effects of secret political policing on the practice of liberal democracy.
>
> Fears for internal security and of enemies within tend to be sparked in the first instance by international insecurity. The pathologies of counterintelligence, described above, are intimately linked to the perception of the enemy within as an insidious extension of the enemy without. The "fifth columnist," the spy, the saboteur, the foreign-directed terrorist or subversive: these are images that draw their menace, and fascination, from the blurring of Inside and Outside, of Us and Them. The Cold War image of "reds under the bed" captures this anxiety indelibly. Xenophobia, ideology, and sexual/cultural panic all reinforced one another.[5]

3 Arthur J. Cockfield, "The State of Privacy Laws and Privacy-encroaching Technologies after September 11: A Two-year Report Card on the Canadian Government" *University of Ottawa Law and Technology Journal 1* (2003-2004) 327 at 337.
4 Jeff Sallot, "Mounties Bungled Arar File" *The Globe and Mail* (25 September 2004) at A-1.
5 Reg Whitaker, *The End of Privacy: How Total Surveillance Is Becoming A Reality* (New York: New Press, 1999) at 19-20.

Substantive discussion is, in our view, needed about the privacy implications of our present focus on national security and law enforcement, so that meaningful privacy protections are guaranteed in the face of new technologies, techniques and government activities in the name of security and freedom. At the very least, this exercise is necessary because of the post-September 11 expansion of legal authority for state surveillance and the increasingly blurred lines between powers under national security laws and those under criminal laws.

Observing the Rule of Law

The question of where to strike the balance between common-sense precautions against terrorism and checks on our basic liberties is one of the most vexing questions we face today. As the Supreme Court of Canada noted earlier this year, achieving an appropriate balance depends above all on maintaining respect for the rule of law, especially as it applies to the protection of fundamental liberties:

> The challenge for democracies in the battle against terrorism is not whether to respond, but rather how to do so. This is because Canadians value the importance of human life and liberty, and the protection of society through respect for the rule of law. Indeed, a democracy cannot exist without the rule of law. So, while Cicero long ago wrote "*inter arma silent leges*" (the laws are silent in battle): Cicero, *Pro Milone* 14, we, like others, must strongly disagree: see, A. Barak, "Foreword: A Judge on Judging: The Role of a Supreme Court in a Democracy" (2002), 116 Harv. L. Rev.16, at p. 150-51.
>
> Although terrorism necessarily changes the context in which the rule of law must operate, it does not call for the abdication of law. Yet, at the same time, while respect for the rule of law must be maintained in the response to terrorism, the Constitution is not a suicide pact, to paraphrase Jackson J.: *Terminiello v. Chicago*, 337 U.S. 1 (1949), at p. 37 (in dissent).
>
> Consequently, the challenge for a democratic state's answer to terrorism calls for a balancing of what is required for an effective response to terrorism in a way that appropriately recognizes the fundamental values of the rule of law. In a democracy, not every response is available to meet the challenge of terrorism. At first blush, this may appear to be a disadvantage, but in reality, it is not. A response to terrorism within the rule of law preserves and enhances the cherished liberties that are essential to democracy. As eloquently put by President Aharon Barak of the Israeli Supreme Court:
>
> > This is the fate of democracy, as not all means are acceptable to it, and not all methods employed by its enemies are open to it. Sometimes, a democracy must fight with one hand tied behind its back. Nonetheless, it has the upper hand. Preserving the rule of law and recognition of individual liberties constitute an important component of its understanding of security. At the end of the day, they strengthen its spirit and strength and allow it to overcome its difficulties.[6]

In both Canada and the US, anti-terrorism laws were passed in 2001 with great haste, spurred by the perception of imminent national danger. Given the circumstances at the time, it is not surprising that protecting civil liberties was not the highest priority for legislators. Three years later, however, it is time to take stock and to consider to what degree privacy and security are complementary goals and what protections for civil liberties need to be in place if concerns about terrorism persist and intensive surveillance continues indefinitely.

Social Impacts of Secret Surveillance

Secret surveillance may be necessary in well-defined circumstances but, if taken too far, threatens freedoms on which successful democracy depends. Awareness of widespread surveillance makes people nervous about speaking their minds, engaging in possibly unpopular political or social activities or

6 *Application Under s. 83.28 of the Criminal Code (Re)*, [2004] S.C.J. No. 40, 2004 SCC 42.

Surveillance Excesses: Lessons from East Germany

British writer Timothy Garton Ash found out first-hand about errors in secret files. After the fall of the Berlin Wall, the legislature of the reunited Germany passed a law allowing access to the files of the Stasi, the former East German secret police. Having lived in East Germany from 1979 to 1981, Ash was curious about what his Stasi file might contain and travelled to Berlin to have a look. Much to his bemusement, the file was riddled with erroneous details about his activities, which had been provided by state informants instructed to keep an eye on him. In his memoir, *The File*, Ash comments on an entry in his Stasi file in which an informer recounts a conversation with him. Ash consults his diary entry for the conversation and concludes that, even though the Stasi file "basically rings true", it is inaccurate on some important details:

> This passage [in the Stasi file] illustrates how small distortions creep into the Stasi records …. Now suppose for a moment that the content of this passage were altogether more serious and compromising; suppose that the interpretation of the whole passage hinged—as it sometimes can—on the one word; suppose I had subsequently become a prominent East German politician; and suppose that I woke up one morning to find the passage quoted against me as a headline in a West German tabloid: quote unquote. Calls for resignation follow. Who would believe me when I protested: "No, I didn't say that! Well, not *exactly*. And anyway, they've got the date wrong. And the title of *The Spectator*. And the spelling of my name."[7]

Ash notes that, "wherever there has been a secret police, not just in Germany, people often protest that their files are wholly unreliable, full of distortions and fabrications".[8]

The East German Stasi recruited as many as one in every 50 citizens to spy and report on other citizens. Ash was able to be almost light-hearted in reporting the misinformation in his file, much of which had been provided by people he thought of as friends but who were also informants. East German citizens, on the other hand, did not have the good fortune to be visitors like Ash.

In 2002, the US Department of Justice announced the creation of the Terrorism Information and Prevention System (TIPS), after President Bush had called for it in his State of the Union address. Described as "a national system for concerned workers to report suspicious activity", the program would have recruited "millions of American truckers, letter carriers, train conductors, ship captains, utility employees and others" as government informants. The pilot program alone would have recruited one in every 24 Americans, in just 10 major cities, to report each other's "suspicious activities". The proposal was later shelved following public concern and unease in Congress, but the US government continues to run several programs that are similar to TIPS.[9] Although there is no information to suggest that Canadian authorities employ informants on a wide-scale basis, Ash's experience is worth remembering.

Large-scale informant programs may be useful for rooting out "suspicious activities", but one of their shortcomings is that harmless citizens may pay a price if a neighbour holds a grudge or their eccentric but harmless behaviour is considered by the fearful or merely intolerant to be abnormal.

7 Timothy Garton Ash, *The File* (New York: Random House, 1997) at 29-30.
8 *Ibid*. at 22.
9 Jay Stanley, "The Surveillance-Industrial Complex: How the American Government is Conscripting Businesses and Individuals in the Construction of a Surveillance Society" (New York: American Civil Liberties Union, 2004) at 3.

doing anything that might arouse suspicion. As David Flaherty has written, "the existence of dossiers containing personal information collected over a long period of time can have a limiting effect on behaviour; knowing that participation in an ordinary political activity may lead to surveillance can have a chilling effect on the conduct of a particular individual".[10]

Excessive surveillance in the name of national security has the effect of herding people towards conformity and discouraging the individual autonomy and diversity that free societies need to flourish. Surveillance tends to single out people or groups perceived to be "different", often with grave impacts—especially when the product of surveillance is misleading or wrong information about a person. Even if many of us will never trigger the surveillance radar, as citizens we have a responsibility to look beyond ourselves and consider how others could suffer because they may attract surveillance—in some cases because of who they are, not what they might have done. If, in our vigilance against the threat of terrorism, we lose respect for others' civil liberties, we risk losing the right to call ourselves a free democracy.

No Fly Lists and Secret Mistakes

Hundreds of innocent people have found their names on no fly lists in the past couple of years because surveillance of their personal information in data banks has turned up 'false positives'. The frequency of mistakes that affects the lives of ordinary people reveals the need for careful regulation of secret surveillance.

One of the primary focuses of the "war on terrorism" has been the risk to air travel. The dilemma posed by no fly lists for national security authorities is that respecting people's privacy could reduce the likelihood of weeding out suspicious flyers. The dilemma for travellers is that intensive and widespread scrutiny of data banks, apart from its intrusiveness, increases the risk of errors that can have both immediate and lasting impacts on people's lives. People also worry that collections of information about them, synthesized for the purpose of keeping terrorists off planes, may prove too convenient to be limited to one purpose and may be permanently filed or shared for other uses, a phenomenon known as function creep.

Not surprisingly, the likelihood of error in no fly lists is magnified for people whose names are common. US Senator Edward Kennedy, a familiar figure internationally, found this out the hard way when he was prevented from boarding planes in the US on several occasions this year. Unfortunately for him, the name "T. Kennedy" had been used as an alias by someone on the list of terrorist suspects.[11] Senator Kennedy was able to fly after all because he is well known and influential. Many others have not been so lucky. Their stories are largely unknown because people are naturally reluctant to broadcast the fact that, rightly or wrongly, they have been the target of law enforcement or national security scrutiny.

In July 2004, citing privacy concerns, US Homeland Security Secretary Tom Ridge announced that security leaders had scrapped plans to implement the Computer Assisted Passenger Prescreening System II (CAPPS II) in the US.[12] A Department of Homeland Security spending bill approved by the US Senate in September 2004 prohibits further funding

10 David Flaherty, *Protecting Privacy in Surveillance Societies* (Chapel Hill: University of North Carolina Press, 1989) at 9.

11 Sara Kehaulani Goo, "No Fly List's 'T. Kennedy' Irks Senator" *The Washington Post* (20 August 2004), available online at www.seattletimes.nwsource.com.

12 USA Today (14 July 2004). CAPPS II would have rated every airline passenger according to terrorist risk level based on compulsorily provided personal information and information from other sources. CAPPS II was criticized because, among other things, although it was justified on anti-terrorism grounds, it was also going to be used for ordinary law enforcement purposes. Since this announcement, a similar program—known as Secure Flight—has been announced.

for CAPPS II pending the implementation of a system of due process for passengers prohibited from flying, assurance of a low risk of false positives arising from the use of government and private databases and effective oversight provisions.[13]

Transport Canada acknowledged in September 2004 that it is negotiating with Canadian air carriers to compile a Canadian no fly list, as contemplated by the new Public Safety Act passed by Parliament in May 2004.[14] The Information and Privacy Commissioner of British Columbia recently expressed concern to the federal Privacy Commissioner that the proposal appears to include no plan to implement basic fair information practices:

> One major concern is that we do not know what criteria will be used to place individuals on the no fly list. Nor do we know what steps if any will be taken to minimize confusion between individuals with the same or similar names. It is an accepted principle of fair information practices, of course, that an organization must take reasonable steps to ensure that personal information it uses to make a decision affecting an individual is accurate and complete.
>
> Another critical component of any meaningful privacy protection scheme, of course, is the ability for individuals to gain access to their own personal information and to have the opportunity to correct mistakes. The available information suggests Transport Canada does not intend to honour this basic principle of privacy protection.
>
> Ordinary Canadians who are barred from flying—for pleasure or for their livelihoods—at the very least should have the assurance of a timely, free and effective redress mechanism respecting any Canadian no fly list. They must be able to challenge their no fly status with the prospect that errors will be corrected promptly and, if they are not, be subject to challenge on appeal. Transport Canada's reported plan to allow such individuals to write to the Minister of Transport for an explanation is woefully inadequate.[15]

Governments faced with grave dangers may need to take decisive steps to minimize risk. Nevertheless, it is important that civil liberties not be degraded or lost in the process. Security initiatives and fair information practices are not contradictory terms. More openness about the criteria used to compile 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 continuing respect for their civil rights as it does on their confidence in public safety.

Privacy is a subtle right, one that until recently rarely made the news. Everyone understands the meaning of security threats because the consequences of inaction may be dramatic. But you may never notice the loss of privacy until it directly affects your own livelihood or your freedom of expression or movement.

Why Care About Surveillance?

People may think they have nothing to hide, but if they have no idea what the state thinks it knows about them, this cockiness can in a surveillance society be fatally misplaced. As Russian writer Alexander Solzhenitsyn said:

> As every man goes through life he fills in a number of forms for the record, each containing a number of questions. A man's answer to one question on one form

13 US, Bill H.R. 4567, Department of Homeland Security Appropriations Act, 2005, 108th Cong. 2005, S.514. Previous US pressures to draw other countries into CAPPS II revived earlier tensions between Europe and the US over privacy protection and led to divisions within the European Union over balancing privacy against national security. In June 2004, European Parliament President Pat Cox announced that the Parliament would seek to annul the May 2004 agreement, signed by the US and the European Commission, requiring airlines to transfer passenger personal information to the US Department of Homeland Security. Cox warned against the growing pervasiveness of a "new form of creeping extraterritoriality."

14 Jane Taber, "Ottawa compiles 'no-fly' list of banned passengers" *The Globe and Mail* (3 September 2004) A-1.

15 Correspondence from David Loukidelis, Information and Privacy Commissioner for British Columbia, to Jennifer Stoddart, Privacy Commissioner of Canada, 8 September 2004.

> becomes a little thread, permanently connecting him to the local center of personnel records administration. There are thus hundreds of little threads radiating from every man, millions of threads in all.... They are not visible, they are not material, but every man is constantly aware of their existence. The point is that a so-called completely clean record was almost unattainable, an ideal, like absolute truth. Something negative or suspicious can always be noted down against any man alive. Everyone is guilty of something or has something to conceal. All one has to do is to look hard enough to find out what it is. Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads ... and for these people's authority.[16]

Solzhenitsyn was writing about the time of handwritten notes and index cards. Much later, Colin Bennett noted the concern that "information technology could become a tool of tyranny" because it so enhances the power of government to collect and manipulate vast quantities of information about individual citizens. It is important to remember, he noted, that citizens' interests in privacy may cause them to limit state use of information if it becomes too intrusive, although it is much easier to place one's faith in government to do the right thing. This is the problem that everyone faces—whether to assume that those "in authority" know best and leave it up to them or whether to scrutinize and question state use of information and whatever safeguards exist to deter abuses.

Trends in privacy polls suggest that Canadians and Americans alike are becoming less accepting of private sector privacy invasions—though they may feel helpless to do anything about it. But they do not really know what to make of increasing government surveillance. Overall,

> most people share a basic sense that there is a zone of private life that deserves some kind of protection, about which we have some kinds of claim to influence how far others can come to know about us or even rule out certain things, if we wish to. In short, people share—although in differing degrees about different issues—a sense that there are certain *risks to privacy* that are worth being concerned about.[17]

Still, some people take the view, "I don't see why I or my family would be of any interest, so why should I worry about surveillance?" Others might think, "I don't care if they watch me or have my information, I've got nothing to hide."

As more of our personal information is stored electronically and is kept for longer and longer, our past actions are more likely to linger in the digital shadows and emerge eventually to haunt us. As our personal information survives for longer periods, social attitudes or laws can change, transforming youthful embarrassments into adult faults in the eyes of others.

A law-abiding, middle-aged man who loudly denigrates privacy by saying he has nothing to hide and thus nothing to fear should, logically, have no objection to his entire health history and professional history being available to anyone who asks. If a mortgage lender denies him a loan because the lender learns he lost his last job for incompetence and he now has prostate cancer, how could he object?

What if the information about why he lost his job is wrong? The streams of data about each of us are frequently muddied with little or not so little mistakes resulting from lack of diligence or human error. With the flow of information about consumers (whether of goods, insurance or health care) between private and government data banks, identical information about individuals may be accessible to them in one place, and subject perhaps to correction, yet secret and virtually incapable of being corrected in another. It takes a very

16 Alexander Solzhenitsyn, *Cancer Ward* (New York: Farrar, Straus and Giroux, 1969) at 192 (quoted in Colin J. Bennett, *Regulating Privacy*: *Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1992) at 30-31). As David Flaherty has observed, the storage of "personal data can be used to limit opportunity and to encourage conformity": *supra* note 10 at 9.

17 Perri 6, *The Future of Privacy*, Vol.1 (London: Demos, 1998) at 39.

persistent person to find out about and seek to correct mistakes embedded in the data, assuming he or she is allowed access to his own information (which is almost impossible with terrorist watch lists and other national security information).[18]

Informational privacy has been described as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others",[19] but, as Ann Cavoukian and Don Tapscott have written, the most important question may be not "What do I have to hide?" but "Why do they need to know and what will they use it for?"[20]

A 1993 editorial in *The Globe and Mail* reminded its readers of the essence of the state-citizen relationship:

> The state is the creation of a self-governing people. We do not have such rights as the state allots us; rather, it has such powers, and only such powers, as we consent to give it. All rights not expressly limited are reserved to the people; all powers not expressly granted are denied. It is never incumbent on the people to show why they should have rights; the burden of proof is always on those who would restrict them.[21]

This applies with great force to the creation and use of secret powers by the state. Most people have no idea of the scope or methodology of government surveillance. This means that we are, as a nation, ill-equipped to make informed decisions about how to achieve an appropriate balance between the desire of governments and law enforcement agencies to collect and use personal information and the desire of most people to enjoy private lives. This is all the more reason why it is always incumbent on government, not only to explain the rationale for new surveillance powers, but to implement them only where there is a clear and pressing need for them and in a manner that intrudes on our rights and freedoms civil liberties to the least extent possible.

Conclusion

Since 2001, both the United States and Canada have increased the intensity and breadth of surveillance to detect and deter terrorist activities. New technologies for gathering and analyzing data have increased both the sophistication and the scope of surveillance. Laws to ensure the protection of privacy rights require careful deliberation and review, but advancing technology doesn't always provide that opportunity. Clear rules regarding fair information practices are needed because secret surveillance provides opportunities for abuse and errors can have serious impacts on individuals.

Adequate justification must be provided for the use of secret surveillance whenever it occurs in a democratic society and adequate safeguards must be attached to deter abuses and protect the rights of citizens who may be affected by its use. Canadian governments should carefully assess existing and proposed surveillance activities, laws and technologies to ensure they are appropriate and subject to meaningful controls and independent oversight.

In Chapters 6 and 7, we turn our attention to the legal basis for surveillance under new anti-terrorism laws in the United States and Canada. We also look at the processes the two countries use for sharing or accessing personal information across borders for intelligence purposes or the prosecution of offences.

18 As an example, Clayton Ruby, the well-known civil rights lawyer, has for years struggled in vain to see his CSIS security file, with a trip to the Supreme Court of Canada being of relatively little assistance: *Ruby v. Canada (Solicitor General)*, [2000] 4S.CR.3.
19 Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967) at 7.
20 Ann Cavoukian & Don Tapscott, *Who Knows: Safeguarding Your Privacy in a Networked World* (Toronto: Vintage Canada, 1995) at 21.
21 *The Globe and Mail* (11 December 1993), quoted in Cavoukian & Tapscott *ibid*. at 16.

6 ANTI-TERRORISM LAWS IN THE US

USA-Canada: Distinction with a Difference

The USA Patriot Act has ten parts, known as Titles, and is largely a compilation of changes to numerous existing US laws. These include the Electronic Communications Privacy Act, the Immigration and Nationality Act, the Right to Financial Privacy Act and the Foreign Intelligence Surveillance Act (FISA). Section 215, in Title II of the USA Patriot Act, amended the FISA provisions that empower the US Foreign Intelligence Surveillance Court (FIS Court) to issue secret orders to enable the FBI to obtain records from third parties.

Some submissions to us, notably that of the Information Technology Association of Canada (ITAC), contend that it is only problematic for a FISA order to reach into British Columbia if the confidentiality attaching to the information involved is "degraded" as a result. ITAC says this would not occur because the substance of the legislative amendments introduced by Canada's Anti-terrorism Act[1] is comparable to that of the USA Patriot Act. ITAC states:

> Underlying the opposition to exposing personal information to the reach of the Patriot Act is an assumption that exposing personal information to potential disclosure under the Patriot Act degrades the confidentiality attaching to it, and is accordingly something in respect of which public bodies must take additional preventative measures in order to comply with s. 30 of FOIPPA. This is not necessarily so … personal information that is not subject to an order under the Patriot Act—whether it remains within public or private custody—is still subject to disclosure in the public interest in many of the same circumstances contemplated by those provisions.
>
> Indeed, the *Patriot Act* itself is not necessarily exceptional legislation. It has counterparts in other jurisdictions (including Canada), each of which has sought to balance the fundamental public values of security and privacy in a world wracked by gathering threats of terrorism.[2]

The unilateral extension of a FISA order to information in British Columbia is both offensive to Canadian sovereignty and contrary to our reasonable expectations that Canadian constitutional protections and rights under FOIPPA will apply to the personal information—particularly intimate details of our lives and lifestyles—that we entrust to public bodies in British Columbia in order to benefit from public services such as medical care. The ITAC perspective fails to recognize these concerns. They are not addressed by observing that an order made under US law is similar to an order that might be made under Canadian law.

The ITAC perspective also overlooks the fact that the implications for privacy of the USA Patriot

1 Anti-terrorism Act, S.C. 2001, c. 41.
2 Submission of Information Technology Association of Canada (28 May 2004) p. 26.

Act and Canada's Anti-terrorism Act are controversial in both countries. The changes to the law made by these statutes remain largely untested in both US and Canadian courts, and it is entirely possible that apparently comparable provisions—such as a particular search or seizure power—could be found constitutionally valid in the US but not in Canada.

We agree, however, that both the text of section 215 of the USA Patriot Act and the wider context of developments in foreign intelligence gathering and international anti-terrorism legislation, notably in the US and Canada, are relevant to capturing the concerns communicated to us about the implications of the USA Patriot Act for the security of personal information of British Columbians.

In this chapter and the next, we will describe the nature of intelligence gathering and its relationship to personal privacy and information technology. We will discuss how previous distinctions between intelligence gathering and law enforcement have become blurred by fairly recent evolution in the means and purposes of foreign intelligence gathering and how this may imperil privacy and other democratic values in the US and Canada.

In this chapter, these matters will be discussed in relation to two US laws—FISA and the USA Patriot Act. We will examine the text of section 215 and, briefly, two other provisions, then set out the sharp division of opinion in the US about the USA Patriot Act. In Chapter 7, we will describe developments relating to three Canadian laws—the Canadian Security Intelligence Service Act,[3] the Anti-terrorism Act[4] and the Public Safety Act[5]—and the Canadian reaction to those measures.

Intelligence and Privacy

The July 2004 Butler report[6] to the British House of Commons, *Review of Intelligence on Weapons of Mass Destruction,* described the nature of intelligence as compared to other types of information:

> Governmental decisions and actions, at home and abroad, are based on many types of information. Most is openly available or compiled, much is published, and some is consciously provided by individuals, organizations or other governments in confidence. A great deal of such information may be accurate, or accurate enough in its own terms. But equally much is at best uninformed, while some is positively intended to mislead. To supplement their knowledge in areas of concern where information is for one reason or another inadequate, governments turn to secret sources. Information acquired against the wishes and (generally) without the knowledge of its originators or possessors is processed in collation with other material, validation, analysis and assessment and finally disseminated as 'intelligence'. To emphasise the point, the term 'secret intelligence' is often used (as, for instance, enshrined in the title of the Secret Intelligence Service), but in this Review we shall use the simple word 'intelligence'.[7]

The Butler report described intelligence gathering as

> painstaking work, involving the piecing together over extended timescales of often fragmentary information. There are the surprises and 'lucky breaks'. But they often come from the foundation of knowledge developed over several years. It requires the close collaboration between all involved, in agencies and departments, to build the jigsaw, with teams available to have access to available intelligence and make the most of each clue.[8]

[3] Canadian Security Intelligence Service Act, R.S.C. 1985, c. C-23.
[4] Anti-terrorism Act, *supra* note 1.
[5] Public Safety Act, 2002, S.C. 2004, c. 15.
[6] UK, Report of a Committee of Privy Counsellors, *Review of Intelligence on Weapons of Mass Destruction (Return to an Address of the Honourable the House of Commons),* Chairman, the Rt Hon the Lord Butler of Brockwell, (London: The Stationery Office, 14 July 2004). The report is available on the website of the Butler Review Committee: www.butlerreview.org.uk
[7] *Ibid*. p. 7, para. 21.
[8] *Ibid*. p. 149, para. 2.

The Butler report also described the most important limitations on intelligence as its incompleteness, the fact that "intelligence seldom acquires the full story" and that "it can be incomplete in undetectable ways".[9]

Many details of ordinary people's lives—as reflected in their consumer, financial and other day-to-day recorded transactions and activities—are spread far and wide through private and government data banks. Intelligence gathering, whether it is aimed at protecting national security or at fighting organized crime, is distinguished by secrecy—of collection, collation with other information, validation, analysis, assessment, use and further disclosure. It is both profoundly invasive of personal privacy and inherently primed to exploit large-scale private and government collections of personal information and advanced technologies for surveillance, data collection and manipulation. Intelligence gathered about the individual is likely to be incomplete and is not subject to verification or challenge by the individual.

Intelligence gathering is more extensive in totalitarian than in democratic societies—in large part because surveillance in totalitarian societies focuses as much on citizens of the state as on the activities of foreign agents. The threat of terrorism has provided a catalyst, however, for increased domestic surveillance in North America and elsewhere that threatens to blur the lines between intelligence gathering and law enforcement in countries with strong democratic traditions.

The real danger is that powers of intrusion are widened for one reason (to address threats to national security) but end up being commonly used for other reasons (to conduct regular domestic law enforcement searches or seizures). Information gathering is justified for one reason (control of border entry) but ends up being used for other reasons (to track individuals for generalized law enforcement objectives).

The risk is that civil liberties which in a democratic society we expect will only be set aside, even temporarily, in response to the most extraordinary national emergencies, end up being set aside all the time; that it becomes a routine matter to set them aside for the innocent, suspect and guilty alike, for serious or mundane law enforcement activities or, worse yet, for arbitrary reasons. When this happens, the traditional law enforcement restraints we have come to rely upon to protect us from disproportionate action by the state against disfavoured groups, or based on incomplete or mistaken information, are not there.

Blurring the Lines: National Security and Law Enforcement

There used to be a clearer distinction between national security and law enforcement measures. Law enforcement, while broadly describing measures to ensure compliance with statutes, is more commonly understood to deal with maintaining public order and safety through the enforcement of criminal or like laws. National security measures describe the approach taken by states to ensure their security and survival against perceived external or internal threats. A Canadian example of the latter was the 1970 "October crisis" in Quebec that led to implementation of the War Measures Act and the suspension of civil liberties. Intelligence gathering is generally conducted for the purpose of strengthening national security. Anti-terrorism measures deal with a specific type of threat to public safety and national security.

Until the last few years, terrorism was generally seen as a phenomenon that plagued certain other parts of the world but not North America. Terrorism is now perceived as such a severe threat that governments consider it necessary to grant extraordinary powers

[9] *Ibid*. p. 14, paras. 49-50.

to agencies of the state to detect and deter terrorist activities. While extraordinary powers may be necessary, they need to be very well defined to ensure both that they are clearly linked to the objectives for which they are created and that they are not abused by being applied to activities that have nothing to do with terrorism. As mentioned earlier, one of the defining characteristics of police states is the blurring of distinctions between law enforcement and national security functions, such that the rule of law eventually gives way to arbitrary decision-making by law enforcement authorities and the rights of ordinary citizens lose meaning. Democracies depend upon clear and effective rules that are suited to the state activities they are intended to govern and that reflect the essential values of a free society.

Since September 11, governments in several countries have passed laws and have authorized activities that blur the line between national security laws and activities and ordinary law enforcement.[10] The USA Patriot Act does so, in part, under the expanded surveillance powers described in Title II. A US Department of Justice report states that one of the effects of the USA Patriot Act has been to tear down the "wall" that previously separated law enforcement and intelligence gathering activities. The report details the great extent to which USA Patriot Act provisions have been used in ordinary criminal investigations and how effectively they have expedited surveillance in a myriad of circumstances, only some of which are terrorism related.[11]

In another example, a 2002 decision of the US Foreign Intelligence Surveillance Court of Review, on appeal from the FIS Court, confirmed that the FBI now has greater flexibility under US Department of Justice guidelines and the USA Patriot Act to share information that is gathered through national security activities for ordinary law enforcement purposes.[12] Reports from the US suggest that the special USA Patriot Act powers and offences are indeed being used in ordinary criminal cases. A recent news report indicated that several Canadians suspected of smuggling money into Canada in exchange for marijuana have been charged with bulk cash smuggling under anti-terrorism provisions enacted by the USA Patriot Act.[13]

In Canada, amendments to the Customs Act and regulations authorize Canadian border officials to require private sector organizations to provide border officials with extensive advance information about arriving passengers.[14] These changes expanded our government's ability to use and share that information, not only for national security purposes, but also for ordinary law enforcement and other purposes, including (according to government statements in 2002) public health surveillance. The information sharing authority includes a broad ability to share personal information about Canadians and others with the US and other foreign governments. The amendments do not restrict information sharing arrangements to national security uses—they could easily include ordinary law enforcement or other purposes defined on a case-by-case basis or in an agreement.[15]

[10] The Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135, an extensive piece of legislation in its own right, also supplemented the USA Patriot Act by bringing together 22 stand alone agencies under the umbrella of the new Department of Homeland Security. The Department of Homeland Security does not have investigatory or prosecution powers outside of its component agencies, but it does have significant authority under the Homeland Security Act of 2002 to access, receive and analyze law enforcement, intelligence and other information from federal, state and local government agencies and private sector entities (see §§ 201 and 202).

[11] U.S. Department of Justice, *Report from the Field: The USA Patriot Act at Work* (July 2004), at 2, 3, 5. The report is available on the website the U.S. Department of Justice hosts on the USA Patriot Act: www.lifeandliberty.gov.

[12] *In re Sealed Case*, 310 F.3d 717 (Foreign Intell. Surv. Ct. Rev. 2002).

[13] "U.S. Patriot Act used in pot case" *CBC News, British Columbia News Online* (webposted 05 Aug 2004), www.cbc.ca; David Ticoll, "U.S. Patriot Act's reach is a concern for Canadians" The Globe and Mail (14 October 2004) B13.

[14] Customs Act, R.S.C. 1985 (2d Supp.), c. 1, s. 107.1, as am. by S.C. 2001, c. 25, s. 61. The Passenger Information (Customs) Regulations, SOR/2003-219, require commercial carriers, travel agents and reservation system operators to provide information disclosing the name, birth date, sex, nationality, travel documentation, reservation number and any information about a traveller that happens to be in a reservation system.

[15] Informative opinions by Hon. Gérard V. La Forest, C.C., Q.C., retired Supreme Court of Canada justice (November 12, 2002) and by Roger Tassé, O.C., Q.C. (November 21, 2002) about federal government proposals for a passenger name record database on the foreign travel activities of Canadians, enabled by section 107.1 of the Customs Act, are available on the website of the Privacy Commissioner of Canada: www.privcom.gc.ca.

Origin and Goals of the US Foreign Intelligence Surveillance Act

The US Supreme Court, in cases in the 1960s and 1970s, hinted that the executive branch of the US federal government had greater leeway to engage in spying on foreign agents than might be permissible under the US Constitution in relation to US persons. In *Katz v. United States,*[16] the court found that the Constitution's Fourth Amendment protection against unreasonable searches and seizures extended to electronic surveillance of communications. The court added, however, that this conclusion did not extend to cases involving national security. In *United States v. United States District Court,*[17] the court held that the Fourth Amendment to the US Constitution required prior judicial approval for domestic intelligence gathering for national security purposes[18] and effectively invited Congress to legislate in this area:

> We recognize that domestic surveillance may involve different policy and practical considerations from the surveillance of "ordinary crime." …
>
> Given these potential distinctions between … criminal surveillances and those involving domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes…. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection …
>
> It may be that Congress, for example, would judge that the application and affidavit showing probable cause need not follow the exact requirements [prescribed for criminal surveillance] but should allege other circumstances more appropriate to domestic security cases; that the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court ... ; and that the time and reporting requirements need not be so strict ….[19]

In 1976, a US Congressional committee, chaired by Senator Frank Church, reported on the Watergate, Pentagon Papers and other domestic spying scandals. The committee identified examples of abuses by the FBI and others in spying on Americans.

The 1978 enactment of FISA was in many ways the culmination of these developments in the courts and Congressional investigation of US intelligence activities. FISA was an attempt to place controls on intelligence activities. It authorized electronic and physical searches for the purposes of gathering "foreign intelligence information" and set out procedures, including obtaining court approval, to be followed in undertaking those activities.

Prior to the enactment of FISA, US government intelligence agents had to obtain warrants to conduct searches and wiretap phones. While this requirement remained, the traditional demand for some evidence of potential criminal activity was dropped. Instead, the principal requirements shifted to a showing of probable cause that the surveillance target was the agent of a foreign power, as well as government certification that the purpose of the surveillance was to obtain foreign intelligence information.

FISA also created the Foreign Intelligence Surveillance Court (FIS Court) and set out that court's powers in relation to searches and seizures. Its members are US federal judges whom the Chief Justice of the US appoints to sit on the FIS court. The FIS Court conducts all of its proceedings in secret and, with only two exceptions in 2002, has not published its rulings. Its sole purpose is to review requests by

[16] *Katz v. United States*, 389 U.S. 347 (1967).
[17] *United States v. United States District Court*, 407 U.S. 297 (1972).
[18] The court did not touch on the President's surveillance power respecting the activities of foreign powers inside or outside the US.
[19] *United States v. United States District Court*, *supra* note 18 at 322-323.

the Justice Department for warrants related to foreign intelligence investigations. Between 1979 and 2001, it is estimated, the FIS Court approved all but five of more than 14,000 warrant requests.[20]

The guiding principle behind FISA was that, since foreign intelligence work is aimed at protecting national security and has no bearing on domestic law enforcement, the restrictions on government activities should be somewhat looser. It has been described this way:

> The FISA provides a statutory framework for electronic and other forms of surveillance in the context of foreign intelligence gathering. These types of investigations give rise to a tension between the government's legitimate national security interests, on the one hand, and, on the other hand, constitutional safeguards against unreasonable government searches and seizures and excessive government intrusion into the exercise of free speech, associational, and privacy rights. Congress, through legislation, has sought to strike a delicate balance between national security and constitutionally protected interests in this sensitive arena.[21]

The scope of FISA originally was limited to electronic surveillance but, in 1995, was expanded to allow orders for "seizure of certain records".[22] Then, in 2001, the USA Patriot Act amended FISA to include gathering terrorism related intelligence. It also widened the grounds and further lowered the bar for the issuance of FISA orders that enable the FBI to obtain records and things from third parties.

A Snapshot of the USA Patriot Act

Following September 11, both US Houses of Congress moved quickly to pass the USA Patriot Act and President Bush signed it into law on October 26, 2001. USA Patriot Act is an acronym for the formal title: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act) of 2001. The broad scope of the USA Patriot Act is captured in the following description in its preamble: "An Act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes."

A report from the US Congressional Research Service summarizes the main provisions of the USA Patriot Act as follows:

> The Act eases some of the restrictions on foreign intelligence gathering within the United States, and affords the U.S. intelligence community greater access to information unearthed during a criminal investigation, but it also establishes and expands safeguards against official abuse. More specifically, it:
> - permits "roving" surveillance (court orders omitting the identification of the particular instrument, facilities, or place where the surveillance is to occur when the court finds the target is likely to thwart identification with particularity);
> - increases the number of judges on the FISA court from 7 to 11;
> - allows application for a FISA surveillance or search order when gathering foreign intelligence is *a significant* reason for the application rather than *the* reason;
> - authorizes pen register and trap & trace device orders[23] for e-mail as well as telephone conversations;
> - sanctions court ordered access to any tangible item rather than only business records held by lodging, car rental, and locker rental businesses;
> - carries a sunset provision;
> - establishes a claim against the U.S. for certain

[20] Stephen J. Schulhofer, "No Checks, No Balances: Discarding Bedrock Constitutional Principles" in Richard C. Leone and Greg Anrig Jr., eds., *The War on Our Freedoms: Civil Liberties in an Age of Terrorism* (New York: PublicAffairs, 2003) 74 at 81.

[21] Senators Patrick Leahy, Charles Grassley & Arlen Specter, *Interim Report on FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures,* (February 2003) at 3-4; the report is available on the website of the Federation of American Scientists: www.fas.org.

[22] For an extensive review of FISA, see Elizabeth B. Bazan, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions* (CRS Report for Congress, 2003); the report is available on the website of the Federation of American Scientists: www.fas.org.

[23] Pen registers are surveillance devices that capture the phone numbers dialled on outgoing telephone calls; trap and trace devices capture the numbers of incoming calls.

communications privacy violations by government personnel;

- expands the prohibition against FISA orders based solely on an American's exercise of his or her First Amendment rights.[24]

Aspects of the USA Patriot Act that enjoy widespread support in the US include provisions amending federal money-laundering laws, creating new federal crimes for attacks on mass transportation facilities and use of biological weapons, toughening penalties for existing federal crimes related to acts of terrorism and authorizing new appropriations to enhance border security and to help law enforcement and intelligence agencies track and prevent terrorism. More controversial are the provisions that relate to the expansion of government surveillance powers, including section 215, which has attracted widespread critical attention.

Section 215 of the USA Patriot Act

Title II of the USA Patriot Act is called Enhanced Surveillance Procedures. It expanded existing authority under various US federal laws—notably FISA—to intercept wire, oral and electronic communications relating to terrorism and to computer fraud and abuse offences.

Section 224 of Title II also created a sunset clause for most of the amendments to enhance surveillance authority, including section 215, with the designated provisions automatically being repealed on December 31, 2005, unless Congress eliminates the sunset clause or re-enacts the provisions.[25] Some submissions to us suggest that the sunset clause should be a source of comfort, but we see no reason to draw that conclusion. US lawmakers may allow section 215 to expire, or they may not, or they may expand it further. The existence of the sunset clause does not justify pointing our expectations in any direction.

Section 215 of the USA Patriot Act amended section 501 (and two other sections) of Title V of the Foreign Intelligence Surveillance Act of 1978.[26] The result now reads as follows:

§1861. ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS

(a) Application for order; conduct of investigation generally

(1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

(2) An investigation conducted under this section shall—

(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

(B) not be conducted of a United States person solely upon the basis of activities protected by the first

[24] Charles Doyle, *The USA Patriot Act: A Legal Analysis* (CRS Report for Congress, 2002) at 14; the report is available on the website of the Federation of American Scientists: www.fas.org.

[25] In his January 20, 2004, State of the Union address, President Bush called on Congress to renew the USA Patriot Act. The text of the address is available on the US White House website: www.whitehouse.gov. No such automatic repeal is found in Canada's comparable post-9/11 legislation, the Anti-terrorism Act, *supra* note 1, and the Public Safety Act, 2002, *supra* note 5. However, section 145 of the Anti-terrorism Act directs that a Parliamentary review of that Act be undertaken within three years of royal assent.

[26] 50 U.S.C. §§ 1861, 1862.

amendment to the Constitution of the United States.

(b) Recipient and contents of application

Each application under this section—

(1) shall be made to—

(A) a judge of the court established by section 1803(a) of this title; or

(B) a United States Magistrate Judge under chapter 43 of title 28, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

(2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) to protect against international terrorism or clandestine intelligence activities.

(c) Ex parte judicial order of approval

(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.

(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a) of this section.

(d) Nondisclosure

No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.

(e) Liability for good faith disclosure; waiver

A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.[27]

Concerns about Section 215

Submissions made to us point to the following main concerns about section 215 as it might relate to the interests of British Columbians.

The threshold for making orders

FISA orders were previously issued only where the FBI showed specific and articulable facts giving reason to believe that the person the records are sought about was a foreign power or an agent of a foreign power. Section 215 lowered the threshold to a showing by the FBI that records are sought for an authorized investigation to obtain foreign intelligence information not concerning a US person or to protect against international terrorism or clandestine intelligence activities.

We are told that this creates significant concerns for British Columbians. While the articulable cause threshold for a FISA order was never as high as the Canadian reasonably based probability threshold, the new FISA threshold requiring specification that records are sought for an authorized investigation is even lower. As a result, if a FISA order could be issued for personal information of British Columbians that is located in this province or taken to the US in conjunction with an outsourcing arrangement, concerns about the prospect of the information being obtained by US authorities would be compounded by the fact that a FISA order can be issued in circumstances that would not be considered sufficient in Canada.

27 50 U.S.C. § 1861.

Scope of orders

We are told that this concern about the lower threshold for the issuance of FISA orders is further exacerbated by the significantly expanded scope for the issuance of the FISA order in the first place. FISA orders were previously limited to certain business records held by public carriers and accommodation, physical storage or vehicle rental facilities. Section 215 expanded the power to make FISA orders to obtain "any tangible things" and removed the restriction on the kinds of organizations covered.

The removal of the restriction on the kinds of organizations that can be subject to a FISA order has caused considerable consternation in the US about these orders being presented to hospitals, libraries, bookstores, schools and all varieties of businesses. A significant number of those making submissions to us are clearly aware of this issue in the US and share concerns about it. The following passage from the submission of the British Columbia Library Association is only one example:

> Libraries have supported privacy rights in order to assure the broadest possible access to information. While seemingly contradictory, the right of access and the right of privacy are closely intertwined. If the public cannot be assured that their access to information and material in libraries and bookstores is confidential, a chill will be cast over their willingness to access provocative, controversial or highly personal material.
>
> While this review directly concerns access through the *USA Patriot Act* to the private records of the British Columbia Medical Services Plan and Pharmacare Plan, the issues concern all individuals and organizations who are concerned about privacy and confidentiality, or whose credibility and service depend upon providing confidential services.
>
> Libraries, unlike many other organizations making submissions, have experience through our colleagues in the American Library Association in understanding the potential impact on libraries of the *USA Patriot Act*. Attached as Appendix B is an American Library Association resolution opposing the Act and copies of posters distributed by some librarians to warn patrons of the insidious impact of the Act.
>
> British Columbia librarians understand that the present issue regarding access to medical records through the *USA Patriot Act* is only the thin edge of the wedge. However, the issues addressed in this review will have far-reaching consequences, which will ultimately impact the confidentiality of a broad range of library records. A ruling that the BC Medical Services Plan and Pharmacare records are vulnerable to requests through the *USA Patriot Act* will provide the basis for a re-examination of many library contracts with US vendors.[28]

Critics say that the expansion of the power to make FISA orders to "any tangible things", combined with no limit on the number records obtained, means FISA orders may now be made in relation to entire databases of information. The BC government's perspective, however, is that information is not a tangible thing because it does not have physical form, so a FISA order could only be issued in respect of hard copy records, hard drives and other equipment containing electronically stored information. Further, the BC government says, the FIS Court does not appear to have power to require someone to create a tangible record by copying or transferring information to a physical, or tangible, medium.[29]

The BCGEU has offered a sharp comeback on this by drawing our attention to testimony of US Attorney General Ashcroft to the US House Judiciary Committee suggesting that a FISA order could be used to obtain computer files and genetic information. The BCGEU also observes that the inability of a FIS Court to require the creation of a tangible thing is of

28 Submission of British Columbia Library Association (5 August 2004) pp. 2-3.
29 Submission of Government of British Columbia (9 September 2004) p. 5.

little significance, because this could be overcome by requiring the handing over of the hard drive or other medium on which the information is stored.[30]

With all due respect to the BC government, we think that—regardless of Attorney General Ashcroft's testimony—the phrase "any tangible things" is, even on a narrow reading, broad enough to be of real concern to British Columbians where their personal information is involved. We also do not think it wise to make assumptions about the FIS Court adopting a narrow interpretation of "any tangible things" or about the likelihood or not of a FISA order being issued or executed in respect of bulk collections of information.

Secrecy of orders

FISA orders are issued and executed in secret. The significance of this for British Columbians is that if a FISA order were issued for personal information of British Columbians that is located in this province, or that is taken to the US in conjunction with an outsourcing arrangement, the issuance of the order, and compliance with it, would occur without notice to those interested in British Columbia.

How can we prevent or respond to the issuance of a FISA order if we do not know when it happens? How can we attempt to challenge a FISA order in a US court if we do not know that it exists?

Incentives for compliance

Would a person within the jurisdiction of a FIS Court feel compelled to comply with a FISA order? There is some reason to think so. The failure of a person to comply with a FISA order as required could constitute contempt punishable as an offence in the US. Section 215 also relieves a person of liability, at least in the US, for complying with a FISA order. As a result, if a contract or other legal duty applied to prevent a person from disclosing records affected by a FISA order, the person would be relieved of liability, at least in the US, for violating those obligations in order to comply with a FISA order.

Other Relevant USA Patriot Act Provisions

The submissions have alerted us to two other specific sections of the USA Patriot Act that amended existing FISA provisions.

Section 218

Section 218 of the USA Patriot Act altered the authority for physical searches and electronic surveillance under FISA, so that instead of requiring foreign intelligence gathering to be "the purpose" of the search or surveillance, it only needs to be "a significant purpose".[31] Critics say this new latitude permits foreign intelligence gathering tools, which offer less rigorous protections for individual rights and liberties than the investigative tools that apply to criminal law enforcement, to become backdoor tools of convenience for ordinary criminal law enforcement.

The perceived significance of physical searches and surveillance under FISA for British Columbians is that they could apply to personal information that a public body in this province allowed to pass through or reside in the US:

> Any data transmission to or through the U.S. would be subject to electronic surveillance provisions of American law. Depending on how outsourcing

[30] Submission of BCGEU (15 September 2004) p. 2, citing the testimony of US Attorney General John Ashcroft before the House Judiciary Committee on June 5, 2003.
[31] 50 U.S.C. §§ 1804(a)(7)(B) and 1823(a)(7)(B).

> contracts are written, they may permit electronic transmission of data to or through the U.S. This could happen on data backup or processing, or simply by internet transmissions routed through the U.S. The broad surveillance provisions of the *USA Patriot Act*, now available for purposes other than investigating terrorism, would then jeopardize the privacy rights of British Columbians.[32]

Section 505

Section 505 of the USA Patriot Act altered—its critics say lowered—the threshold for the FBI to itself issue orders, under a number of statutes,[33] called "national security letters" that compel financial institutions, phone companies and internet service providers to disclose information about their customers. It did this by changing the previous specific and articulable facts threshold to a requirement of relevance to an authorized intelligence investigation. The FBI's authority to issue national security letters has since been expanded again to cover records held by travel agencies, real estate agents, the US Postal Service, jewellery stores, casinos and car dealerships.[34]

The submissions to us did not directly address the significance of national security letters to British Columbians but, as with physical searches or electronic surveillance under FISA, the significance appears to be their potential application to personal information that a public body in this province allows to pass through or reside in the US.

An important distinction between national security letters and orders issued by the FIS Court requiring third parties to produce records or authorizing physical searches or electronic surveillance, is that national security letters are issued by the FBI directly, and secretly, without judicial supervision. A US District Court has, in a very recent decision that is being appealed by the US government, sustained a challenge to the FBI's authority to issue national security letters to internet service providers on the ground that the secrecy of the process is inconsistent with the First Amendment to the US Constitution:

> In particular, the Court agrees with Plaintiffs that [18 U.S.C.] § 2709(c), the non-disclosure provision, is unconstitutional. In simplest terms, § 2709(c) fails to pass muster under the exacting First Amendment standards applicable here because it is so broad and open-ended. In its all-inclusive sweep, it prohibits the NSL [national security letter] recipient, or its officers, employees, or agents, from revealing the existence of an NSL inquiry the FBI pursued under § 2709 in every case, to any person, in perpetuity, with no vehicle for the ban to ever be lifted from the recipient or other persons affected, under any circumstances, either by the FBI itself, or pursuant to judicial process. Because the Court cannot sever § 2709(c) from § 2709(a) and (b), the Court grants the remedy Plaintiffs request enjoining the Government from using § 2709 in this or any case as a means of gathering information from the sources specified in the statute.[35]

Perspectives on Patriot: Sharp Divisions in the US

The extent of data mining by government agencies (discussed in Chapter 4) has caused growing concern about privacy intrusions in the US. In September 2004, the US Senate unanimously approved a bill requiring federal agencies to report to Congress on the privacy impact of their activities. One of the bill's co-sponsors, Senator Patrick Leahy, explained: "This is about accountability. The American people deserve to know what kind of information is gathered about them and how federal agencies intend to store and use it." An

[32] Submission of BCGEU (15 September 2004) p. 15.
[33] 18 U.S.C. § 2709 (counterintelligence access to telephone toll and transactional records); 12 U.S.C. § 3414 (special procedures for financial records); 15 U.S.C. § 1681u (credit record disclosures to FBI for counterintelligence purposes).
[34] Intelligence Authorization Act for Fiscal Year 2004, HR 2417, 108 Cong., 1st sess., Congressional Record 149, no. 95 (June 25, 2003): H 5870-5881 (became effective December 13, 2003).
[35] *Doe and ACLU v. Ashcroft,* No. 04-CIV-2614; 2004 U.S. Dist. Lexis 19343 (S.D.N.Y. 2004) at 6-7.

aide added that the senator "is open to the concept that certain forms of data mining might enhance security. His concern is that whenever you are going to use the technology, you put in place protections for people's privacy".[36]

The US Congress has shown far greater ambivalence in grappling with the question of balancing security and privacy in the context of the powers granted to federal agencies under the USA Patriot Act. Privacy rights have given way to security concerns whenever the issue has arisen in relation to the USA Patriot Act. As recently as July 2004, the US House of Representatives voted on amendments to the USA Patriot Act that would have barred the Justice Department from searching bookstore and library records. The proposed amendments were defeated on a controversial 210-210 tie.[37]

Superficially, there may not be an obvious distinction between federal agencies dipping into aggregated databases and the Justice Department dipping into library records. The key difference appears to be that the latter activity is being carried out in the name of intelligence gathering for national security purposes. National security interests also have much to do with the recent increase in data mining by federal agencies, though data mining does not carry the approval of the USA Patriot Act.

The question being asked more frequently is whether security has gone beyond merely trumping privacy to trampling it. Even the staunchest privacy advocates acknowledge that protecting national security is of the highest importance. They argue, however, that disregarding basic civil liberties poses threats to the foundations of democracy and that the US administration has gone much too far in shifting the balance towards national security and away from privacy protection. The coalition of critics who agree on this point includes an unlikely amalgam of civil libertarians, librarians, staunch conservatives and pro-gun groups.

Those who support the curtailment of privacy rights argue the need for continuing to guard against acts of terrorism by identifying and dealing with persons likely to commit them. Taking the opposing view are critics who maintain that democracy stands or falls on the level of respect shown for individual rights and that, by eroding constitutional guarantees, such as those protecting free speech and assembly and against unreasonable search and seizure, the USA Patriot Act creates the climate for abuses of governmental authority.

Are the new legislative measures simply a refinement of long-existing powers to better deal with the specific threat of terrorism? Or do they introduce a new dimension of authority that challenges basic assumptions about the civil liberties of ordinary citizens?

As we will see in the next chapter, there is a similar debate in Canada, whose anti-terrorism initiatives have attracted less notice but are also apparently far reaching. Two distinctions between the two countries, however, are that national security has been a more immediate and preoccupying issue in the US and legal protections for privacy do not, as we discussed in Chapter 3, have as sure a footing in the US as in Canada. As we noted earlier in this chapter, it is quite conceivable that a search or seizure power associated with intelligence gathering could be constitutionally permissible in the US but not in Canada.

[36] Drew Clark, "Senate Votes for Privacy Study on Agencies' Data-mining Use" *National Journal's Technology Daily* (16 September 2004); a copy of this article is available on *Government Executive Magazine* website: www.govexec.com.

[37] Dan Morgan and Charles Babington, "Push by GOP Ends Attempt to Scale Back Patriot Act" *The Seattle Times* (9 July 2004); a copy of this article is available in the news archive on The Seattle Times website: www.seattletimes.com.

7 ANTI-TERRORISM LAWS IN CANADA

The two questions posed at the outset of this report focus on the USA Patriot Act. As the discussion so far demonstrates, however, there is no escaping the fact that they open up a Pandora's Box of related issues. We can only capture the concerns that have been expressed to us about the implications of the USA Patriot Act for the security of personal information of British Columbians by also discussing how developments in Canada have paralleled and interrelate with those in the US.

The September 11 attacks created almost irresistible political pressure for new intelligence and surveillance tools, for legislative changes to existing laws and for passage of new laws. Governments around the world responded. In doing so, they acted to equip themselves to combat what they—and most of their citizens—consider a radically new and dangerous terrorist threat. The USA Patriot Act was enacted. Canada's anti-terrorism legislation, enacted shortly afterward, also introduced significant new intelligence gathering and national security powers.

The new Canadian anti-terrorism laws provided the Canadian Security Intelligence Service (CSIS) and other agencies such as the Royal Canadian Mounted Police (RCMP) with enhanced surveillance powers that may be used to share information with US and other foreign authorities. Canadians need to consider whether these powers adequately take into account personal privacy. They need to consider the potential for misuse if these laws are applied to conventional criminal law enforcement and the potential for misuse and mistakes if they are used to assist foreign countries without controls in place to protect affected Canadians. The new Canadian laws also conscript the private sector in the collection and disclosure of personal information that may have a bearing on national security interests. Canadians also need to consider whether these laws adequately protect their privacy.

Canadian National Security Laws and Measures

Late in 2001, Parliament enacted the Anti-terrorism Act.[1] Like the USA Patriot Act, the Canadian Anti-terrorism Act amended existing legislation, notably the Criminal Code[2] and the Canadian Security Intelligence Service Act (CSIS Act).[3] In December 2001, the two countries also agreed to a border security plan that involves collecting and sharing information and intelligence on persons crossing the border as well as other individuals. As noted in the last chapter, the Customs Act[4] was amended in relation to the collection

1 Anti-terrorism Act, S.C. 2001, c. 41.
2 Criminal Code, R.S.C. 1985, c. C-46.
3 Canadian Security Intelligence Service Act, R.S.C. 1985, c. C-23.
4 Customs Act, R.S.C. 1985 (2d Supp.), c. 1.

and use (including cross-border sharing) of personal information of Canadians. In 2004, Parliament passed the Public Safety Act[5] as well.

Further, in April 2004 the federal government issued a new National Security Policy, a high-level policy statement pointing to improvements in national security initiatives and their integration.[6] The policy promises new measures in six key areas—emergency planning and management, public health emergencies, transportation security, border security and international security. These measures include establishing an Integrated Threat Assessment Centre and a National Security Advisory Council made up of security experts. To address citizen concerns about the secret nature of intelligence gathering and the potential for misuse, the government proposes to create an arm's length review mechanism for RCMP activities relating to national security, as well as a National Security Committee of Parliamentarians. In addition, the government announced that it plans to create an advisory Cross-Cultural Roundtable on Security comprising members of ethno-cultural and religious communities.

The Canadian Security Intelligence Service Act

The CSIS Act, which is the Canadian parallel to FISA, was originally passed in 1984 and created CSIS, Canada's domestic and international intelligence and national security agency. CSIS took over intelligence and security work previously performed by the RCMP.

The CSIS Act sets out the mandate and powers of CSIS to protect the security of Canada. Section 12 of the CSIS Act directs CSIS to

> collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada.[7]

One feature of the Anti-terrorism Act was to expand the CSIS Act definition of "threats to the security of Canada".[8] These are now defined as:

> (a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage,
>
> (b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person,
>
> (c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state, and
>
> (d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada
>
> but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d).[9]

As paragraph (b) of this definition indicates, "threats to the security of Canada" need not involve a threat of actual terrorism. It means that CSIS can,

5 Public Safety Act, 2002, S.C. 2004, c. 15.
6 Government of Canada, Securing an Open Society: Canada's National Security Policy (Privy Council Office, April 2004); available on the website of the Privy Council Office: www.pco-bcp.gc.ca
7 Canadian Security Intelligence Service Act, *supra* note 3, s. 12.
8 Anti-terrorism Act, supra note 1, s. 89 amended paragraph (c) of the definition in s. 2 of the Canadian Security Intelligence Service Act, *supra* note 3.
9 Canadian Security Intelligence Service Act, *supra* note 3, s. 2.

if there are reasonable grounds for suspicion, gather intelligence regarding any activity that is "foreign influenced", clandestine or deceptive and "detrimental to the interests of Canada". These are not phrases with precise meaning. On its face, paragraph (b) constitutes a generous mandate to gather information or intelligence about people.

CSIS's mandate to investigate or gather intelligence about threats to the security of Canada can be carried out in several ways. CSIS can itself investigate "or otherwise" gather information about threats to the security of Canada. Section 17 of the CSIS Act confirms that the words "or otherwise" would allow CSIS to gather information or intelligence through information sharing agreements with US or other foreign authorities. Section 17 allows CSIS to, with ministerial approval, "enter into an arrangement or otherwise cooperate with" a Canadian government or Canadian police force or a foreign government or institution of a foreign government. An arrangement or co-operation with a foreign government could include information sharing by which CSIS collects information in Canada and discloses it to US authorities. An arrangement or co-operation with an institution of a foreign government could include information sharing by which CSIS collects information or intelligence that US authorities have gathered under FISA or another US law. In other words, we see no barrier in the CSIS Act to CSIS getting information about persons in Canada from the US or from sharing such information with the US.

Section 21 of the CSIS Act allows CSIS to obtain a warrant for surveillance or the seizure of things. CSIS may seek a warrant where it has reasonable grounds to believe the warrant is required to enable it to investigate a threat to the security of Canada or to gather intelligence about foreign agents or others specified in section 16. The maximum duration of a warrant respecting investigation of a threat to the security of Canada is sixty days, or one year in any other case under the Act. Section 22 allows a judge to renew a warrant on further application by CSIS. CSIS must make the application for the warrant to a judge of the Federal Court of Canada who has been specially designated for the purpose. Section 7(2) requires CSIS to consult the Deputy Minister before making the initial application or applying to renew a warrant.

CSIS is required to support a warrant application with a sworn statement setting out the facts justifying the belief, on reasonable grounds, that a warrant is required to enable CSIS to investigate a threat to the security of Canada or to investigate foreign agents in Canada. At least one of the following must also be sworn to: that other investigative procedures have been tried and have failed or why it appears they are unlikely to succeed; that the urgency of the matter is such that it would be impractical to carry out the investigation using other investigative procedures alone; or that without a warrant it is likely that information of importance would not be obtained. An application for a warrant must also describe the communications to be intercepted or things to be obtained and the persons or class of persons from whom communications or things are to be intercepted or obtained.[10]

Section 26 of the CSIS Act provides that Part VI of the Criminal Code,[11] which governs interception of communications for criminal investigations, does not apply to any interception of communications under a CSIS warrant. Part VI of the Criminal Code provides a much more detailed and restrictive set of legal rules and procedures that must be met before private communications can be intercepted or disclosed for the purposes of investigation and prosecution of criminal offences. However, section 19(2) of the CSIS Act allows CSIS to disclose information it obtains in the performance of its functions and duties to the police and to the Attorney General "where the information

10 *Ibid*. s. 21(2).
11 Canadian Security Intelligence Service Act *supra* note 3, s. 27

[obtained] may be used in the investigation or prosecution of an alleged contravention" of any federal or provincial law.

This is reminiscent of the situation in the US where information gathered for broad national security purposes can also be shared and used for ordinary law enforcement purposes. Similarly, the requirement that a CSIS warrant or renewal application be "heard in private"[11] by a specially designated judge makes the proceeding in this way akin to the secret FISA court process. One submission drew the following analogy between a CSIS warrant and an order made under FISA:

> The Section 21 warrant is arguably similar to a Section 215 application made to the FISA court – both do not necessitate probable cause and both can be used to obtain any type of records or any other tangible thing. Moreover, the target of both warrants need not be the target of the national security investigation. Like a FISA application, a Section 21 application is usually heard *ex parte*. The PIPEDA amendment in the *Public Safety Act* which allows collection and use of information without consent for national security purposes further underscores the potential disclosure of sensitive information by private organizations to Canadian law enforcement.[12]

Despite these similarities in the laws and procedures of the US and Canada, there are also some significant differences. For example, the authority for electronic and physical searches and seizures under the CSIS Act continues to be tied to the investigation of "threats to the security of Canada", as broadly defined. It was not diminished, as FISA was, from "the purpose" to "a significant purpose" by section 218 of the USA Patriot Act.

The Anti-terrorism Act

The main vehicle for Canada's legislative response to September 11 was the Anti-terrorism Act,[13] which amended the Criminal Code[14] and a number of other federal laws. The Anti-terrorism Act introduced new legal concepts such as investigative hearings before a judge, preventive arrests, broad motive-based crimes for participation in and support for terrorist groups at home or abroad and new powers to list terrorist groups, deprive them of charitable status and take their property. The new Part II.1 of the Criminal Code entitled "Terrorism" criminalized many forms of financing and facilitating of terrorism, including participation in and support for terrorist organizations.[14]

The amendments implemented by the Anti-terrorism Act include the definition of "terrorist activity" that now appears in s. 83.01(1) of the Criminal Code. Essentially, that section defines terrorist activity as an act committed within or outside of Canada that

- if committed in Canada would be an offence under one of the UN anti-terrorism conventions and protocols; or
- is committed for political, religious or ideological purposes and with the intent to intimidate the public concerning its security or compel a person, government or domestic or international organization to do something; and which causes death or serious harm, or endangers a person, or that causes serious risk to the health and safety of the public, causes substantial damage to property likely to result in such harm; or seriously interferes with or disrupts an essential service, facility or system in a way intended to cause such harm.

Similarly, the amendments to the Criminal Code

12 Submission of Professor Michael Geist & Milana Homsi (July 2004) p. 24.

13 Also see substantial amendments made by the Anti-terrorism Act, supra note 1 to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, S.C. 2000, c.17, including incorporation into that Act of the definition of "threats to the security of Canada" found in s. 2 of the Canadian Security Intelligence Service Act, *supra* note 3.

14 Criminal Code, *supra* note 2.

now make it a crime to, among other things:

- knowingly collect, provide or use property or funds, either directly or indirectly, in order to carry out or facilitate the commission of terrorist crimes;[15]
- knowingly participate in or contribute to a terrorist group for the purpose of enhancing its ability to carry out or facilitate terrorist activity;[16]
- instruct anyone to carry out an activity for the benefit of a terrorist group or to carry out a terrorist activity;[17]
- knowingly harbour or conceal a person for the purpose of enabling the person to carry out or facilitate any terrorist activity.[18]

The changes to the Criminal Code implemented by the Anti-terrorism Act also include provisions for bringing a person to court when there are reasonable grounds to believe a terrorist activity will be carried out and imposing supervisory conditions on them if necessary.[19] Under certain conditions, police may simply arrest and detain a person without a warrant if there are reasonable grounds to suspect detention of the person is necessary to prevent a terrorist activity.[20]

In addition, the Anti-terrorism Act did the following:

- it amended the Canada Evidence Act to implement a procedure to deal with potential disclosures of "sensitive information" in the possession of the federal government in court proceedings (sensitive information is defined as information relating to international relations, national defence or security originating inside or outside of Canada which the federal government is taking steps to safeguard);[21]
- it amended the National Defence Act to clarify the mandate of the Communications Security Establishment (CSE) to acquire information from the global information infrastructure for the purpose of providing foreign intelligence through means including interception of communications of foreign targets abroad, and to ensure the security of electronic information and government computer networks;[22]
- it replaced the Official Secrets Act with a new Security of Information Act, which addresses national security concerns;[23]
- it amended the Proceeds of Crime (Money Laundering) and Terrorist Financing Act to authorize the Financial Transactions and Reports Analysis Centre of Canada to disclose information about financial transactions that may constitute threats to Canada's security to CSIS and other law enforcement agencies;[24]
- it amended the Criminal Code to include terrorist offences in the list of "primary designated offences" for which DNA samples can be taken from an offender and stored.[25]

The Public Safety Act

The Public Safety Act[26] was passed in May 2004, although not all of its provisions are yet in force. When they are, they will create new public safety offences and expand police investigation powers. They will

15 Criminal Code, *supra* note 2, ss. 83.02-83.04.
16 *Ibid*. s. 83.18.
17 *Ibid*. ss. 83.21-83.22.
18 *Ibid*. s. 83.23.
19 *Ibid*. s. 83.3.
20 *Ibid*. s. 83.3(4).
21 Canada Evidence Act, R.S.C. 1985, c. C-5, ss. 38-38.15.
22 National Defence Act, R.S.C. 1985, c. N-5, Part V.1.
23 Security of Information Act, R.S.C. 1985, c. O-5.
24 Proceeds of Crime (Money Laundering) and Terrorist Financing Act, *supra* note 16.
25 Criminal Code, *supra* note 2, ss. 487.04, 487.051-091.
26 Public Safety Act, 2002, *supra* note 5.

also expand the federal government's ability to share personal information regarding immigrants and refugees with other government agencies or foreign governments, including the US.

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 Minister or other designated authorities for "transportation security" purposes.[27]

Still to come into force are the amendments to the Aeronautics Act that will permit the Director of CSIS to require any air carrier or operator of an air reservation system to disclose specified information in its control to any person the Director designates, for the purposes of transportation security or investigation of "threats to the security of Canada". [28]

The Public Safety Act amendments to the Aeronautics Act will also allow the Commissioner of the RCMP to require any air carrier or operator of an air reservation system to, for the purposes of transportation security, disclose specified information in its control to any person the Commissioner designates.[31] Despite the Public Safety Act reference to "transportation security", the amendments allow this data to be matched with other data and to be disclosed to assist in executing certain outstanding arrest warrants. In effect, this new authority will compel the private sector to assist the state, in the absence of a warrant or court order, in surveillance of all air travellers for the broader general purposes of both national security and ordinary law enforcement.

Consistent with these powers to conscript the private sector into both national security and law enforcement activities, the Public Safety Act also amended the Personal Information Protection and Electronic Documents Act (PIPEDA) to permit private sector organizations to collect personal information without an individual's knowledge or consent if

- the collection is for the purpose of making a subsequent disclosure that is required by law;[29]
- CSIS, the RCMP or another authorized government institution makes a request and the information relates to national security, the defence of Canada or the conduct of international affairs; [30] and
- the organization suspects the information may be relevant to national security, the defence of Canada or the conduct of international affairs and the organization intends to disclose it to an investigative body or government institution.[31]

These amendments invite (and in some cases, compel) the private sector to assist the state in surveillance for both general national security and ordinary law enforcement purposes. One privacy expert has questioned the justification for these PIPEDA amendments, asking whether commercial organizations should "be in the business of spying on behalf of the government—and certainly not of their own accord and without any guidance."[32]

The Public Safety Act also amended the Proceeds of Crime (Money Laundering) and Terrorist Financing Act to authorize the Financial Transactions and Reports Analysis Centre of Canada to collect information it considers relevant to money laundering or financing of terrorist activities from publicly available information, including "commercially available databases". That agency is also authorized to obtain, under information

27 Aeronautics Act, R.S.C. 1985, c. A-2, s. 4.81. Personal information disclosed for such purposes must be destroyed within seven days after disclosure.
28 Public Safety Act, 2002, supra note 5, s. 5, amending Aeronautics Act, supra note 29 s. 4.82. The Schedule to the Public Safety Act specifies 32 data elements that may be the subject of a disclosure requirement by CSIS or the RCMP, discussed in the following paragraph of the main text.
29 Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, s. 7(1)(e)(ii).
30 *Ibid.* s. 7(1)(e)(i).
31 *Ibid.*
32 Interview of Murray Long by Terry McQuay (July 2004); available in PrivaViews on the Nymity Inc. website: www.nymity.com/privaviews.

sharing agreements, information maintained by federal or provincial governments for law enforcement or national security reasons.

Where Do We Go From Here?

The Information and Privacy Commissioner and other Canadian privacy oversight officials have voiced concern about or opposition to a number of the post-September 11 measures and to proposals such as a national identification card or system. An overall concern is that some of these measures do not meet the test of a demonstrated clear and compelling need, balanced with the least possible intrusion on the rights and freedoms of people in Canada.

The Information and Privacy Commissioner has on many occasions acknowledged that the rights and freedoms which we have come to expect will be upheld in Canada, including privacy rights, are not absolute. Global uncertainties may necessitate new strategies to protect the security of all people. It is imperative, however, that government abridgements of privacy rights in the name of protection against terrorism not be intended merely to assuage fears by making people feel more secure, as opposed to effectively and rationally addressing real risk.[33]

This is not to say that the risk of terrorist attacks on the US or Canada is not real. Government must, however, take great pains not to overstep the line. Although it may be true that, the more freedom people have, the greater the potential risks, the corollary is equally important to remember. Every increase in security almost inevitably curtails rights and freedoms that are at the heart of democratic societies. Rights and freedoms that we tend to take for granted because we have always been fortunate enough to have them can be easily eroded—in good faith or otherwise—and we must ensure our elected officials maintain life and vibrancy in them.

Against the backdrop of controversy surrounding Canada's anti-terrorism legislation, and in light of Canada's new National Security Policy, it is worth noting that in August 2004 Canada's Minister of Justice, Irwin Cotler, affirmed the imperative of crafting security measures that complement rather than conflict with our fundamental rights and freedoms:

> The underlying principle here is that there is no contradiction between the protection of security and the protection of human rights. In a word, anti-terrorism law and policy itself is anchored in a twofold human rights perspective: first, transnational terrorism—the slaughter of innocents—constitutes an assault on the security of a democracy and the most fundamental rights of its inhabitants—the right to life, liberty and security of the person.
>
> Accordingly, antiterrorist law and policy should be seen as the promotion and protection of the security of a democracy and fundamental human rights in the face of this injustice—the protection, indeed, of human security in the most profound sense.
>
> At the same time, the enforcement and application of counterterrorism law and policy must always comport with the rule of law. Minorities must never be singled out for differential and discriminatory treatment; torture must always and everywhere be prohibited; and counterterrorism must not undermine the very human security we seek to promote and protect.
>
> It is important that we bear these bedrock principles in mind over the next few months as we undertake a number of important initiatives in the area of national security, like the Parliamentary review this fall of Bill-36, the Anti-terrorism Act.[34]

These comments about the need to strike the right balance between public safety and privacy apply with

33 David Loukidelis, "Identity, Privacy & Security—Can Technology Really Reconcile Them?" (Speech, Victoria, British Columbia, February 2004).
34 The Honourable Irwin Cotler, Minister of Justice and Attorney-General of Canada, (Address to the Canadian Bar Association, 16 August 2004) [unpublished].

equal force to all of the laws discussed in this chapter.

At the 2004 annual meeting of the Canadian Bar Association, members passed two resolutions aimed at ensuring an appropriate balance between privacy and security. The first urges all governments to do a better job of "preserving, promoting and respecting privacy," including regarding the use of personal information for national security or police investigations. The second calls on the federal government to toughen the federal public sector Privacy Act, to limit government intrusion into the lives of Canadians and to balance privacy and personal freedoms with government need for personal information about individuals.[35]

Just days after these resolutions were passed, the annual conference of the Canadian Association of Chiefs of Police called on the federal government to allow police greater access to Canadians' email, wireless and electronic communications, with the association's president claiming that legal and technical difficulties faced by police in attempting to gain access to such communications pose "a serious threat to public safety" in Canada.[36] At the end of the conference, the outgoing president of the Association and the Commissioner of the RCMP were quoted in the media as citing the threat of terrorism to support their assertion that the world is a much more dangerous place than when they began their careers.[37]

The balance between privacy and Canada's national security and public safety interests is dynamic. In the ongoing quest for the right balance it is vital that, as we discussed in Chapter 5, our national security needs not blur into ordinary law enforcement interests and demands. The constitutional and statutory privacy protections we enjoy should not be set adrift in the name of national security to founder on the rocks of law enforcement expedience. The need to deal with the threat of terrorism seems much more immediate and easier to understand than the need to maintain basic liberties that we are used to taking for granted. But our measures for dealing with terrorism must be carefully guided so we do not lose the safeguards of our liberties in law or in practice. Democracy is no less fragile for the fact that we have enjoyed it for a long time.

Patriot North: Parallels with the US Approach

As the above discussion illustrates, Canada's Anti-terrorism Act, with its extensive changes and additions to the Criminal Code and other laws, pursues similar objectives to the USA Patriot Act and confers similar powers for the acquisition of personal information considered necessary to detect and deter terrorism. Several of the submissions we received make this point but draw markedly different conclusions from that observation.

ITAC has concluded that exposing the personal information of British Columbians to the jurisdictional reach of the USA Patriot Act is not problematic and does not require any mitigation at all because it does not constitute "a material change to the degree of confidentiality previously attaching to that personal information".[38] We explained in Chapter 6 that there is indeed a distinction, in terms of national sovereignty and protection of personal privacy, between disclosure of information to Canadian governments and to a foreign government. We also explained in this chapter why we must inquire about and question what information our government is collecting about us, the grounds on which that collection is being justified, how that information is or can be used,

35 Canadian Bar Association (Annual Meeting 2004), CBA Resolution 04-05-A, "Privacy Rights in Canada"; CBA Resolution 04-06-A, "Limiting State Access to Private Information". Privacy Act, R.S.C. 1985, c. P-21.
36 Maurice Bridge "Police Want More Access to Your E-mail" *The Vancouver Sun* (24 August 2004), A03.
37 Maurice Bridge "World Is Less Safe Now, Says RCMP's Top Boss" *The Vancouver Sun* (26 August 2004), A05.
38 Submission of Information Technology Association of Canada (28 May 2004) p. 40.

whether it is or can be passed on to others—including foreign governments—the purpose for doing so, the protections in place to guard against mistakes and misuse and so on.

Privacy International, by contrast to ITAC, argues that part of coping with globalization means putting our own house in order regarding anti-terrorism legislation and the protection of privacy, and that there is no room for complacency in Canada:

> … Canadian laws and practices are as equally invasive as the USA Patriot Act, and also provide access to this personal information by other foreign entities.
>
> … Canadian laws were created to protect privacy and civil liberties, and yet they are often in vain. Fighting terrorism is legitimate; applying terror rules to non-terror-related situations is dishonest, and we ask that this situation be fixed. Failing that, the trust and faith of Canadians citizens in their laws and in their human rights protections will continue to erode, even as these Canadian laws and practices are copied by other countries. This practice is corrosive to human rights internationally.
>
> …
>
> … Laws passed abroad will affect Canadian subsidiaries, Canadian firms with offices abroad, and Canadian data. This is globalisation in all ways, for better and for worse. As the Geist and Homsi submission states clearly, the powers and practices that allow for such extra-jurisdictional access to personal data arose mostly in the 1970s and 1980s. It is not a development of the 1990s globalization growth, nor the 2000s dearth in surveillance. Nowadays, to make surveillance effective, an international reach is optimal.
>
> … We should avoid seeing Canada as a lonely lamb about to be engulfed by the American wolf. The laws that protect privacy in Canada are many and they act as models to the rest of the world. Canada's laws on surveillance, however, are also models of invasiveness. As a number of submissions stated, most remarkably the one from ITAC, Canadian law enforcement and national security agencies already have similar practices to the Americans. How can Canada turn down another for something that they would choose to allow for themselves? The problem thus begins at home.
>
> …
>
> Reasonable people may say that the USA Patriot Act is not problematic because of the letter of the law, or it is no different to existing practices and laws. These people are probably right in much of what they say. But within our current legislative and political environment we cannot separate the concerns of those who fear anti-terrorism laws but do not know its contents, from the concerns of those who worry about being sent to jails in third-world countries because of opaque regimes of international co-operation, from the concerns about not being able to get onto airplanes or open bank accounts because of inaccurate information, or from the concerns of being wiretapped by all-listening ears. Perhaps these fears are not well grounded, but the lack of confidence and the fears themselves are real. Reasonable people may debate about truth and facts, but the results of such a debate are almost secondary to our decreased confidence that our rights are adequately protected.
>
> The situation may not be legally wrong, but it remains dishonest and sufficiently opaque to all. Much needs to be done to increase our confidence, all these years after so much has been done in the name of increasing our security.
>
> The legal situation in the US regarding the treatment of personal information is indeed appalling. It does create a problematic situation for Canadian law, as it did with EU practices. The situation must be fixed. Yet Canada must also fix its own house. The legal protection of privacy and due process in Canadian law is increasingly problematic, to the point that Canada is in less and less a position to criticize others, even as Canada's laws are increasingly being used as standards for other countries. These conditions are establishing unacceptable risks particularly with an increasingly docile set of legislatures.
>
> The British Columbia Commission, as well as all other privacy and information commissions, need to protect the hard fought data protection and privacy laws in light of these developments, in order to protect the regime in Canada from the corrosive effects of international policy dynamics and degradation by

internal legislative dynamics. At some point this madness must stop. Someone has to stand up and say that this cannot continue. We hope this will begin in British Columbia.[39]

Several other submissions agree that it is wrong thinking to simply accept the fact we now live in a different world where, rightly or wrongly, state powers to obtain information have increased no matter where we live and that it makes little difference whether authorities using those powers are American or Canadian. These submissions argue that, if we truly value our basic civil liberties, we have to draw the line somewhere and say no, or else we face the slippery slope that leads to totalitarianism. It is not a question of not being serious about fighting terrorism, they submit. Rather, it is a question of following the rule of law that is fundamental to the health of democracies. Following the rule of law means not only respecting and enforcing existing privacy laws—including FOIPPA in British Columbia—but also ensuring that antiterrorism laws, written in time of crisis but with the watermark of permanence, do not swing the balance too far away from protecting public freedoms for the sake of appearing to protect public safety.

This will be one of the greatest challenges of coming years—to determine how much privacy we are prepared to relinquish in return for security or a sense of security. The dilemma is that no government or technology can guarantee absolute security and the question that arises from that is where to draw the line. How much do we lose by sacrificing individuality, by slow degrees, for that elusive feeling or fact of collective safety? If we value and seek national security, how much—if at all—should we tolerate the fading of lines between national security surveillance and law enforcement operations?

A Call for Clarity: A View from the Supreme Court of Canada

The Supreme Court of Canada earlier this year underscored the dual aspect of many so-called anti-terrorism or national security laws. In its decision regarding a challenge to the constitutionality of section 83.28 of the Criminal Code—a provision added in 2001 by the Anti-terrorism Act that, in certain circumstances, authorizes compelled, secret testimony by an individual before a judge—the court declined to characterize section 83.28 as a 'national security' law. The court acknowledged that the preamble to the Anti-terrorism Act refers to the "challenge of eradicating terrorism" and the need to strengthen Canada's capacity to "suppress, investigate and incapacitate terrorist activity". The court also noted similar references in debate in Parliament. However, in declining to characterize the Anti-terrorism Act as a 'national security' law the court said this:

> It was suggested in submissions that the purpose of the [Anti-terrorism] Act should be regarded broadly as the protection of "national security". However, we believe that this characterization has the potential to go too far and would have implications that far outstrip legislative intent. The discussions surrounding the legislation, and the legislative language itself, clearly demonstrate that the Act purports to provide means by which terrorism may be prosecuted and prevented. As we cautioned above, courts must not fall prey to the rhetorical urgency of a perceived emergency or an altered security paradigm. While the threat posed by terrorism is certainly more tangible in the aftermath of global events such as those perpetrated in the United States, and since then elsewhere, including very recently in Spain, we must not lose sight of the particular aims of the legislation. Notably, the Canadian government opted to enact specific criminal law and procedure legislation and did not make use of exceptional powers, for example under the *Emergencies Act*, R.S.C. 1985, c. 22 (4th Supp.), or invoke the notwithstanding clause at

39 Submission of Privacy International (August 2004) pp. 1-3, 7.

s. 33 of the *Charter*.

> We conclude that the purpose of the Act is the prosecution and prevention of terrorism offences.[40]

These comments have particular relevance to the protection of privacy. In essence, the court was saying that, if the government chooses to enact changes to the Criminal Code without resorting to the kind of exceptional powers it exercised under the War Measures Act in the 1970 'October Crisis', it is bound to respect and protect the civil rights to which any law applies.

We must remember the risk of blurring distinctions between national security and ordinary law enforcement laws and activities in considering the impact of national security laws on our rights and freedoms. Clear distinctions are especially vital in light of the nature, history and likely future of intelligence gathering activities and uses, which by their very nature are clouded in secrecy and often enjoy greater leeway in the balance with our rights and freedoms.

Conclusion

Canadian and American anti-terrorism initiatives have much in common, but Canada and the US do not necessarily have a common level of privacy protection that each affords its citizens by law. While the US may be the bastion of individual liberties, it has in many ways been a more reluctant guardian of individual privacy rights. As we explained in Chapter 3, Canada has followed the lead of the European Union in enshrining the principles of the Universal Declaration of Human Rights in federal and provincial privacy laws, whereas the US has taken a relatively hands-off approach, except in the regulation of commercial privacy. Similarly, US courts have taken a narrower approach to privacy rights under the US Constitution, which is not identical to Canada's Charter of Rights and Freedoms. In the next chapter, we discuss the ways in which the Charter protects individual privacy, including informational privacy, and the implications that Charter values could have for interpreting the privacy protections in FOIPPA.

40 *Application Under s. 83.28 of the Criminal Code (Re)*, [2004] S.C.J. No. 40, 2004 SCC 42 at paras. 39-40.

8 PRIVACY UNDER THE CANADIAN CHARTER OF RIGHTS AND FREEDOMS

Because of the fundamental importance of privacy in a free and democratic society, rights of privacy are part of the constitutional protections enshrined in the Canadian Charter of Rights and Freedoms (Charter).[1] The Charter is our defining statement of the civil liberties that are protected from Canadian government action[2] and can only be curtailed by such reasonable limits as are "demonstrably justified in a free and democratic society".[3] Government action includes legislation and actions taken by government under the authority of legislation or the common law. Canadian governments and their agencies must act in accordance with the Charter and the legislation enacted and programs and policies pursued by government must comply with the Charter.[4]

The Relevance of the Charter to this Report

Many submissions from organizations and individuals exhibit a keen awareness of Canadian privacy rights at a constitutional level. They speak eloquently to a pressing concern about a possible erosion of privacy rights stemming from outsourcing that could or would expose the personal information of British Columbians to US authorities.

This report is not intended to judge the scope of Charter rights or whether British Columbia laws—such as provisions of the Freedom of Information and Protection of Privacy Act (FOIPPA)—or specific outsourcing initiatives comply with the Charter. Having said this, we agree with those who have referred to the Charter or presented Charter analyses in their submissions that the Charter's privacy protections provide essential context for examination of implications of the USA Patriot Act for the outsourcing of public services in British Columbia. The privacy protections in Part 3 of FOIPPA are discussed in more detail in Chapter 9 of this report. This chapter's discussion of Charter privacy protections provides important context for analyzing disagreements in the submissions about the privacy protections in FOIPPA.

For example, there is disagreement in the

1 Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (U.K.), 1982, c. 11.

2 Section 32(1) of the Charter confines the application of the Charter to the Parliament and government of Canada and the legislatures and governments of the provinces and the territories.

3 All rights guaranteed by the Charter are subject, under section 1 of the Charter, to reasonable limits prescribed by law that can be demonstrably justified in a free and democratic society. If a law is found to infringe a Charter right, the burden is on the government that enacted the law to prove that the infringement is justified under section 1.

4 Section 52(1) of the Constitution Act, 1982 provides that any law inconsistent with the provisions of the Constitution is of no force or effect. However, section 33 of the Charter enables Parliament or a provincial legislature to override the rights accorded by section 2 or sections 7-15 of the Charter by an express declaration in a statute that it is to operate notwithstanding one or more of those Charter provisions. The so-called "notwithstanding clause" in section 33 of the Charter is rarely used. Peter W. Hogg, *Constitutional Law of Canada* (Toronto: Thomson-Carswell, 2004) at 36-2, 36-3, 36-9.

submissions about whether an outsourcing arrangement that involves risk of disclosure of personal information of British Columbians to US authorities under a Foreign Intelligence Surveillance Act (FISA) order can meet the requirements of section 30 of FOIPPA. That provision requires every public body to protect personal information in its custody or under its control "by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal".

There is also no consensus in the submissions as to whether disclosure of personal information in response to a FISA order would be a permitted disclosure under section 33 of FOIPPA. Nor is there consensus about the scope and significance of other avenues of disclosure to US authorities recognized in section 33. That section sets out the only circumstances in which a public body can disclose personal information that is in its custody or under its control.

The courts have left no room to doubt the appropriateness of considering Charter values in order to resolve the meaning of an ambiguous law or the limits of an imprecise discretion or standard in a law.[5] The Charter therefore can have a role to play in the resolution of conflicting perspectives on FOIPPA compliance. Where a FOIPPA provision can be read in a way that conforms with the Charter and in a way that does not, we should adopt the interpretation that is Charter compliant.

The Charter is also relevant to broader socio-political issues raised in the submissions. For example, several submissions reflect the view that Canadians must not lose sight of the fact that the US is not our country and that we should not assume that privacy rights under the Charter or Canadian statutes will be safeguarded by US authorities who are governed by US laws and public policy imperatives. The Public Services International submission put it this way:

> When citizens exchange information with their government for the purpose of obtaining government services or where required by their government, they have a right to demand a certain level of privacy in respect of that information.
>
> As citizens, we expect to be governed by our own elected representatives. We expect to be governed by the laws in our own countries. As a result, the potential for the FBI to demand information through an American company from a subsidiary or affiliate in another country offends the basic principles of democracy. Using the long arm of the USA Patriot Act to extend American legislation and American principles onto foreign soil is highly offensive to these basic principles. It offends our basic understanding of sovereignty.
>
> No contract provision or technological solution will allow an American company to contract out of the USA Patriot Act. Given the present American extreme interest in terrorism and national security, as evidenced by the USA Patriot Act, such excuses offered by an American company would not be tolerated. Any suggestion otherwise is naïve.[6]

The BC Public Interest Advocacy Centre submission noted:

> The United States has made a strategic decision, captured in the USA Patriot Act, that it is willing to sacrifice personal privacy rights in order to enhance police authority. We in British Columbia are not parties to that decision. Our government and other agencies in the provincial public sphere have an obligation to ensure that our privacy rights are not swept away in the US tide. American legislators have demonstrated a willingness to constrain commercial freedom of activity in order to meet statutory security objectives. We must be prepared to accept constraints on public contracting activity in order to meet our own privacy objectives.[7]

5 *Bell ExpressVu Limited Partnership v. Rex,* [2002] 2 S.C.R. 559 at paras. 28-30, 60-66 and *Slaight Communications Inc. v. Davidson*, [1989] 1 S.C.R. 1038 at 1077-78.
6 Submission of Public Services International (14 July 2004) p. 2.
7 Submission of the British Columbia Public Interest Advocacy Centre (June 2004) p. 6.

Other submissions ascribe importance to individual privacy but predict that the USA Patriot Act will have little impact on privacy and stress that there are other—apparently more readily available—ways for personal information in Canada to flow into the hands of US authorities. A US legal opinion made available by a major government contractor describes the likelihood of FISA being used to affect Canadians' interests as "vanishingly small".[8] The British Columbia government submission maintains that outsourcing to US-linked contractors can still afford reasonable privacy protection to British Columbians because FISA presents only a "small incremental" risk in light of other means of transnational information sharing and access.[9]

The transnational sharing of personal information that Canadian governments or their agencies gather about Canadian residents for the purpose of delivering public services in this country raises broad social, political and legal issues. It is difficult, if not impossible, to reflect on those issues without an appreciation of the dimensions of privacy as a constitutionally protected right in Canada.

Some submissions invite assessment of whether FISA, if enacted in Canada, would violate the Charter or whether Canadian courts would refuse to assist in the enforcement in Canada of FISA orders because such orders would offend the Charter in a manner that shocks the Canadian conscience. Serious questions may be raised about the constitutionality of some Canadian laws or bureaucratic practices relating to transnational accessibility of personal information that Canadian governments or their agencies acquire in the delivery of public services in Canada. It is conceivable—even probable, depending on the sensitivity of the personal information involved—that an information sharing, matching or mining arrangement or practice between Canadian and US authorities could constitute, in relation to Canadian-derived information, an unjustifiable infringement of individual liberty and security guaranteed under section 7 of the Charter.

These are clearly important and interesting questions that, realistically, cannot be resolved within the time-line and framework for this process, but it is necessary to canvass privacy rights in the Charter in this report for the other reasons we have mentioned above.

Section 8: Unreasonable Search and Seizure

The right of privacy—specifically, an individual's right to a reasonable expectation of privacy—is a core component of section 8 of the Charter, which guarantees the right of everyone in Canada to be secure against unreasonable search or seizure.[10]

Search or seizure need not involve an entry onto property or the forced taking of property. The invasion of a reasonable expectation of privacy is what constitutes the search or seizure.[11] Surveillance that intrudes on reasonable privacy expectations, whether or not it involves electronic or other devices, constitutes a "search" for the purposes of section 8. This includes sniffing at the front door of a home[12] or attaching a tracking device to a car.[13]

Taking records or bodily substances without consent constitutes a "seizure".[14] This includes an order or direction to produce a record or thing.[15] An

8 Submission of EDS Canada (19 July 2004) p. 29 (legal opinion of Stewart A. Baker, Steptoe & Johnson LLP, Washington, DC).
9 Submission of Government of British Columbia (23 July 2004) pp. 3-5, 35, 39.
10 *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145.
11 *R. v. Evans,* [1996] 1 S.C.R. 8 at para. 11.
12 *Ibid*. at paras. 9-21.
13 *R. v. Wise,* [1992] 1 S.C.R. 527.
14 *R. v. Dyment,* [1988] 2 S.C.R. 417 at 430-36; *R. v. Dersch*, [1993] 3 S.C.R. 768 at 778.
15 *R. v. Mills*, [1999] 3 S.C.R. 668 at para. 77.

order or other requirement to produce that is made under Canadian national security legislation would be a "seizure", as would a Canadian court order that enables the enforcement of a FISA order in Canada.

A two-part analysis applies to section 8 of the Charter. The threshold question is whether an individual has a reasonable expectation of privacy in the circumstances. If not, section 8 is not engaged. If there is a reasonable expectation of privacy, the second question to be answered is whether the search or seizure was reasonable. A search or seizure is reasonable if it is authorized by law, the law itself is reasonable and the manner in which the search or seizure is conducted is reasonable.[16]

The Charter protects privacy in places (such as an individual's home), privacy of the person (an individual's body) and privacy in information (notably an individual's core biography but also information about one's whereabouts or movements from place to place).[17]

Whether or not there is a reasonable expectation of privacy in particular information is determined from various contextual factors, including the type of information involved:

> [I]n order for constitutional protection to be extended, the information seized must be of a "personal and confidential" nature. In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the *Charter* should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.[18]

The fact that information about an individual is in the hands of a third party—such as a government, business or professional—does not mean that the individual no longer has a reasonable expectation of privacy in the information:

> Privacy is not an all or nothing right. It does not follow from the fact that the Crown has possession of the records that any reasonable expectation of privacy disappears. Privacy interests in modern society include the reasonable expectation that private information will remain confidential to the persons to whom and restricted to the purposes for which it was divulged, *Dyment*, *supra*, at p. 429. Where private information is disclosed to individuals outside of those to whom, or for purposes other than for which, it was originally divulged, the person to whom the information pertains may still hold a reasonable expectation of privacy in this information, *R. v. Boudreau*, [1998] O.J. No. 3526 (QL) (Gen. Div.), at para. 18.[19]

Thus, when the government or a third party has possession of information about an individual for a particular lawful purpose, the government is not excused from establishing the reasonableness of its seizure and use of the information for another purpose.[20] Whether or not a search or seizure by the government is reasonable depends on balancing the government's interest in obtaining the information against the individual's interest in maintaining privacy. This involves assessing the nature of the government's interest—which may vary widely from criminal prosecution to regulatory audit to detection of danger to public health—against the degree to which the individual has a reasonable expectation of privacy and the impact of the government's interest on the individual.

It will only be reasonable, in most cases, to infringe on a reasonable expectation of privacy if the government-sanctioned search or seizure is authorized

16 *R. v. Collins,* [1987] 1 S.C.R. 265 at 278.
17 *R. v. Dyment, supra* note 14; *R. v. Wise, supra* note 13.
18 *R. v. Plant*, [1993] 3 S.C.R. 281 at 293.
19 R. *v. Mills, supra* note 15 at para. 108.
20 *R. v. Colarusso*, [1994] 1 S.C.R. 20.

in advance by an independent judge who applies objective criteria and has residual discretion to refuse the authorization. In a law enforcement setting, there generally must be legal authority that requires a prior warrant or order, issued by an independent judge, on a sworn showing of reasonable and probable grounds to believe that an offence has been committed about which there is evidence to be found at the place of the search or in the things to be seized.[21] In a national security setting, the legal authority for the intrusion must require an independent judge to be satisfied on reasonable and probable grounds, established by sworn evidence, that a threat to the security of Canada exists and that a warrant is required to enable its investigation.[22]

Reasonable Expectation of Privacy

The question, in each case, is whether, by the standards of privacy that we can expect to enjoy in a free and democratic society, it is reasonable for government or its agents to intrude on privacy of place, person or information without first establishing reasonable and probable grounds on sworn evidence before an independent judge. Canadian courts constantly refine our understanding of the standards of privacy in a free and democratic society and they give those standards vitality with reference to new technologies that, if uncontrolled, have the potential to annihilate individual autonomy over when, how and to whom we reveal information about ourselves.

In *R. v. Dyment*, the Supreme Court of Canada held that a sample of blood taken by a doctor for medical purposes from a bleeding and unconscious hospital patient is intimately personal and confidential, as is other information about a patient concerning his or her medical treatment. The use for other purposes of bodily substances provided for medical purposes is a profound violation of personal autonomy that infringes on reasonable expectations of spatial, personal and informational privacy, as does the disclosure of specific medical care information without patient consent.[23] In *R. v. O'Connor* and *R. v. Mills*, the Supreme Court of Canada established that an extremely high expectation of privacy also attaches to therapeutic counselling records.[24] Also in this category, without doubt, would be pharmaceutical records of medications issued to a person for his or her medical care.

In *R. v. Plant*,[25] the City of Calgary arranged for a computer terminal to be located at a police station to give police access to computerized records indicating the electricity consumption at the home of an individual. The Supreme Court of Canada agreed that an individual has a reasonable expectation of privacy with respect to information that is personal and confidential, but it split on the status of electricity consumption records. A majority of the court decided there was no reasonable expectation of privacy because the electricity records revealed so little about the individual's personal lifestyle or private decisions.

In the minority, Justice McLachlin (now Chief Justice of Canada) concluded that electricity consumption records actually do reveal a lot about one's personal lifestyle and what is going on in one's home, such that an individual has a reasonable expectation that, in the absence of a properly authorized warrant, these records will be used only for the purpose for which they were made—the delivery and billing of electricity.

The majority in *R. v. Plant* appeared to be

21 *Hunter v. Southam Inc., supra* note 10.
22 *Atwal v. Canada,* [1988] 1 F.C. 107 (C.A.).
23 *R. v. Dersch, supra* note 14.
24 *R. v. O'Connor,* [1995] 4 S.C.R. 411; R. v. Mills, supra note 15.
25 *R. v. Plant, supra* note 18.

somewhat influenced in concluding that there was no reasonable expectation of privacy by the fact that, in Calgary, at that time, at least, electricity consumption records were available for public inspection. The events in this case predated provincial public and private sector privacy legislation in Alberta. Under FOIPPA and the Personal Information Protection Act (PIPA) in British Columbia, it would not be permissible for household electricity consumption records to be made available to the general public. The factor of pre-existing public availability was not present in the more recent case of *R. v. Tessling*[26], where the Ontario Court of Appeal decided that use of an aircraft equipped with an infrared camera to fly over and record the heat radiating from a home was an intrusion on the occupant's reasonable expectation of privacy in the activities carried on in the home. This decision is currently on appeal to the Supreme Court of Canada.[27]

R. v. Plant also highlighted the fact that Canadian and US constitutional privacy standards are different, and significantly so. Although the members of the court split on the privacy expectations attributable to electricity consumption records in a free and democratic society, they all rejected the view in US law that commercial records, such as cancelled cheques, are not constitutionally protected because they are not personal and confidential in nature.

In *Schreiber v. Canada (Attorney General),*[28] the Canadian government had asked Swiss authorities to assist with a Canadian criminal investigation by ordering the seizure of Swiss bank records relating to a Canadian resident. The Supreme Court of Canada split on various issues about when and how section 8 of the Charter applies to international criminal law enforcement activity by Canadian authorities, but all justices confirmed that, in Canada, there is a reasonable expectation of privacy in personal financial records.

In *R. v. Jarvis,*[29] the Supreme Court of Canada confirmed there is a diminished expectation of privacy in records produced during the ordinary course of regulated activities. The court concluded taxpayers have no reasonable expectation that records a tax auditor validly inspects or requires to be produced for the purpose of determining taxes owing will not be passed on, if irregularities are detected, to a tax investigator for the purposes of determining criminal liability for tax evasion.

In *Smith v. Canada (Attorney General),*[30] a provision in the Canada Customs Act, in combination with a data-matching agreement between customs and unemployment insurance authorities, permitted information from a customs declaration form (name, date of birth, postal code, purpose and dates of travel) to be matched to the individual's employment insurance status. As a result of a match, unemployment insurance officials ordered an individual to repay benefits that she had received while improperly out of the country. The Supreme Court of Canada concluded, in regrettably brief reasons, that the individual did not have a reasonable expectation of privacy in the information in her customs declaration that was made available to unemployment insurance officials considering the nature of the information, the relationship of returning Canadian residents and customs authorities, the place and manner of the disclosure in the form and the seriousness of the unemployment insurance violation under investigation.

The highly specific and time-limited purpose of detecting particular instances of employment insurance fraud is less invasive of privacy than information gathering or sharing for more generalized

26 *R. v. Tessling* (2003), 171 C.C.C. (3d) 361 (Ont. C.A.).
27 Appeal heard and reserved April 16, 2004, [2003] S.C.C.A. No. 116.
28 *Schreiber v. Canada (Attorney General)*, [1998] 1 S.C.R. 841.
29 *R. v. Jarvis,* [2002] 3 S.C.R. 757. Also see *R. v. Ling,* [2002] 3 S.C.R. 814.
30 *Smith v. Canada (Attorney General)*, [2001] 3 S.C.R. 902.

purposes. The latter has, in fact, proven to be highly controversial for federal government proposals for a passenger name record database on the foreign travel activities of Canadians.[31]

Generally speaking, the expectation of privacy that surrounds the collection, use or disclosure of information is greater the nearer the information is to an individual's biographical core—such as information about one's health, one's genetic characteristics, sexual orientation, employment, social or religious views, friendships and associations. Yet other contextual factors are also important—such as whether records are produced in the ordinary course of a regulated activity and whether their secondary use for a prosecution is related to the regulatory regime involved. Also, as noted earlier, technological advances continue to make it easier and easier to integrate, share and mine data collected for all kinds of purposes from all kinds of sources. Interpreting our privacy rights in the Charter in light of these new technological capabilities—and increased government adoption of them—remains a developing frontier for Canadian courts.

Section 7: Life, Liberty and Security of the Person

Section 7 of the Charter gives everyone the right to life, liberty and security of the person—rights that may only be infringed in accordance with the principles of fundamental justice. The privacy guarantee against unreasonable search and seizure in section 8 of the Charter is an application of the broader principles of fundamental justice that are referred to in section 7 and must be accommodated by a search or seizure that is reasonable.[32]

The right of privacy in terms of the physical integrity and dignity of one's body and the therapeutic care of one's psychological wellbeing is present in the security interest in section 7.[33] There is also a still-emerging view that, because individual privacy lies at the heart of what it means to be free, the right of privacy is part of the liberty interest in section 7.[34]

The right of privacy in section 7 of the Charter may be a particularly important source of constitutional protection in circumstances where Canadian authorities permit, or are instrumental in permitting, an intrusion on the reasonable expectation of the privacy of Canadians, but where section 8 does not apply because there is no search or seizure by a Canadian government.

These circumstances might arise in international criminal law enforcement settings. It is well established that the use of evidence obtained through foreign officials abroad can be precluded through a combination of section 7 and section 24(1) of the Charter in order to preserve the fairness of a criminal trial in Canada[35] and that section 7 may be applied to impose conditions of evidentiary immunity on testimony gathered in Canada to assist a foreign state in a criminal matter.[36] In *Purdy v. Canada (Attorney General),*[37] section 7 was applied to require the

31 Informative opinions on this issue by Hon. Gérard La Forest, C.C., Q.C., retired Supreme Court of Canada justice, (November 19, 2002) and by Roger Tassé, O.C., Q.C. (November 21, 2002) are available on the website of the Privacy Commissioner of Canada: www.privcom.gc.ca.

32 *R. v. Mills, supra* note 15 at para. 88.

33 *Rodriguez v. British Columbia (Attorney General)*, [1993] 3 S.C.R. 519; *R. v. O'Connor, supra* note 24; *Blencoe v. British Columbia (Human Rights Commission)*, [2000] 2 S.C.R. 307 at paras. 81-86.

34 *Ruby v. Canada (Solicitor General)*, [2000] 3 F.C. 589 (C.A.) at para. 165 rev'd on another point [2002] 4 S.C.R. 3. Also see the judgment of Justice La Forest in *R. v. Dyment, supra* note 14 at 427, referring to A .F. Westin: " … society has come to realize that privacy is at the heart of liberty in a modern state"; similarly, the judgment of Justice L'Heureux-Dubé in *R. v. O'Connor, supra* note 24 at para. 113: "Respect for individual privacy is an essential component of what it means to be 'free'. As a corollary, the infringement of this right undeniably impinges upon an individual's 'liberty' in our free and democratic society".

35 *R. v. Harrer*, [1995] 3 S.C.R. 562; R. v. Terry, [1996] 2 S.C.R. 207; *R. v. Schreiber, supra* note 28.

36 *U.S.A. v. Ross,* [1995] Q.J. No. 506 (C.A.); leave to appeal refused [1995] C.S.C.R. No. 410.

37 *Purdy v. Canada (Attorney General)* (2003), 230 D.L.R. (4th) 361 (B.C.C.A.).

Canadian federal government to disclose investigative material relating to a joint operation in Canada, by Canadian and US officials, that resulted in proceedings in the US against a Canadian citizen. Canadian courts have also refused—so far primarily on the basis of judicial discretion and abuse of process—to allow evidence gathered at the request of a foreign state under mutual legal assistance legislation to be sent to the requesting state where foreign officials took more than an observer or resource person role in the search and seizure in Canada or received or copied the results of the search or seizure outside of the court-supervised process.[38]

The right to privacy under section 7 might also arise in respect of domestic or transnational schemes for the sharing, matching or mining of personal information gathered by Canadian governments or their agencies where the information reveals intimate details about Canadian residents and their personal choices and its use or disclosure is a serious interference with individual autonomy or psychological integrity. The case of *Canadian AIDS Society v. Ontario*[39] held that a provincial law requiring the Red Cross Society to notify blood donors and public health authorities that blood taken and stored had tested HIV positive 10 years later, violated the security of the person under section 7 of donors, who had been told that no HIV test could be conducted when they donated and did not know of or consent to the storage and testing that had occurred. The court concluded the infringement did not offend the principles of fundamental justice, however, because of the importance of promoting public health and the balances in place respecting further disclosure by public health officials.

The submission from the BC Persons With AIDS Society observes that, because of a discriminatory US entry law, HIV-positive British Columbians could be denied entry to the US if information revealing their HIV status became accessible to US authorities:

> It is not just the prospect of their personal medical and other information falling into the hands of the US FBI that greatly concerns HIV-positive people living in British Columbia. Other American laws may work together with the *USA Patriot Act* to create serious and immediate difficulties for such persons in addition to those confronting their HIV-negative fellow citizens.
>
> …
>
> Numerous provisions of the American *Homeland Security Act* permit the centralization of information into enormous secret databanks, routinely available to various law enforcement and other agents of the American government, but of which the individuals concerned are given no notice and to which they are permitted no access.
>
> …
>
> Assuming concerns regarding the *USA Patriot Act* outlined above are legitimate, it is entirely possible that HIV status information obtained by the FBI could be passed along to US border agents through devices created by the *Homeland Security Act*. At that point, routine identification of HIV-positive British Columbians at the US border, and the denial of their request to enter could become a reality. Consequently, the lives of thousands of HIV-positive British Columbians could be seriously disrupted. And they would never even know until, one day, they are identified as being HIV-positive at the border and turned back.[40]

This would clearly be an intensely personal and highly prejudicial consequence of the health care information of HIV positive British Columbians becoming accessible to US authorities through information sharing or the failure of data security arrangements. Unlike *Canadian AIDS Society v.*

38 *Germany (Federal Republic) v. Ebke* (2001), 158 C.C.C. (3d) 253 (N.W.T.S.C.), aff'd (2003), 173 C.C.C. (3d) 261 (N.W.T.C.A.), leave to appeal refused [2003] S.C.C.A. No. 178; *U.S.A. v. Schneider,* [2002] B.C.J. No. 1561 (S.C.); *U.S.A. v. Orphanou*, [2004] O.J. No. 622 (Sup. Ct.).
39 *Canadian AIDS Society v. Ontario*, [1995] O.J. No. 2361 (Gen. Div.), aff'd [1996] O.J. No. 4184 (C.A.), leave to appeal refused [1997] S.C.C.A. No. 33.
40 Submission of British Columbia Persons With AIDS Society (14 July 2004) pp. 8-10.

Ontario[41], that consequence would not be balanced against public health concerns.

Application of the Charter outside Canada

The Charter may apply outside Canada to protect Canadians from the actions of Canadian authorities in circumstances where compliance with Charter standards by Canadian authorities acting abroad will not conflict with the laws of the foreign state in which they are operating.[42] More generally, however, the Charter, like other national laws, applies within national borders only[43] and does not apply to the actions of a foreign country or to the actions of foreign authorities in a foreign country, even when those actions are taken in co-operation with or at the request of Canadian authorities.[44]

When personal information about Canadians crosses our national border—whether in someone's briefcase, an electronic storage device or over the Internet—the protections in the Charter and in Canadian privacy laws do not follow. They are left behind in a very real sense and, in the absence of nation-to-nation agreements, the privacy protections that attach to the information when it is outside Canada are determined by the laws of the country where it has been sent. No doubt this was a driving consideration behind the commitment the BC government has made in its submission that it "will not send sensitive personal information to the US on a temporary or permanent basis".[45] This commitment is reflected in Bill 73, the Freedom of Information and Protection of Privacy Amendment Act, 2004, which at the time of writing had received Third Reading by the Legislative Assembly of British Columbia.[46]

People ordinarily and reasonably expect their activities to be governed by the laws of the place where they are.[47] When Canadians choose to travel to foreign countries, they do not expect the Charter to travel with them. A Canadian who has property or records in a foreign country also knows he or she runs the risk that the privacy of his or her affairs will be intruded on in accordance with the laws of the country where the property or records are located.[48]

In relation to their lives and activities in this country, however, Canadians expect to benefit from the protections of the Charter and other applicable Canadian laws. This includes, in our view, a reasonable expectation by British Columbians that the privacy rights in the Charter and in FOIPPA will apply to the personal information—particularly intimate details of their lives and life style—that they entrust to a public body in British Columbia for the purpose of receiving public benefits and services in this province.

41 *Canadian AIDS Society v. Ontario, supra* note 39.
42 *R. v. Cook,* [1998] 2 S.C.R. 597; *R. v. Harrer, supra* note 35 at paras. 10-11.
43 *R. v. Terry, supra* note 35.
44 *R. v. Terry, ibid.*; *R. v. Cook, supra* note 42.
45 Submission of Government of British Columbia (23 July 2004) p. 5.
46 Bill 73, Freedom of Information and Protection of Privacy Amendment Act, 2004, 5th Sess., 37th Parl., BC, 2004, (3rd reading 19 October 2004).
47 *Tolofson v. Jensen*, [1994] 3 S.C.R. 1022 at 1050-51; *R. v. Terry, supra* note 35.
48 *R. v. Schreiber, supra* note 28 at para. 24.

9 PROTECTING PRIVACY IN BRITISH COLUMBIA

Freedom of Information and Protection of Privacy Act

As mentioned earlier in this report, every Canadian province and territory has an access to information and privacy protection law and so does the federal government. Public sector privacy laws have spread across the country over the last twenty years as governments recognize the public's demand for controls on their collection, use and disclosure of citizens' personal information.

British Columbia is no exception. Since it was passed in 1993, the Freedom of Information and Protection of Privacy Act (FOIPPA) has governed the access to information and privacy practices of public bodies in British Columbia, of which there are over 2,000. They include all ministries of the BC government, a wide variety of designated government agencies, Crown corporations, boards, commissions and other bodies, and an even wider variety of local government bodies, hospitals, schools, colleges, universities and self-governing occupational organizations.[1]

FOIPPA gives the public a right of access to records in the custody or under the control of a public body. It also gives individuals a right of access to their own personal information in the hands of a public body[2] and the right to request correction of that information. FOIPPA also prevents a public body from engaging in unauthorized collection, use or disclosure of personal information.[3] The rights of access to information are found in Part 2 of FOIPPA, while the provisions respecting the collection, security, retention, use, correction and disclosure of personal information are in Part 3. These provisions aim to ensure accountable and responsible management of personal information by public bodies.

FOIPPA is considered fundamental legislation. Its subject matter—particularly informational privacy relating to the individual—is a human right that, as we have seen, receives significant constitutional protection under the Canadian Charter of Rights and Freedoms (Charter). The purposes of FOIPPA are properly understood in the context of the fundamental importance of privacy in a free and democratic society and the rights of privacy that are part of the constitutional protections in the Charter. Like human rights legislation, FOIPPA generally overrides any other conflicting provincial legislation.[4]

1 See definitions of "public body", "local public body", "local government body", "health care body" and "educational body" in FOIPPA Schedule 1 and the bodies listed in FOIPPA Schedules 2 and 3.

2 "Personal information" is defined in FOIPPA Schedule 1 as "recorded information about an identifiable individual".

3 These are three of the five explicit purposes of FOIPPA set out in s. 2(1). The other two stated purposes are to specify limited exceptions to the rights of access (see FOIPPA ss. 12-22.1); and to provide for an independent review by the Commissioner (or a delegate of the Commissioner) of decisions made under FOIPPA (see FOIPPA Part 5).

4 Section 79 of FOIPPA provides that if a provision of FOIPPA is inconsistent or in conflict with a provision of another Act, the provision of FOIPPA prevails unless the other Act expressly provides that it, or a provision of it, applies despite FOIPPA. Express FOIPPA overrides are rare.

The Information and Privacy Commissioner for British Columbia, an independent officer of the Legislature, is responsible for generally overseeing the administration of FOIPPA and ensuring compliance with its requirements. This chapter explores issues that go to the heart of that oversight mandate under FOIPPA. We discuss the status under FOIPPA of a Foreign Intelligence Surveillance Act (FISA) order for disclosure or production of records in British Columbia. We do this with reference to public bodies and to contractors working under outsource arrangements with public bodies. We discuss the contention in several submissions that, rather than resorting to a FISA order respecting information in this province, US authorities would use, and indeed are required to use, mutual legal assistance and other transnational information sharing mechanisms that are recognized in FOIPPA. Finally, we discuss how the risk of disclosure under a FISA order fits within the FOIPPA framework for reasonable security arrangements to protect against unauthorized disclosure of personal information.

In addressing these matters, we will concentrate on sections 30 and 33, the key provisions in Part 3 of FOIPPA governing security arrangements for personal information and when public bodies are permitted to disclose personal information.[5]

Unauthorized Access, Collection, Use, Disclosure or Disposal

Section 30 of FOIPPA reads as follows:

> 30 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.

This requires public bodies to protect personal information by making "reasonable" security arrangements against such risks as "unauthorized" access, collection, use, disclosure or disposal. The question arises whether access or disclosure under an order authorized by a foreign law, such as FISA, is "unauthorized" under section 30. If it is not "unauthorized", then a FISA order is not a risk against which section 30 gives protection, whether or not a public body has outsourced the management of personal information to a private service provider.

The British Columbia government observes in its submission that an "unauthorized" disclosure under section 30 is one that is not authorized under section 33 of FOIPPA. The government considers section 30 to oblige a public body to make reasonable security arrangements against disclosure for the purposes of the USA Patriot Act.[6] The submission of the Canadian Internet Policy and Public Interest Clinic says "unauthorized" should be interpreted to mean not authorized under FOIPPA or, at most, not authorized under Canadian law generally.[7] The submission from Fasken Martineau DuMoulin suggests that "unauthorized" in section 30 may not refer to legal authority at all, but simply to physical and administrative safeguards.[8] We disagree. On that premise, "unauthorized" access would be surreptitious or accidental access, not access that is unauthorized by law—be it FOIPPA, other Canadian law, or foreign law such as FISA.

We conclude that "unauthorized" under section 30 refers to disclosure that is unauthorized under applicable law, which would be FOIPPA and would include British Columbia's Document Disposal Act[9]

5 Also see s. 32 of FOIPPA, which regulates permitted use of personal information by a public body.
6 Submission of Government of British Columbia (23 July 2004) pp. 22, 24-25.
7 Submission of Canadian Internet Policy and Public Interest Clinic (2 August 2004) p. 12.
8 Submission of Fasken Martineau DuMoulin, by Jeffrey Kaufman and Richard Butler (5 August 2004) p. 5.
9 Document Disposal Act, R.S.B.C. 1996, c. 99.

for any public body covered by that Act. Access, collection, use, disclosure or disposal that is authorized by a foreign law is "unauthorized" under section 30 because it is not an applicable law, any more than a law of another province would be an applicable law in this province.

The reasons for interpreting "unauthorized" in section 30 in this way are straightforward. FOIPPA does not define the words "authorized" or "unauthorized". The point of reference for "authorized" varies in FOIPPA, but, when it is used with reference to legislation, either British Columbia or Canada, or both, is specified.[10] Other than section 30 of FOIPPA, the term "unauthorized" appears only in section 2(1), which sets out the purposes of FOIPPA. Section 2(1)(d) incorporates similar language to section 30 in a context that logically refers to permitted collection, use or disclosure under Part 3 of FOIPPA and is not restricted to protection against surreptitious or accidental activity.[11]

Neither FOIPPA's purposes nor context suggest that the words "authorized" or "unauthorized" are used in relation to foreign law. To interpret section 30 so that disclosure under a foreign law would not be an "unauthorized" disclosure under that section is contrary to legal principles—and to public expectations—of sovereignty and territoriality. The interpretive rules about the territorial application of legislation are based on the international law doctrine of territorial sovereignty, under which a sovereign state has exclusive jurisdiction in its own territory.[12] This means that everything within a state's borders is subject to its jurisdiction and the jurisdiction of each state is confined to its own territory. Although it is possible for a legislature to adopt or give effect within its own borders to a foreign law or order, it is presumed not to intend to do so without some express or implied indication, neither of which is present with respect to the word "unauthorized" in section 30 or elsewhere in FOIPPA.

To interpret section 30 so that disclosure under a foreign law would not be an "unauthorized" disclosure would also clash with section 33. For example, section 33(d) permits a public body to disclose personal information "in accordance with an enactment of British Columbia or Canada that authorizes or requires its disclosure." This explicit limitation on disclosure to a disclosure authorized or required by British Columbia or Canadian federal law would be meaningless if disclosure under the law of another province or of the US was an authorized, rather than an "unauthorized", disclosure against which a public body must protect under section 30.

Finally, we do not regard the meaning of "unauthorized" in section 30, in relation to foreign law, to be ambiguous or unclear. There is therefore no need to choose one reasonable interpretation over another on the basis of conformity with Charter values. On the other hand, to interpret section 30 so that disclosure under a foreign law would not be an "unauthorized" disclosure, in the absence of express language or necessary implication in that regard in FOIPPA, would run against reasonable expectations of privacy in this country.

10 See FOIPPA ss. 22(4)(c), 26(a), 27(1)(a)(iii), 33(d), 33(d.1). Note that, as a result of section 1 of the Interpretation Act, R.S.B.C. 1996, c. 238, when the phrase "an Act" (as opposed to "this Act") is used in FOIPPA it means an Act of the BC Legislature; when the term "enactment" is used it means a BC Act or a regulation as defined in the Interpretation Act.

11 Section 2(1)(d) FOIPPA provides that its purposes are to make public bodies more accountable to the public and to protect personal privacy by "preventing the unauthorized collection, use or disclosure of information by public bodies".

12 R. Sullivan, *Driedger on Construction of Statutes,* 3d ed. (Vancouver: Butterworths, 1994) at 333, referring to H.M. Kindred et al., *International Law Chiefly as Interpreted and Applied in Canada*, 5th ed. (Toronto: Emond Montgomery, 1993) at 325 and *Morguard Investments Ltd. v. De Savoye*, [1990] 3 S.C.R. 1077 at 1095.

Outsourcing and Control under FOIPPA

Outsourcing is not inconsistent with FOIPPA. It is contemplated by the extended definition of "employee" in Schedule 1 to FOIPPA, which includes "a person retained under contract to perform services for the public body"[13] and, by section 33(f), which permits disclosure to an "employee" of personal information in the custody or under the control of a public body where the disclosure is necessary for the performance of the employee's duties.

The fact that outsourcing is contemplated by FOIPPA does not, however, authorize a public body to do so in circumstances that would reduce security arrangements for personal information below those required of the public body directly. A public body cannot contract out of FOIPPA either directly or by outsourcing its functions.[14] The decision to outsource does not change the public body's responsibilities under FOIPPA. Nor does it change public and individual rights in FOIPPA, which are not balanced against any 'right' to outsource.

Section 30 requires public bodies to make reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal of personal information. When a public body contracts out functions, it must ensure there will be reasonable security arrangements for the personal information that it discloses to the contractor and that the contractor collects or generates in fulfilling the outsourced function. The public body's responsibilities under section 30, and the required standard of security, are constants, with or without outsourcing.

Submissions to us from the BC government and from contractors alike agree that, when a contractor possesses personal information in connection with outsourcing of public body functions, the personal information continues to be under the public body's control under FOIPPA. They emphasize that their diligence in this respect includes fashioning contract terms that embody FOIPPA obligations, thereby ensuring that the personal information "enjoys substantially the same protection it enjoyed prior to being made available to an outsourcing partner".[15] The public body is bound to comply with FOIPPA and the contractor is contractually bound not to disclose information without the authority of the public body.

Ongoing public body control of personal information under FOIPPA and the contractual extension of public body FOIPPA obligations to contractors do not resolve concerns about data that is sent abroad to places where FOIPPA is not the law and is neither respected nor enforced by the legal system abroad. Without a nation-to-nation accord that provides otherwise, data that travels to the US is subject to US law, including FISA. A British Columbia public body could try to live up to its FOIPPA responsibilities through its contract with a US-located contractor, but US law would all but inevitably determine the status and enforceability in the US of those contract terms.

The British Columbia government said in its submission to us that it would address this situation by committing not to send sensitive personal information to the US either on a temporary or permanent basis. This is constructive. It raises the question of whether this commitment will also apply for public bodies

13 "Person" is not defined in FOIPPA. However, section 29 of the Interpretation Act, *supra* note 10, which applies to FOIPPA, defines "person" as including "a corporation, partnership or party, and the personal or other legal representatives of a person to whom the context can apply according to law".

14 Order 04-19, [2004] B.C.I.P.C.D. No. 19; Order 00-47, [2000] B.C.I.P.C.D. No. 51 at paras. 10-45. Also see *Canada (Information Commissioner) v. Canada (Minister of Citizenship and Immigration)*, [2003] 1 F.C. 219 (C.A.) at para. 11; *Ontario (Criminal Code Review Board) v. Ontario (Information and Privacy Commissioner)* (1999), 180 D.L.R. (4th) 657 (Ont. C.A.); and *Canada (Information Commissioner) v. Canada (Immigration and Refugee Board)* (1997), 4 Admin L.R. (3d) 96 (F.C.T.D.) at para. 26.

15 Submission of Information Technology Association of Canada (5 August 2004) at p. 25. See also submissions of Government of British Columbia (23 July 2004) pp. 22ff; EDS Canada Inc. (19 July 2004) pp. 14ff; and Maximus (16 July 2004) p. 2.

under FOIPPA that are not part of a government ministry.[16] We believe there is no reason in principle, if such a commitment is implemented, not to extend it further. Indeed, the need for protection of personal information of British Columbians held by public bodies under FOIPPA is as compelling for Schedule 2 and 3 public bodies as it is for ministries of the provincial government. Many Schedule 2 public bodies—such as hospitals and other health care bodies—hold extremely sensitive personal information about patients. Many Schedule 3 public bodies—such as self-governing professional and occupational bodies—hold extremely sensitive personal information about their members and about their members' clients or patients. It also raises the question of whether FOIPPA should be amended to make this commitment a statutory requirement. We think this should be seriously explored by the British Columbia government.

The British Columbia government also says it intends to amend FOIPPA to "expressly prohibit service providers from disclosing personal information that has been provided to them by public bodies unless permitted by [FOIPPA], and require that such service providers notify government in the event their foreign affiliate requests that they disclose such information".[17] These would be important new safeguards for personal information that contractors hold in British Columbia under outsourcing arrangements with public bodies, whether or not the contractors have corporate or other links to the US.

Permitted Disclosure Under FOIPPA

Section 33 is a core component of FOIPPA's privacy protections. Its goal is to prevent indiscriminate disclosure of personal information by public bodies. It accomplishes this by prohibiting disclosure of personal information except under the expressly listed conditions. Any other disclosure is a breach of section 33—it is illegal. Depending on the circumstances, an actual unauthorized disclosure may entail a breach of reasonable security requirements in section 30 and, in contrast to section 33, an unrealized risk of unauthorized disclosure may involve a breach of section 30.

We have already explained the link between section 33(f) and disclosure to a contractor. We will now discuss the following particular paragraphs of section 33 with reference to FISA orders, outsourcing, compliance with section 33 and compliance with the reasonable security arrangements requirement of section 30:

> 33 A public body must ensure that personal information in its custody or under its control is disclosed only …
>
> (d) in accordance with an enactment of British Columbia or Canada that authorizes or requires its disclosure,
>
> (d.1) in accordance with a provision of a treaty, arrangement or agreement that
>
> (i) authorizes or requires its disclosure, and
> (ii) is made under an enactment of British Columbia or Canada,
>
> (e) for the purpose of complying with a subpoena, warrant, or order issued by a court, person or body with jurisdiction to compel the production of information, …
>
> (n) to a public body or a law enforcement agency in Canada to assist in an investigation
>
> (i) undertaken with a view to a law enforcement proceeding, or
> (ii) from which a law enforcement proceeding is likely to result,

16 For example, municipal government bodies, hospitals, colleges, universities and bodies that are listed in Schedules 2 and 3 of FOIPPA.
17 Submission of Government of British Columbia (23 July 2004) p. 3. During the preparation of this report, the intended amendments were introduced in Bill 73, Freedom of Information and Protection of Privacy Amendment Act, 2004, 5th Sess., 37th Parl., BC, 2004 (3rd reading 19 October 2004).

(o) if the public body is a law enforcement agency and the information is disclosed

(i) to another law enforcement agency in Canada, or
(ii) to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority, …

Disclosure authorized or required by law or treaty

Section 33(d) permits a public body to disclose personal information if authorized or required to do so by an enactment of British Columbia or Canada. This provision operates regardless of whether the public body has outsourced the management of the personal information. No one has suggested that there is legislation of British Columbia or Canada that authorizes or requires a public body to disclose personal information in response to a FISA order.

Section 33(d.1) is a variation on section 33(d). It permits a public body to disclose personal information in accordance with a provision of a "treaty, arrangement or agreement" that authorizes or requires disclosure and is made under legislation of British Columbia or Canada. Some treaties, arrangements or agreements may entail direct supervision of the disclosure process by a Canadian court. This is not, however, a requirement of section 33(d.1), which creates the potential for disclosure of personal information of British Columbians by public bodies to other public bodies and to other governments and government authorities in Canada and abroad, on the widest scales and without judicial supervision or intervention.

In discussing section 33(d.1), the British Columbia government concentrates on the Canada-US Mutual Legal Assistance Treaty (MLAT),[18] which governs requests for assistance by law enforcement authorities of one country to the other in order to obtain records and other evidence relating to the investigation or prosecution of offences. Canada implemented MLAT through the Mutual Legal Assistance in Criminal Matters Act (MLACMA),[19] which came into force in 1990.

The British Columbia government describes MLAT as the "streamlined default process"[20] and "primary method"[21] by which US officials obtain information held in Canada. The British Columbia government also says that, in "most" cases, the US will use MLAT, not FISA directly, to obtain personal information located in British Columbia.[22] These arguments appear to be based on the MLAT provision that requires each country to have recourse to MLAT first in seeking evidence located in the other country.[23] Similar arguments are found in the submissions of EDS Canada Inc. and of the Information Technology Association of Canada.[24]

These assertions are correct only to a degree. MLAT explicitly provides that it governs only requests for assistance in relation to the investigation or prosecution of an "offence".[25] It does not apply to intelligence gathering or surveillance where no investigation or prosecution of an "offence" is involved. MLAT is not, therefore, a mechanism for US authorities to gather information from Canada for foreign intelligence or national security purposes where no investigation or prosecution of an "offence" is contemplated.

18 Treaty between the Government of Canada and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters, 18 March 1985, Can. T.S. No. 19, (in force January 24, 1990; C. Gaz. 1990.I.953).
19 Mutual Legal Assistance in Criminal Matters Act, R.S.C. 1985 (4th Supp.), c. 30.
20 Submission of Government of British Columbia (23 July 2004) p. 10, para. 2.19.
21 *Ibid.* p. 7, para. 2.04.
22 *Ibid.* p. 8, para. 2.10 and p. 9, para. 2.16.
23 Article IV(1) of MLAT states: "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 as otherwise agreed pursuant to Article III(1)."
24 Submissions of EDS Canada Inc. (19 July 2004) p. 120; and Information Technology Association of Canada (5 August 2004) pp.16-17.

There is another important qualification. MLAT provides that each country may still use other agreements, arrangements or practices.[26] The request for assistance process in MLAT need not be followed, therefore, if a co-operative information sharing agreement, arrangement or practice is available.

Even if we assume, hypothetically, that US authorities could use MLAT for foreign intelligence gathering purposes alone, there is reason to doubt that they would if another information sharing arrangement were available. The request for assistance process in MLAT requires Canada to use best efforts to maintain secrecy in providing assistance, but this is not a guarantee of secrecy. The MLAT procedures that must be followed under MLACMA and the case law under that Act suggest that the level of secrecy contemplated by FISA, and almost invariably sought for intelligence gathering activities, is unlikely to be available once Canada's generally open court processes under MLACMA are in motion. Similarly, perceived delays in carrying out the letter of request process contemplated by MLAT and required by MLACMA could be expected to cause US authorities to avoid using MLAT.

In summary, we conclude that mechanisms other than MLAT will be used where US authorities are engaged in foreign intelligence information and no investigation or prosecution of an offence is involved. Further, even when the information gathering is in respect of the investigation, prosecution or suppression of an "offence" under the USA Patriot Act or another qualifying US law, US authorities can be expected to prefer less open and co-operative information sharing agreements, arrangements or practices, when they are available, to requests for assistance under MLAT.

Information sharing agreements and arrangements

The British Columbia government makes the wider point that all of the means of authorized information sharing under FOIPPA—whether under MLAT or other agreements or arrangements—could be expected to decrease the risk that US authorities would attempt to use FISA extra-territorially to acquire personal information in British Columbia. It says that disclosure under treaties, agreements and arrangements relating to criminal law enforcement, national security, foreign intelligence and regulatory activity—all of which is disclosure authorized by FOIPPA and the federal Privacy Act—is so extensive that US authorities would not resort to the extra-territorial use of a FISA order, as there is no need to.

This raises different and broader issues than the question of whether a US or US-linked contractor located in British Columbia might be susceptible to the reach of a FISA order. As the BCGEU submission puts it:

> We are not concerned here with information which has been lawfully acquired by law enforcement agencies in Canada, and which is then forwarded to U.S. authorities by those Canadian law enforcement agencies. This type of information collection and exchange would be subject to Canadian judicial scrutiny, and indeed, subject to the Charter. It is worth noting that the case of Maher Arar has made many Canadians increasingly concerned about the ability of the Canadian government to protect the rights of Canadian citizens when information is freely shared between law enforcement agencies here and in the United States. Instead, the information that we are concerned with here is information that was

25 Article I of MLAT defines "offence" as meaning, "for the United States, an offence for which the statutory penalty is a term of imprisonment of one year or more or an offence specified in the Annex" to MLAT. The Annex lists certain consumer protection, environmental and similar offences, but does not mention FISA or the USA Patriot Act. Consistent with the provisions of MLAT, MLACMA, the federal statute that implements MLAT in Canada, defines the term "offence" as "an offence within the meaning of the relevant agreement."

26 Article III(1) of MLAT states: "The Parties, including their competent authorities, may provide assistance pursuant to other agreements, arrangements or practices." Similarly, s. 3(2) of the MLACMA specifically preserves these arrangements or practices.

> provided to the provincial government, often with the explicit expectation that it would be kept confidential, in order to access provincial programs and to otherwise engage in civil society in the Province….[27]

The British Columbia government position does signal important concerns, however, about the extent to which Canadians' personal information is being shared with other countries and the grounds, terms and safeguards for doing so. In a more recent development in the Maher Arar affair, the Arar Inquiry[28] has released a redacted version of an RCMP report, which reportedly indicates that in the fall of 2002 Canadian authorities provided their US counterparts with intelligence about Maher Arar, who is a citizen of Canada and Syria, that may not have been reliable and without imposing conditions on its use (such as use for intelligence purposes only and not in legal proceedings). The information was then used in US proceedings that resulted in Arar's deportation from New York to Syria where he was imprisoned for a year, and reportedly tortured, before his return to Canada was arranged.[29]

Government information transfers about Canadians to other countries warrant rigorous study and national dialogue. The following passage from the submission of the Privacy Commissioner of Canada underlines the scope and seriousness of the problem:

> In 2003-04, the Office of the Privacy Commissioner of Canada carried out a preliminary review of Sharing of Information agreements (sometimes called "Memoranda of Understanding" (MOUs) between Canada and the US. MOUs from 18 federal departments and agencies were examined. The review found that most of these arrangements between the two countries did not address important issues such as unauthorized use, disclosure, retention and disposal of personal data. Only half of the MOUs contained a third party caveat—a statement indicating that information received under the agreement will not be disclosed to a third party without the prior written consent of the party who provided the information.
>
> The review also found that only a small number of these agreements (these can be counted by the hundreds in some departments) contained an audit provision and that none of these agreements had actually been subjected to an audit. These initial findings suggest that the sharing of personal information between the two countries is highly informal, with little oversight to ensure that the fair information principles (as defined in PIPEDA, for example) are adhered to by the respective governments.[30]

Need for audits

In British Columbia, there has been very little methodical documentation or examination of the information sharing in which public bodies engage under FOIPPA and none at all with respect to their data mining activities. Several years ago, the Information and Privacy Commissioner expressed concern about this in relation to information sharing and some work was done within the BC government to assess the number and nature of information sharing agreements and arrangements. That effort was laudable but inconclusive.

In 2002, section 69 of FOIPPA, which required the minister responsible for FOIPPA to publish a freedom of information directory, was replaced by an expanded provision that includes requirements for greater accountability and transparency in the

27 Submission of BCGEU (6 August 2004) p. 51.

28 The Honourable Dennis R. O'Connor, Associate Chief Justice of Ontario, was appointed to head the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, which was established on February 5, 2004 under Part I of the Inquiries Act, R.S.C. 1985, c. I-11. The mandate of the Arar Inquiry is to investigate and report on the actions of Canadian officials in relation to Maher Arar (Factual Inquiry) and to make recommendations on an arm's length review mechanism for RCMP activities with respect to national security (Policy Review). The work of the Arar Inquiry is currently underway.

29 Jeff Sallot "Mounties bungled Arar file" *The Globe & Mail* (25 September 2004) pp. A1 and A4.

30 Submission of Privacy Commissioner of Canada (16 August 2004) pp. 13-14.

area of information sharing agreements.[31] Under sections 69(2) and (3), the minister responsible for FOIPPA must now maintain and publish a personal information directory that includes "the information sharing agreements into which each ministry of the government of British Columbia has entered" and "any other information the minister responsible for this Act considers appropriate". Section 69(4) requires each ministry to correct as soon as possible any errors in the personal information directory that relates to the ministry. Under section 69(5), a ministry must also prepare an information sharing agreement in accordance with the directions of the minister responsible for FOIPPA. Finally, under section 69(7), the minister responsible for FOIPPA may require public bodies that are not ministries of the provincial government to comply with all or part of section 69 as if it were a ministry.

The information sharing agreement summaries that are published under section 69[32] as part of the personal information directory are relatively uninformative, however, and they do not cover agreements entered into by Schedule 2 or 3 public bodies, including police forces. We also consider the quality of reporting of information sharing agreements under section 69 to be suspect in that some of the summaries list expired agreements and many ministries and agencies report having no information sharing agreements at all (for example, Attorney General and Ministry Responsible for Treaty Negotiations, Management Services, Forests, Health Services, Office of the Premier, Organized Crime Agency, Public Safety and Solicitor General, Sustainable Resource Management, Transportation and Water, Land and Air Protection). It is inconceivable that all of these ministries and agencies—which include major law enforcement ministries and agencies—are not engaging in the sharing of personal information and highly unlikely, one would hope, that the sharing is occurring on an entirely ad hoc basis, without information sharing agreements in place. The 2002 amendment to section 69 with respect to information sharing agreements was a step in the right direction, no doubt, but it is not, so far, proving very useful in practice.

For this reason, and in light of the post-September 11 environment of increased national security powers—and, quite clearly, expanded information transfer and use—we recommend that the BC government undertake a comprehensive, independent audit of the interprovincial, national and transnational information sharing arrangements and agreements affecting all public bodies in British Columbia. This exercise should 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 doing so; the public bodies or private sector organizations involved; and the conditions in place to control the use and security of the information shared. The result should be a published report that will be a concrete move towards better transparency and accountability in this important but insufficiently studied area. We also believe that the information sharing agreements and arrangements entered into by all public bodies should be generally available to the public, under section 71 of FOIPPA, without a request for access under FOIPPA.

The Information and Privacy Commissioner supports the recommendation of the Privacy Commissioner of Canada, in her submission to us, that the federal government undertake a similar audit exercise.[33] Information sharing audits are especially important since, as the Privacy Commissioner of

31 Freedom of Information and Protection of Privacy Amendment Act, 2002, S.B.C. 2002, c. 13, s. 13.
32 The personal information directory that is required to be maintained and published under section 69, and is required to include information sharing agreement summaries, is available at the BC Ministry of Management Services website: www.mser.gov.bc.ca.
33 Submission of Privacy Commissioner of Canada (16 August 2004) pp. 13-15.

Canada points out, the federal Privacy Act contains no provision like section 30 of FOIPPA.[34] This means, significantly, that the security of information shared with the federal government is, in that government's hands, not protected by a specific reasonable security requirement as it is in the hands of a public body subject to FOIPPA.

We also recommend that the British Columbia government undertake a comparable comprehensive, independent audit of operational and planned data mining efforts by all public bodies in British Columbia. The result should be a published report that will also lend transparency and accountability to this area and will be a first, concrete step towards legislated accountability and transparency respecting data mining.[35]

Disclosure in compliance with a subpoena, warrant or order

Section 33(e) of FOIPPA permits a public body to disclose personal information "for the purposes of complying with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of information". The question arises whether "with jurisdiction" includes a subpoena, warrant or order issued under foreign law. If it does, then FOIPPA permits a public body to disclose personal information in response to a FISA order.

The British Columbia government maintains that section 33(e) does not permit disclosure by a public body in response to a subpoena, warrant or order issued or made by a court, person or body outside Canada.[36] It points out that

> where the FOIPP Act refers elsewhere to disclosures being authorized by an enactment, it refers only to enactments of British Columbia or Canada. There is no reference in the FOIPP Act to a public body being able to disclose personal information where a foreign enactment authorizes such a disclosure.[37]

The submission of Professor Michael Geist and Milana Homsi observes that this issue also presents itself in the similarly worded section 7(3)(c) of the federal Personal Information and Electronic Documents Act (PIPEDA),[38] which enables an organization to disclose personal information where it is required "to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel production of information".[39] Their submission states that PIPEDA

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

The submission of Fasken Martineau DuMoulin, on the other hand, interprets section 33(e) to include foreign subpoenas, warrants and orders on the reasoning that

34 *Ibid*. p. 10.

35 As discussed in Chapter 4, in 2003-2004 the General Accounting Office (now called the Government Accountability Office or GAO), which is the audit, evaluation and investigative arm of the US Congress, undertook a survey of data mining systems and activities US federal agencies. The result was its May 2004 report, "Data Mining: Federal Efforts Cover a Wide Range of Uses", available at the GAO website: www.gao.gov.

36 Submission of Government of British Columbia (23 July 2004) p. 25.

37 *Ibid*.

38 Similar wording to s. 33(e) is also found in some other Canadian privacy statutes: Privacy Act, R.S.C. 1985, c. P-21, s. 8(2)(c); Freedom of Information and Protection of Privacy Act, R.S.A. 2000, c. F-25, s. 40(1)(g); Freedom of Information and Protection of Privacy Act, C.C.S.M., c. F175, s. 44(1)(m); Access to Information and Protection of Privacy Act, S.N.L. 2002, c. A-1.1, s. 39(1)(e); Freedom of Information and Protection of Privacy Act, S.N.S. 1993, c. 5, s. 27(e); Access to Information and Protection of Privacy Act, S.N.W.T. 1994, c. 20, s. 48(n); Access to Information and Protection of Privacy Act (Nunavut), R.S.N.W.T. 1994, c. 20, s. 48(n); Freedom of Information and Protection of Privacy Act, R.S.P.E.I. 2002, c. F-15.01, s. 37(1)(f); Freedom of Information and Protection of Privacy Act, S.S. 1990-91, c. F-22.01, s. 29(2))(b); Access to Information and Protection of Privacy Act, R.S.Y. 2002, c. 1, s. 36(e).

39 Submission of Professor Michael Geist and Milana Homsi (July 2004) p. 20.

> [a]ssuming that a Patriot Act order has been properly obtained by the FBI, there is no basis on which to conclude that such an order would not fall within the provisions of s. 33(e) ... particularly when … this provision has no jurisdictional limitations.[40]

We agree with the British Columbia government's interpretation of section 33(e), with one refinement. We agree that in no circumstance would section 33(e) permit a public body to disclose personal information in response to a FISA order (or a national security letter) because such an order does not have the force of law here. We also agree that "with jurisdiction" would include a subpoena, warrant or order issued in British Columbia or possibly elsewhere in Canada under a federal law but, in our view, it would not include process issued under the authority of a provincial law of another province. This is because that other province's process would apply in British Columbia only if made enforceable by a British Columbia law or judicial order.

Inter-jurisdictional assistance proceedings

Section 33(e) would operate, though, in respect of a subpoena, warrant or order that is issued by a British Columbia court in a legal proceeding brought in British Columbia for the purpose of seeking judicial assistance in British Columbia with legal proceedings outside this province. International judicial assistance proceedings may concern a foreign criminal investigation or prosecution (these would be brought by or on behalf of a requesting foreign state) or a foreign civil action (these could be brought by a private litigant or by a foreign state or authority that is engaged in foreign civil litigation).[41]

Most criminal international assistance proceedings now involve bilateral or multi-lateral legal assistance treaties (such as MLAT) that are implemented by legislation (such as MLACMA). *U.S.A. v. Ross*[42] in fact describes a gathering order made by the BC Supreme Court under MLACMA that required the BC Ministry of Health to produce a letter of inquiry from an individual regarding medical coverage and care, for eventual transmittal to US authorities to assist their prosecution of a criminal case.

Civil international assistance proceedings (and still some criminal ones[43]) are brought through a reciprocal judicial letter of request system that is codified in rules of court and evidence statutes.[44] Under this system, a request is made by a court of one jurisdiction to a court of another to compel witnesses to be examined under oath or to secure the production of documents, with the testimony or documents being sent to the requesting court.[45] Courts act on letters of request based on the long-standing international custom for courts of one jurisdiction to respect the laws and judicial decisions of another jurisdiction, not because they are obliged to, but out of mutual deference and respect (under the principle of "comity").[46]

---

40 Submission of Fasken Martineau DuMoulin, by Jeffrey Kaufman and Richard Butler (5 August 2004) p. 21.

41 International legal and judicial assistance is a large topic that this report will not canvass in detail. Some useful references are: E.F. Krivel, T. Beveridge & J.W. Hayward, *A Practical Guide to Canadian Extradition* (Toronto: Carswell, 2002), Appendix A "Letters Rogatory" and Appendix B "The Mutual Legal Assistance in Criminal Matters Act and Mutual Legal Assistance Agreements"; Robert Goldstein and Nancy Dennison, "Mutual Legal Assistance in Canadian Criminal Courts" (2002) 45 Crim. L.Q. 126; Robert J. Currie, "Peace and Public Order: International Mutual Legal Assistance 'The Canadian Way'" (1998) 7 Dal. J. Leg. Stud. 91; Bradley J. Freedman and Gregory N. Harney, "Obtaining Evidence From Canada: The Enforcement of Letters Rogatory By Canadian Courts" (1987) 21:2 U.B.C.L. Rev. 351.

42 *U.S.A. v. Ross,* [1994] B.C.J. No. 971 (C.A.).

43 *Schreiber v. Canada (Attorney General),* [1998] 1 S.C.R. 841 is an example of a Canadian letter of request to Switzerland in a criminal matter. *Germany (Federal Republic) v. Canadian Imperial Bank of Commerce* (1997), 31 O.R. (3d) 684 (Ont. Ct. Gen. Div.) is an example of a German letter of request to Canada in a criminal matter.

44 British Columbia, Rules of Court, r. 38; Canada Evidence Act, R.S.C. 1985, c. C-5, s. 46; Evidence Act, R.S.B.C. 1996, c. 124, s. 53.

45 *A Practical Guide to Canadian Extradition, supra* note 38, Appendix A.

46 *R. v. Zingre,* [1981] 2 S.C.R. 392.

Among other conditions that must be met, the court must be satisfied that the evidence being sought relates to a civil, commercial or criminal matter pending before a foreign court that has authority to deal with the matter. A letter of request for an order for seizure of tangible things for intelligence purposes under FISA would not qualify because the necessary pending action, suit or proceeding is missing.

It was to contend with this kind of limitation in processes for international judicial assistance that US courts and grand juries developed the practice of issuing extraterritorial subpoenas for evidence located outside the US in relation to the investigation of criminal matters. This practice was strenuously objected to by Canada and led directly to the negotiation of the MLAT for criminal matters. The situation was summarized in the introduction to the US government technical analysis that accompanied the submission of the MLAT to the US Senate:

> [A]ssistance was sometimes forbidden by Canadian law which provided that its courts had authority to order production of documents or examination of witnesses for a foreign country only if the court were satisfied that the evidence produced would be used at trial and that it was not sought solely for the purpose of furthering the investigation. Generally, that meant that assistance could be granted only after charges were filed and not while the case was before a grand jury or otherwise still at the investigative stage. This rule thwarted U.S. efforts to investigate and prosecute certain cases. It also meant unequal treatment since the United States provided assistance without regard to whether the case was pre- or post-indictment.
>
> The United States resorted to judicious "self help" to complete investigations when Canadian assistance was not available. A method used with some frequency to obtain documents needed as evidence located in Canadian branches of institutions doing business in both countries was that of serving subpoenas for the documents on the U.S. branches. Canada viewed these "Bank of Nova Scotia" subpoenas, as they came to be known, as intrusions on its sovereignty but recognized that the United States would continue to use them in those cases where Canada was prevented by its law from assisting the United States.
>
> On March 19, 1985, the United States and Canada signed the Treaty on Mutual Legal Assistance in Criminal Matters. When ratified, that Treaty, together with the Canadian implementing legislation when adopted, will remove the legal barrier and permit (indeed, obligate) Canada to provide assistance prior to indictment. By making assistance available at the investigative stage, it diminishes considerably the need for the United States to issue or enforce Bank of Nova Scotia subpoenas for documents and records located in Canada. It also makes available international cooperative procedures and powers which our experience has shown to be the most desirable and effective.[47]

It is possible to speculate about the feasibility, likelihood or outcome of US authorities bringing an international assistance proceeding in a British Columbia court in respect of an intelligence gathering order made under FISA. Indeed, it may be little more than a theoretical possibility for one or more reasons. There could be other easier means for US authorities to get the information of interest. Further, Canada's strong open court tradition may not be acceptable to US authorities operating under the secret judicial processes that FISA requires.[48] As well, Canadian assistance would be unlikely if the FISA order is not tied to a criminal investigation or prosecution or it offends Canadian public policy, constitutional protections or sovereignty.[49] If a Canadian law specifically prohibits disclosure or transfer of personal information outside of Canada, this could also persuade a Canadian court not to order disclosure in response to a foreign letter

47 Technical Analysis, *Mutual Legal Assistance Treaty Between the United States and Canada*, reprinted in S. Treaty Doc. 100-14, 100th Cong., 2d Sess. at 8-9 (1988).

48 In *Re Vancouver Sun,* [2004] S.C.J. No. 41, 2004 SCC 43, the Canadian open court tradition was confirmed in relation to legislation for the investigation, prosecution and prevention of terrorism offences. This includes judicial investigative hearings in respect of which the presumption of openness should only be displaced on proper consideration of the competing interests at every stage of the process.

of request for that information.[50]

The important overall point, in terms of ensuring respect for the privacy rights and expectations of British Columbians, is that an international assistance proceeding in a Canadian court that could result in a subpoena, warrant or order for disclosure would involve Canadian officials, having regard to Canadian international obligations and Canadian legal and judicial traditions and sensibilities, including the Charter. In short, any disclosure that might be ordered, and thus be a permitted disclosure for the public body under section 33(e) of FOIPPA, would reflect the benefits and protections of Canadian political, legal and judicial systems.

There should be no grave concerns about outsourcing in relation to the operation of section 33(e). There may be technical or practical issues about notice of the subpoena, warrant or order being given to the public body as well as to the contractor, but personal information that is in the control of a public body under FOIPPA is no more or less within the reach of legal processes described by section 33(e) if it is being managed by a contractor so long, of course, as the information is not taken, or allowed to be accessed from, outside the province.

Disclosure for law enforcement

Section 33(n) permits a public body to disclose information to another public body or to a law enforcement agency in Canada—the RCMP would be an example—to assist in an investigation of a "law enforcement matter". It is difficult to see how section 33(n) could apply to disclosure to assist an intelligence investigation that is not in relation to criminal activity or other offences, but section 33(n) would certainly be available to permit a public body in British Columbia to disclose information to a Canadian police authority to assist its investigation of a terrorism offence under the Criminal Code.

If the public body is itself a law enforcement agency—for example, a municipal police force—section 33(o) would permit that agency to disclose personal information directly to another law enforcement agency in Canada or to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority.

Public bodies that deliver social services to the public, such as the government ministry that administers health care in British Columbia, are not law enforcement agencies and therefore could not disclose information under section 33(o). Public bodies that oversee regulatory regimes and their administrative enforcement, and have no direct responsibility for investigating or prosecuting penal legislation, are also not law enforcement agencies.

The real significance of section 33(n) and section 33(o) for the purposes of this report is that these provisions are authorized mechanisms under FOIPPA for disclosure of personal information to law

49 "The considerations encompassed by the phrase 'Canadian sovereignty' … include an assessment of whether the request would "give extra-territorial authority to foreign laws which violate relevant Canadian [federal] or provincial laws … [and] whether granting the request would infringe on recognized Canadian moral or legal principles": *Re Republic of France and De Havilland Aircraft of Canada Ltd.* (1991), 65 C.C.C. (3d) 449 (Ont. C.A.) at 463, citing *Re Westinghouse Electric Corp. and Duquesne Light Co.* (1977), 78 D.L.R. (3d) 3 (Ont. H.C.J.).

50 In *Gulf Oil Corp. v. Gulf Canada Ltd.*, [1980] 2 S.C.R. 39, the Supreme Court of Canada refused to order the federal government to disclose government records because both Canadian law and government policy prohibited it. Regulations under the Canadian federal Atomic Energy Control Act expressly prohibited disclosure of the records and the court on that basis refused to order disclosure of them to a US litigant. The court also declined to order disclosure on grounds of public policy. A federal Cabinet minister had publicly stated that the government's refusal to disclose the records was an assertion of Canadian sovereignty in the face of attempted extra-territorial application of US law. The court decided it would be inappropriate to compel disclosure in order for a US court to determine if the government of Canada had broken US law. This case is discussed in more detail by M.T. Rankin, "The Supreme Court of Canada and the International Uranium Cartel: Gulf Oil and Canadian Sovereignty", [1980] 2 Sup. Ct. Rev. 410.

51 BC OIPC Guideline 01-01, *Guidelines for Audits of Automated Personal Information Systems,* p.1, available on the website of the Office of the Information and Privacy Commissioner for British Columbia: www.oipc.bc.ca

enforcement officials in Canada and abroad. The BC government maintains that MLAT extends to US law enforcement authorities the same level of access to non-public information in the hands of the federal and provincial governments in Canada that is available to Canadian law enforcement authorities under FOIPPA. This point, if correct, would not apply to information held by public bodies that are not government—such as universities and hospitals—but it would support the British Columbia government's position that the authorized means of disclosing information under FOIPPA for domestic and foreign "law enforcement" purposes may make it unlikely that US authorities would attempt the extraterritorial use of FISA to gain access to personal information in British Columbia.

As with section 33(d.1), we recommend that the BC government undertake comprehensive independent audits of operational and planned information sharing arrangements and agreements under s. 33(o)(ii) and data mining efforts by all public bodies in British Columbia.

Reasonable Security Arrangements

Meaning of 'reasonable'

Section 33 does not permit a public body, or its contractor, to disclose personal information in response to a FISA order (or a national security letter). As we have explained, such disclosure would also be "unauthorized" disclosure under section 30 and, although FOIPPA contemplates outsourcing, the required standard of security for personal information does not change with outsourcing.

In the next chapter, we discuss the first question posed in the Request for Submissions, which concerns the plausibility, to the extent it can be assessed, of a FISA court issuing an order that extends to information held in British Columbia. Consistent with our conclusions in the next chapter, we will examine the meaning of "reasonable" in section 30 on the basis that it is a reasonable possibility (for both practical and legal reasons) that an extra-territorial FISA order would be sought and issued against an individual in the US or an organization that has a presence in the US, requiring it to produce records that it has a right or authority or practical ability to obtain in British Columbia. Turning, then, to the second question posed in the Request for Submissions: what are the implications for public body compliance with the personal privacy protections in FOIPPA and how may privacy risks in that regard be eliminated or mitigated? More specifically, what are the implications for the obligation, under section 30, for every public body to implement reasonable security measures to protect personal information?

The British Columbia government has provided dictionary definitions of 'reasonable' that it says indicate "reasonable security arrangements" are arrangements that are sensible and proportionate to the type of personal information involved. We agree that reasonable security arrangements are not infallible arrangements, not the least because such arrangements would be impossible. We agree, too, that the nature of the personal information involved and the seriousness of the consequences of its unauthorized disclosure are factors to be taken into account in assessing the reasonableness of security arrangements. The highly contextual approach to informational privacy that is evident in Charter case law may be instructive in this regard, as may the following example from the OIPC's guidelines for public bodies to refer to in designing, and auditing the performance of, automated systems that contain, process, transmit or otherwise deal with personal information:

> A variety of circumstances—including the nature of the personal information involved and the uses for that information—will determine which measures

> are necessary in each case to protect personal privacy and ensure the security of personal information. For example, a self-governing body need not, in creating a list of members' names and addresses, take the same measures for the privacy and security of that limited personal information as a hospital would have to take respecting patients' personal medical information.[51]

We do not, however, agree with the BC government's submission that orders of the Information and Privacy Commissioner about whether a public body has made every 'reasonable' effort to assist an applicant for access to information, as section 6 of FOIPPA[52] requires, are helpful in the context of section 30. We say this because the consequences of the conduct involved must be considered in measuring the degree of vigilance that is reasonably required. Most problem situations under section 6 of FOIPPA can be corrected. In many instances, lax effort in assisting an applicant means a response to an access request is provided later rather than sooner or the applicant gets a series of corrected responses instead of a thorough response the first time around.

Unauthorized disclosure puts private information where it should not be and lax security arrangements create risk that this generally more serious consequence will be realized. Attempting to remedy the unauthorized disclosure of personal information is another matter, especially if the information is disclosed to those who are consciously seeking access for their own purposes, without regard to the privacy protections in FOIPPA. The BCGEU submission expresses this well:

> It is important to recognize that once the information is disclosed to the FBI, it is subject to dissemination throughout the U.S. law enforcement, immigration and security intelligence bureaucracies, without any of the protections guaranteed to personal information which are provided by governments in Canada. The recent inquiries into intelligence failures leading to 9/11 have increased pressure in the Unites States to enhance information sharing between agencies and make information sharing systems even more comprehensive. As a result, it is impossible to predict all of the ways in which British Columbians may be affected by the disclosure. The only limits will be set by the ways in which the U.S. chooses to use the information, a matter over which Canadian courts and the Canadian government will have no control.[53]

It must not be forgotten, as well, that although particularly rigorous security arrangements will be reasonably required for information that is closer to the biographical core of the individual (the unauthorized disclosure of which will have more serious consequences), the requirement for security arrangements is not removed when more attenuated privacy interests are involved. Security arrangements are required to protect against any unauthorized disclosure of personal information. The fact that there is not likely to be any interest in particular information or that it would not occur to anyone to look or ask for it can never be a substitute for security arrangements to protect that information.

Ban on outsourcing?

The BCGEU observes that previous cases dealing with security arrangements in relation to outsourcing did not address a situation "in which the effect of the contracting out has been to subject the personal information of British Columbians to a whole new set of risks, including the application of an entirely different set of legal rules regarding disclosure".[54] It contends that the contracting out of government

52 Section 6(1) of FOIPPA states: "The head of a public body must make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely."
53 Submission of BCGEU (6 August 2004) pp. 55-56.
54 *Ibid*. p. 56.

functions to businesses that may be within the direct or indirect jurisdictional reach of a US court creates a risk of disclosure pursuant to a FISA order, which is a risk of unauthorized disclosure that is singular in kind and in remedy. As the BCGEU submission says:

> [I]n this case, the risk can be entirely avoided without taking any new security measures—simply by retaining the information within government.
>
> As long as the Government does not outsource those functions which involve the use of sensitive personal information of British Columbians, there is no risk that this information will become subject to possible disclosure under an order issued under the USA Patriot Act. Such information can only be disclosed under the conditions set out in s. 33, 35 and 36 of FOIPPA. An order issued by a U.S. court would not meet any of these criteria.
> …
>
> The Government's submission suggests that "risk can never be eliminated." In fact, this particular risk can be entirely avoided, simply by not contracting out the government functions that involve sensitive personal information of British Columbians. The Province's suggestion that other security risks, which cannot be eliminated, are somehow relevant to whether this particular risk should be eliminated is without merit. The Province should not use the possible existence of other risks as an excuse to avoid taking precautions.[55]

We are troubled by the BCGEU's assertion that unauthorized disclosure of personal information as a result of a US court order to obtain information located in this province is a particular problem that can and must be exceptionally resolved by a ban on the outsourcing of government functions that involve the sensitive personal information of British Columbians.

Professor Michael Geist and Milana Homsi point out that banning government outsourcing would not address the wider privacy issue caused by the application of US law to Canadian businesses:

> The BCGEU has called for a ban on government outsourcing of sensitive data. Although a governmental ban would potentially address the immediate issue of protecting the privacy of B.C. medical data, it does not address the wider privacy issue caused by the application of U.S. law to Canadian businesses. An effective ban on outsourcing would affect not only U.S. companies and their Canadian subsidiaries, but also any Canadian company that is subject to U.S. personal jurisdiction. Any ban would thus become ineffective should third party consultants or others come into possession of the data, even within Canada.
>
> A ban would also create an unfortunate disparity between the protection afforded to publicly held data and privately held data, a distinction that federal legislators tried to eliminate with the establishment of PIPEDA. It is arguable whether in all cases government data is more sensitive than privately held data. Many Canadian citizens would be more concerned about having their private emails or bank information disclosed to the FBI, rather than their medical information.
>
> Moreover, even personal information in government hands may still be subject to a U.S. court order. Although the Act of State Doctrine (AOSD), a U.S. common law principle, requires courts to decline to exercise jurisdiction over cases that may embarrass or impede the political branches of government in their conduct of foreign affairs, requests for AOSD are rarely granted. In W.S. Kirkpatrick v. Environmental Tectonics the court of appeal rejected AOSD and granted anti-corruption action for bribes paid to the Nigerian government for a defense contract because the State Department was satisfied that foreign policy would not be compromised by the litigation. In Curtiss-Wright, the court held that "the act of state doctrine should not be applied to thwart legitimate American regulatory

55 *Ibid*. pp. 60-62.
56 Submission of Professor Michael Geist and Milana Homsi (July 2004) pp. 26-27.
57 Submission of ACLU (10 August 2004) pp. 13-14.

> goals in the absence of a showing that adjudication may hinder international relations." Furthermore, the Foreign Sovereign Immunities Act (FSIA) features several AOSD exceptions, the most relevant of which arises in context of commercial activity of a foreign state. FSIA has been used to obtain judgment against government arms of Argentina, Nigeria and Cuba amongst others.[56]

In other words, in order to be effective, a ban on outsourcing would have to extend not only to US businesses, but also to Canadian businesses with US connections. The ACLU makes the point that a rule that bars the sharing of personal information in these circumstances "would also be grossly impractical. The nature of the ties between the United States and Canada make it likely that most or all corporations in Canada have the level of contact with the U.S. that is necessary to trigger jurisdiction [of US courts]."[57]

A ban on outsourcing would have to extend not just to the outsourcing of information management systems, but also to consulting contracts that give US contractors or Canadian contractors with US connections access to personal information held by government. Therefore, the following BCGEU example of a security risk would not be limited to the office of a contractor. It would also apply to a US computer specialist engaged by a government ministry to provide services at a ministry office in British Columbia:

> All it takes is a visit by representatives of the American firm to the Canadian office for data to be exposed. As an example, the Apple I-pod music player is small enough to fit in a pocket yet has enough storage capacity to hold an entire database, and can be plugged into a PC to download this information. All that would be required for a major breach of Canadian privacy would be a public-spirited American employee concerned about homeland security to make a visit to the office of the Canadian operations.[58]

Further, a ban on outsourcing would not exclude the possibility of a US court order being directed at a public body that is itself engaged in business activity in the US, especially if the public body is not part of the provincial government itself and therefore not likely to attract foreign sovereign immunity in the US. As we have already observed, public bodies that are not part of government are frequently responsible for significant collections of sensitive personal information.[59]

Taking these considerations into account, we conclude that the requirement for reasonable security arrangements in section 30 of FOIPPA does not entail absolute security against the possibility of unauthorized disclosure pursuant to an extraterritorial US court order. We also conclude that the possibility of such unauthorized disclosure cannot be eliminated by the suggested ban on outsourcing. The problem is not limited to the outsourcing of functions of government ministries that involve sensitive personal information and it is entirely appropriate to consider the problem having regard to wider mitigation strategies. These include statutory prohibitions against unauthorized disclosure that apply directly to contractors, significant penalties for breach of FOIPPA, express blocking provisions in FOIPPA, or a Canada-US accord on the matter.

It is true that the values embodied in the Charter must not be overlooked:

> In a very real sense, contracting out the information to a firm subject to the Patriot Act will deprive British Columbians of their privacy rights under Canadian law. These individuals have both a statutory and constitutional right to determine how their personal information will be disseminated. Their data is not to be the subject of search and seizure unless the

58 Submission of BCGEU (6 August 2004) p. 58.
59 Examples that come to mind are patient medical records held by hospitals and library loan records held by universities.

> requirements of reasonableness, as determined on a Canadian standard, are met. The privacy rights of these individuals must be determined by Canadian judges, applying Canadian law, which, in the balancing process, reflects Canadian interests and Canadian values. Depriving these individuals of this entitlement simply cannot be "reasonable".
>
> Whether or not the contracting out is sufficient to constitute a breach of these individuals' ss. 7 and 8 Charter rights to privacy, it is clear that any ambiguity in the FOIPPA statute must take into account the Charter value of privacy in certain types of information. In our view, it can never be reasonable to take a step that may have the effect of derogating from the ability of the Constitution to protect British Columbians' rights to privacy.[60]

As we have seen, however, a ban on using contractors would have to be wider than firms that could be the subject of a FISA order. It would also have to cover Canadian businesses that could be the target of clandestine access by an organization or individual that could be the subject of a FISA order—a US parent or other US-related company or a US-based employee or sub-contractor. It would also have to cover US consultants who, if contracted to provide services to a public body, could become the subject of a FISA order requiring them to clandestinely access information held by the public body. It would also have to cover US nationals who are employed in British Columbia by a contractor or a public body and could become the subject of a FISA order.

The closer one looks, the clearer it becomes that disclosure of information in British Columbia under an extraterritorial FISA order would involve illegal and surreptitious conduct that could be perpetrated in relation to contractors and public bodies alike. It also becomes clearer that it is not a sensible and proportionate response to ban the many legitimate relationships that might be associated with this risk, but it is a sensible, proportionate and necessary response to institute rigorous mitigating measures against this insidious form of unauthorized access.

Government efficiency and personal privacy

Before moving to chapters dealing with the plausibility of the Foreign Intelligence Surveillance Court (FIS Court) issuing a FISA order that extends to information held in British Columbia and our recommendations for action, we must briefly address one further argument that was raised about section 30 of FOIPPA.

In analyzing what constitutes reasonable security arrangements under section 30, the BC government contended that "one must consider the tangible benefits of outsourcing public body functions, including reducing costs for government and improving the quality of services to the public".[61] It elaborated that

> any determination as to whether outsourcing initiatives comply with section 30 of the FOIPP Act must consider the benefits of such initiatives including:
> - Increasing operational flexibility; for instance, a private company may be able to provide better operational flexibility through access to a wider range of skills and experience than public bodies have, or can afford, and an increased ability to respond to operational demands;
> - The benefit of transferring risks to the private sector, such as system development risks and the costs of overruns, and service level risks;
> - Making the best use of limited resources available to a public body;
> - Improving client service;
> - Reducing operating costs;
> - Transferring the costs of asset acquisition;
> - The ability to focus on the core business of the public body;
> - Cost certainty;
> - Potential improvements in management reporting; the

60 Submission of BCGEU (6 August 2004) p. 56.
61 Submission of Government of British Columbia (23 July 2004) p. 26.

> private sector can potentially provide improvements in the quantity, quality and timeliness of management reporting available for operational decision making; and
> - Avoidance of significant future capital costs.[62]

We note, first, that the British Columbia government's submission did not in fact establish "tangible benefits" of outsourcing in any meaningful or measurable way. In fairness, though, the process leading to this report was not a particularly appropriate forum for that purpose.

Second, we see danger in allowing the question of whether, or the degree to which, outsourcing a public body function is a cost saving for the public body to be a driving factor in determining the adequacy of security measures for the personal information involved. One aspect of providing less costly service could obviously be to provide less security for personal information. Lax security protections could be reasonable because they cost less. This result would be a formula for rapid, unprincipled, erosion of security protection under section 30—essentially a race to the bottom.

Third, in the area of health care especially, it is obviously inappropriate to conceptualize the benefit of personal privacy as a cost that impedes government efficiency. We are reminded of this by the submission of the British Columbia Medical Association:

> Physicians and the public place high importance on the protection of personal health information. Without confidence that privacy will be maintained, patients may refrain from disclosing critical information; may be reluctant to provide their consent to use their personal health information for research purposes; may lie about their health status or may simply not seek treatment. A 1999 survey by the [Canadian Medical Association] found that 11% of the public held back information from a health care provider because they were concerned about whom it would be shared with, or for what purposes it would be used…
> …
> In summary, the BCMA has serious concerns about the privacy of personal health information, particularly if a U.S. based firm were to take over the administrative functions of MSP and Pharmacare. The personal health information of B.C. citizens could be accessed by American agencies such as the FBI as a result of provisions of the USA Patriot Act. This could have potentially devastating effects including the misuse of personal information, along with a greater reluctance among patients to disclose information, thus, eroding quality of care and the patient-physician relationship.
>
> If the practice of outsourcing government functions to U.S. based companies is to continue, safeguards must be in place, including written statements that exempt foreign agencies such as the FBI from accessing personal information under any circumstance…[63]

Personal privacy is a fundamental value in a democratic society. Government efficiency is important too, of course, but it is a tool in the service of other objectives. Efficiency will describe the quicker and most opportunistic way to proceed and sheer efficiency may occasionally serve fundamental values well. But often it will not. It may be difficult or impossible to restore privacy when it is compromised by efficiency—including the sense of privacy in our day-to-day activities that we so cherish yet also tend to take for granted. Efficiency interests, on the other hand, can be accommodated by various means and must not be confused with or trump fundamental values that governments exist to serve and protect.

Conclusion

In this chapter, we have discussed the legal obligations of British Columbia public bodies to protect personal information under their control. Disclosure of personal information in response to

62 *Ibid.* p. 27.
63 Submission of British Columbia Medical Association (12 July 2004) pp. 1 and 3.

a FISA order or a national security letter would be unauthorized disclosure under sections 30 and 33 of FOIPPA. US authorities engaged in foreign intelligence gathering would not be likely to use MLAT, for practical and legal reasons, and it is not clear that US authorities would have available to them, or would necessarily use, other information transfer methods that are recognized in MLAT and section 33 of FOIPPA.

We have also concluded that, as it is a reasonable possibility that a FISA order or a national security letter would be sought or issued against an individual in the US or an organization that has presence in the US, requiring it to produce records in British Columbia, section 30 of FOIPPA requires reasonable, but not absolute, security against this risk.

We have concluded that a ban on outsourcing would not be a practical or effective response to this risk, but that other mitigating measures should be implemented at legislative, contractual and practical levels.

Finally, we have observed that government efficiency is not on par with personal privacy—it is a tool in the service of other objectives, including the protection of personal privacy. We will now turn, in the next chapter, to consider the likelihood that the FIS Court would issue a FISA order in relation to information in British Columbia that is, through outsourcing, in the hands of a US-linked contractor.

10 ORDERS FOR DISCLOSURE: POTENTIAL USE OF THE USA PATRIOT ACT IN CANADA

The first question posed in the Request for Submissions is whether the USA Patriot Act permits 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 USA-linked private sector service providers and, if so, under what conditions that can occur. We have already noted that, if personal information is located outside British Columbia, it is subject to the law that applies where it is found, regardless of the terms of the outsourcing contract. Chapter 5 provides a summary of USA Patriot Act amendments to the Foreign Intelligence Surveillance Act (FISA). The question this report focuses on is whether an order under the amended FISA could reach directly into British Columbia without the intervention or protection of Canadian law or processes, including the Freedom of Information and Protection of Privacy Act (FOIPPA).

Submissions from the British Columbia government and some information technology corporations conclude that US authorities would use alternative avenues rather than seeking access to personal information in Canada using the powers conferred by the USA Patriot Act. The Information Technology Association of Canada (ITAC) summarizes its position this way:

> [T]he Patriot Act simply does not provide an efficient or effective method of obtaining that information. Rather, given all of the legal and practical obstacles, common sense suggests that pre-existing methods of international criminal investigation such as letters rogatory, the Canada-United States [Mutual Legal Assistance Treaty] and informal requests for assistance (all of which require the cooperation of the Canadian government and Canadian courts) are much more likely to be employed.
>
> It is therefore important to avoid over-emphasizing the relevance of the Patriot Act to situations in which public bodies in British Columbia outsource certain functions to "USA-linked" partners. In a very real sense, the Patriot Act should not be a substantial concern at all in those circumstances.[1]

We disagree. In Chapter 9, we explained that US authorities seeking access to personal information in Canada would be unlikely to make use of the Mutual Legal Assistance Treaty or letters of request to Canadian courts when the Foreign Intelligence Surveillance Act (FISA) provides an alternative avenue. As discussed in Chapter 6, USA Patriot Act amendments to FISA alter the requirements for applications for court orders compelling the disclosure of records held by US-linked companies in Canada. In this chapter we discuss the factors likely to be considered by the Foreign Intelligence Surveillance Court (FIS Court) when it reviews such applications. We conclude that, while there is no way of predicting with certainty what approach the FIS Court may take, there is evidence to

1 Submission of Information Technology Association of Canada (28 May 2004) p. 23.

suggest that current arrangements for the protection of personal information in British Columbia are unlikely to act as a firm disincentive, in all cases, against the issuance of FIS Court orders compelling disclosure.

There is general consensus in the submissions that the FIS Court could, under FISA, order a US corporation to produce records held in Canada by its Canadian subsidiary. There is no general consensus, however, about whether the FIS Court would make such an order in the face of a Canadian law prohibiting disclosure. We will now discuss the existing US case law said to provide the closest analogies to such orders that could be made by the FIS Court, accepting the consensus that the FIS Court would likely apply the same principles. We will then consider the balancing test that US courts use in deciding whether to order disclosure of records held outside the US, including where foreign law prohibits disclosure.

Disclosure of Foreign-Located Records Where Control is Shown

US courts have frequently upheld subpoenas ordering a corporation to disclose records located outside the US but under the corporation's control, even where they compel disclosure of records located in countries whose law prohibits disclosure.[2] US courts have also been willing to order disclosure of records held outside the US for the purpose of US proceedings, as long as a person or corporation subject to the US court's jurisdiction has control of those records.

In such cases, the US-located corporation at which the disclosure requirement is directed must, on penalty of being found in contempt of court, obtain the records from abroad and turn them over. Contempt fines for failing to comply have in some cases been in the millions of dollars.[3]

In these cases, the subpoena or court order has not been enforced through a foreign court or a treaty. It is enforced directly by the US court using its power to punish non-compliance through contempt of court proceedings in the US against persons in the US. It is the threat of contempt of court penalties that leads to compliance and results in the subpoena or order having effect outside the US. In the case of FISA orders, it is a felony not to comply with the order.

Control over records

As the British Columbia government's submission acknowledges, in these cases, control of the records located outside the US is the key.[4] The government also contends, however, that a US court must have what is known in US law as "personal jurisdiction" over the person who has the records before disclosure can be ordered and that the FIS Court is not likely to assert jurisdiction over a Canadian corporation that is affiliated with a US-located corporation where the Canadian corporation operates and is located outside the US.[5] The government says the FIS Court is unlikely to assert personal jurisdiction over a Canadian corporation that has only minimal contacts with the US and says that, if a US court on this basis decided it does not have personal jurisdiction over the Canadian company, a FISA order cannot be served or be effective.[6]

2 See, for example, *In re Grand Jury Proceedings (Bank of Nova Scotia)*, 740 F.2d 817 (11th Cir. 1984). The grand jury is a feature of the US justice system that has no current counterpart in Canada. A grand jury investigates possible criminal activity and has the power to issue subpoenas compelling individuals to testify or compelling production of records.

3 In the case of *In re Grand Jury Proceedings (Bank of Nova Scotia), ibid.* the Bank was fined $1 825 000 for contempt of court arising from its failure to comply with the grand jury subpoena.

4 Submission of Government of British Columbia (23 July 2004) pp. 11-12.

5 *Ibid*. pp. 12-13.

6 *Ibid*. pp. 12-13, 32-33. Although the BC Government submission does not mention it, the submission of the American Civil Liberties Union (10 August 2004) says that, if foreign actions cause harm in the US, the US may assert jurisdiction over the foreign conduct and foreign actors responsible (p. 8). The ACLU refers to, for example, US anti-trust enforcement cases in which US courts have asserted jurisdiction where actions abroad have caused harm in the US, citing *In re Investigations of World Arrangements with Relation to the Production, Transportation, Refining and Distribution of Petroleum,* 13 F.R.D. 280 (D.D.C. 1952). We have chosen not to focus on this issue for the purposes of this report.

The British Columbia government is correct to recognize that control of records located outside the US is the key. It is also true that a Canadian subsidiary of a US-located corporation may not be subject to the personal jurisdiction of a US court. However, if the US parent controls records in the Canadian subsidiary's possession, the US court may still compel the US parent to get the records and produce them.

There are many examples of law enforcement and civil litigation matters where US courts have required US corporations to obtain and produce, in the US, records that are held outside the US but are controlled by the US-located corporation. In such cases, the US courts consider their personal jurisdiction over the US-located corporation to be sufficient to require production regardless of whether the court has personal jurisdiction over the party outside the US. As one court has said,

> personal jurisdiction and "control" of documents are distinct issues in that [the] court can compel discovery of documents in "control" of a party although in "possession" of a person over whom there is no personal jurisdiction.[7]

It is, therefore, clear that US courts do not order disclosure on the basis of jurisdiction over the foreign corporation itself. As long as the court has jurisdiction over a US corporation that controls records located abroad, the court can order disclosure.[8] Location of the records is not the issue[9]—a US court will not permit a US-located corporation to resist producing records simply because the records are located outside the US.[10]

When control is being determined by a US court, its meaning is an issue of US law.[11] US courts use a number of factors to determine whether a US corporation controls records located outside the US. Control is not limited to legal ownership or actual physical possession of records. In deciding whether to order a corporation to obtain records in the physical possession of a foreign affiliate and disclose them in the US, US courts have interpreted the concept of control "broadly as the legal right, authority or practical ability to obtain the materials sought upon demand".[12]

Whether a US-located corporation controls records held abroad by its subsidiary depends on a number of factors, including the degree of ownership and control the parent exercises over the subsidiary, whether the two corporations operate as one, demonstrated access to records in the ordinary course of business and an agency relationship.[13] Courts have held that a US parent corporation will, unless it proves otherwise, be held to control records located abroad that it requires in the ordinary course of business.[14] Similarly, US courts have found that

7 *Dietrich v. Bauer,* 2000 U.S. Dist. LEXIS 11729 (S.D.N.Y. 2000) at 10-11, citing *Afros S/P.A. v. Krauss-Maffei Corp.,* 113 F.R.D. 127, 129 (D. Del. 1986).
8 *Dietrich v. Bauer, ibid*. at 6-7. US federal rules of civil procedure expressly provide that a party or non-party to US litigation can be ordered to produce records in its possession, custody or control: Fed.R.Civ.P. 34 and 45. The test for control is the same regardless of whether the records are sought from a party or a non-party: *Alcan International Ltd. v. S.A. Day Mfg. Co., Inc.,* 176 F.R.D. 75 at 78 (W.D.N.Y. 1996).
9 *In re Marc Rich & Co., A.G.*, 707 F.2d 663 at 667 (2nd Cir. 1983). Also see *In re Grand Jury Subpoenas duces tecum addressed to Canadian International Paper Company et al.*, 72 F.Supp. 1013 (S.D.N.Y. 1947).
10 *United States v. Chase Manhattan Bank,* N.A., 584 F. Supp. 1080 at 1085 (S.D.N.Y. 1984).
11 *Ssangyong Corp. v. Vida Shoes Int'l, Inc.*, 2004 U.S. Dist. LEXIS 9101 at 4-5 (S.D.N.Y. 2004). Section 3(1) of FOIPPA provides that FOIPPA only applies to a record "in the custody or under the control of a public body". In light of US cases confirming that the issue of whether a US corporation has control of records located abroad is a question of US law, the FOIPPA control test is unlikely to be relevant for a US court making a control determination.
12 *Bank of New York v. Meridien Biao Bank Tanzania,* 171 F.R.D. 135 at 146 (S.D.N.Y. 1977). See also, *Dietrich v. Bauer, supra* note 7 at 7, citing, among other decisions, Asset Value Fund, Ltd. v. The Care Group, Inc., 1997 U.S. Dist. LEXIS 19768 at 9 (S.D.N.Y. 1997).
13 *Dietrich v. Bauer, ibid*. at 7-8.
14 *Cooper Industries, Inc. v. British Aerospace, Inc.,* 102 F.R.D. 918 at 920 (S.D.N.Y. 1984).

> a parent corporation has a sufficient degree of ownership and control over a wholly-owned subsidiary that it must be deemed to have control of documents located with that subsidiary.[15]

It has even been said that a US corporation will control a foreign corporation if the US corporation can, directly or indirectly, through another corporation or corporations, elect a majority of the directors of the foreign corporation.[16] The *Restatement (Third) of the Foreign Relations Law of the United States* says this:

> Courts in the United States have generally held United States corporations responsible for production of documents located abroad in the possession of their foreign branches or subsidiaries, unless a defence, such as an effective blocking order, is applicable where the information is located.[17]

It is not possible, in the absence of details of specific outsourcing arrangements, to say whether personal information located in British Columbia is in the control of a US parent corporation on the basis of the ownership or other tests applied by some US courts. We consider, in any event, that the US federal court decisions in which control over foreign records has been found on the basis of the parent-subsidiary relationship alone must be given some weight. We adopt, therefore, the working assumption that control, as a matter of US law, may be found on the basis of corporate relationship alone, regardless of the contractual or practical arrangements between the public body and the service provider or the public body and US-located parent corporation.

Effect of contractual prohibitions and security arrangements

We do not suggest that public bodies cannot or should not implement contractual or practical arrangements relating to control. To the contrary, we recommend that such arrangements be put into place. This is because, despite the cases in which corporate ownership is enough to establish control over records, other cases suggest that such measures might influence the control issue.

For one thing, the US cases usually deal with business records of a foreign subsidiary. The courts have found that the parent company controls a subsidiary's business records that are accessible to the US-located parent in the ordinary course of business. In the case of outsourcing of public services, by contrast, personal information contained in records possessed by the US-linked service provider is third-party personal information. We are not prepared to say a US court would ignore outsourcing agreement provisions and practical arrangements that clearly preclude the US-located parent from having access to the personal information for any purpose at all. It is, again, difficult to predict how the FIS Court might approach the matter, but there is reason to believe that corporate ownership might not be the sole litmus test of control over records under US law.

Any contractual and practical measures to keep personal information out of the control of a US-located parent corporation would also speak to British Columbia public policy respecting the privacy of personal information. This is important because, even if a US court decides that records located outside the US are controlled by a US-located corporation, it will apply a balancing test to decide whether it

15 *Dietrich v. Bauer, supra* note 7 at 8-9, citing several decisions from various US federal courts. Also see, for example, *In re Uranium Antitrust Litigation*, 480 F.Supp. 1138 (N.D. Ill. 1979).

16 *In re Investigations of World Arrangements with Relation to the Production, Transportation, Refining and Distribution of Petroleum, supra* note 6 at 285.

17 *Restatement (Third) of the Foreign Relations Law of the United States* § 442 note 10 (1986).

should order disclosure in the face of foreign law that prohibits disclosure.

We discuss below the balancing test US courts apply in deciding whether to order disclosure of foreign records. Before doing so, however, we will address the contention in some submissions that, apart from the balancing test, other procedural or policy safeguards exist that make it unlikely that US authorities will seek to directly enforce a FISA order in Canada.

Are There Other Safeguards?

The British Columbia government, EDS Canada Inc. (EDS), the FBI and the US Department of Homeland Security (DHS) all contend that protections are in place to guard against inappropriate extraterritorial application of FISA orders. Neither the FBI nor the DHS provides details about these protections. The British Columbia government suggests that US government lawyers are required, before they seek to force disclosure of records abroad, to seek approval from the Office of International Affairs (OIA) of the US Department of Justice. The British Columbia government says this stems from recognition of the distaste expressed by other countries for extra-territorial application of US subpoenas. The British Columbia government adds that the US is now much more sensitive than it was to objections by other countries to extra-territorial application of US subpoenas and is less likely to use them than in the past. It says the use of FISA proceedings will be similarly constrained.[18] EDS makes similar points in its submission.[19]

No basis is offered for the claim that the US government and its institutions are, after September 11, more deferential to foreign sensibilities about extra-territorial application of US laws. In fact, US cases decided before September 11 show that, even then, any concerns about extra-territorial application of US law were often overcome. We see no reason to believe that US courts—including the FIS Court—will be more, not less, inclined after September 11 to shrink from using lawful means to obtain intelligence information from abroad. We also note that, since its enactment in 1978, FISA has specifically distinguished between the interests and rights of US persons and the interests of non-US persons.

Nor does the British Columbia government explain why it believes that the US government's policy to require federal prosecutors to work through the OIA applies to FISA processes and FISA orders. The government points to section 279 of the Criminal Resources Manual of the US Department of Justice and its controls on seeking records abroad. We note, however, that this 1997 version of the manual specifically relates to criminal prosecutions and not national security activities. We are aware of no reason to believe that the FBI and its lawyers may or must follow these rules in seeking a FISA order for intelligence purposes alone.

We have also considered Executive Order 12333,[20] to which the relevant FISA section refers, and the required guidelines approved in 2003 by the US Attorney General (National Security Investigations (NSI) Guidelines).[21] Neither sets out procedural safeguards or policy requirements relating to use of FISA orders to obtain records located abroad, although we note that the published version of the Attorney General's guidelines has been heavily redacted on

18 Submission of Government of British Columbia (23 July 2004) pp. 11-15, 36-37.
19 Submission of EDS Canada Inc. (19 July 2004) pp. 31-35 (legal opinion of Steptoe & Johnson LLP).
20 Executive Order 12333—United States Intelligence Activities 46 FR 59941, 3 CFR, 1981 Comp. A copy of the Order is available on the US Central Intelligence Agency website: www.cia.gov
21 The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (31 October 2003) Reproduced on the website of the US Department of Justice, Office of Legal Policy: www.usdoj.gov/olp/

national security grounds. Nor are any safeguards offered in the rules governing the FIS Court's processes, which only recently came to public attention through a US access to information request. By their terms, the rules only allow specially designated US government lawyers and agents to appear or participate in hearings held in private before the court.[22]

EDS contends that FBI officials are deterred from inappropriately obtaining FISA orders because they might be prosecuted under US law if they were to do so.[23] We do not question the good faith of FBI officials in exercising their power to seek FISA orders, but we note that the British Columbia government's submission indicates only one FISA application of the thousands that have been made to the FIS Court has ever been denied.[24] Although it appears the number of FISA applications increased substantially in 2003, according to the annual FISA report that the US Attorney General is required to make to Congress, only 4 of 1,727 FISA applications made in that year were rejected by the FIS Court.[25]

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, this report proceeds on the basis that US authorities are unfettered in their ability to seek such an order and may do so in some circumstances. One of the recommendations we make in Chapter 11 is that the British Columbia government, 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.

We will now discuss the balancing test for disclosure of records located outside the US.

The Balancing Test for Compelling Disclosure

A number of the submissions referred to the balancing test that US courts apply in deciding whether to order disclosure from outside of US. The British Columbia government, for example, pledged in its submission to enact legislation precluding disclosure of records under FISA, recognizing that a US court will consider such a law as part of the balancing test.[26] The submission of EDS contends, without qualification, that a US court would honour a Canadian statutory prohibition against disclosure,[27] while the BCGEU and ACLU submissions express the opposite view.[28]

A US order for foreign disclosure may or may not be enforced where foreign (including Canadian) law prohibits disclosure. In some cases US courts have been uneasy about enforcing disclosure abroad[29] because they acknowledge that the laws of a country do not generally extend beyond its borders. It is recognized that attempts to enforce laws outside a country are highly unpopular in the international community. As noted in the *Restatement (Third) of the Foreign Relations Law of the United States*:

22 US, Rules of the Foreign Intelligence Surveillance Court, r. 9; a copy of this document is available on the ACLU website: www.aclu.org and on the website of the Federation of American Scientists: www.fas.org.
23 Submission of EDS Canada Inc. (19 July 2004) p. 28 (legal opinion of Steptoe & Johnson LLP).
24 Submission of Government of British Columbia (23 July 2004) p. 29, note 38.
25 The Electronic Privacy and Information Center has published a summary of information taken from the annual FISA reports on its website: www.epic.org. A list of the annual FISA reports is available on the website of the Federation of American Scientists: www.fas.org.
26 We understand the proposed amendments to FOIPPA in Bill 73 to be blocking legislation in this regard: Freedom of Information and Protection of Privacy Amendment Act, 2004, 5th Sess., 37th Parl., BC, 2004 (3rd reading 19 October 2004).
27 Submission of EDS Canada Inc. (19 July 2004) pp. 31-32 (legal opinion of Steptoe & Johnson LLP).
28 Submissions of BCGEU (6 August 2004) p. 49 and American Civil Liberties Union (10 August 2004) pp. 9-11.
29 See, for example, *In re Sealed Case*, 825 F.2d 494 at 497-99; (D.C. Cir. 1987) 498-499.

> No aspect of the extension of the American legal system beyond the territorial frontier of the United States has given rise to so much friction as the requests for documents in investigation and litigation in the United States. As of 1986, some 15 states had adopted legislation expressly designed to counter United States efforts to secure production of documents situated outside the United States….
> The common theme of foreign responses to United States requests for discovery is that, whatever pre-trial or investigative techniques the United States adopts for itself, they may be applied to persons or documents located in another state only with permission of that state. The United States position, on the other hand, has been that persons who do business in the United States, or who otherwise bring themselves within United States jurisdiction to prescribe and to adjudicate, are subject to the burdens as well as the benefits of United States law, including the laws on discovery. This section [of the *Restatement (Third)*] generally supports the United States position, subject, however, to the principle of reasonableness.[30]

Our review of US law leads us to conclude that US courts have been willing to enforce disclosure of foreign-located records sought for use in the US and in some cases have done so even where foreign law prohibits disclosure. In deciding whether to order disclosure from abroad, a US court balances a number of factors in deciding whether the US interest in disclosure outweighs the interest in avoiding extra-territorial application of US subpoenas or court orders.[31] As one US court has observed,

> [m]echanical or overbroad rules of thumb are of little value; what is required is a careful balancing of the interests involved and a precise understanding of the facts and circumstances of the particular case.[32]

Among the various factors a court will consider are those described in the *Restatement (Third)* as follows:[33]

§442. REQUESTS FOR DISCLOSURE: LAW OF THE UNITED STATES

(1) (a) A court or agency in the United States, when authorized by statute or rule of court, may order a person subject to its jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information or the person in possession of the information is outside the United States.

(b) Failure to comply with an order to produce information may subject the person to whom the order is directed to sanctions, including finding of contempt, dismissal of a claim or defense, or default judgment, or may lead to a determination that the facts to which the order was addressed are as asserted by the opposing party.

(c) In deciding whether to issue an order directing production of information located abroad, and in framing such an order, a court or agency in the United States should take into account the importance to the investigation or litigation of the documents or other information requested; the degree of specificity of the request; whether the information originated in the United States; the availability of alternative means of securing the information; and the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located.

(2) If disclosure of information located outside the United States is prohibited by a law, regulation, or order of a court or other authority of the state in which the information or prospective witness is located, or of the state of which a prospective witness is a national;

30 *Restatement (Third) of the Foreign Relations Law of the United States, supra* note 17 at note 1.
31 See, for example, *First Am. Corp. v. Price Waterhouse LLP*, 154 F.3d 16 at 22 (2d Cir. 1998). In the case *In re Grand Jury Proceedings (Bank of Nova Scotia), supra* note 2 at 26-27, the court considered similar factors as set out in the *Restatement (Second) of the Foreign Relations Law of the United States* § 40 (1965).
32 *United States v. First Nat'l City Bank,* 396 F.2d 897 at 901 (2d Cir. 1968).
33 See, for example, *Volkswagen, A.G. v. Valdez*, 909 S.W.2d 900 at 902 (Tex. Sup. Ct. 1995).

> (a) a court or agency in the United States may require the person to whom the order is directed to make a good faith effort to secure permission from the foreign authorities to make the information available;
>
> (b) a court or agency should not ordinarily impose sanctions of contempt, dismissal, or default on a party that has failed to comply with the order for production, except in cases of deliberate concealment or removal of information or of failure to make a good faith effort in accordance with paragraph (a);
>
> (c) a court or agency may, in appropriate cases, make findings of fact adverse to a party that has failed to comply with the order for production, even if that party has made a good faith effort to secure permission from the foreign authorities to make the information available and that effort has been unsuccessful.[34]

While a court may consider other factors, we are proceeding on the assumption that those set out in §442(1)(c) of the *Restatement (Third)* are the core factors.

It should be noted here that the factors set out in the *Restatement (Third)* have been fashioned for the purposes of US litigation or investigations where foreign subsidiaries of companies subject to the US court's jurisdiction hold relevant records abroad. These cases involve proceedings in ordinary US courts. We cannot say with certainty what approach the special FIS Court would apply to the extra-territorial enforcement issue in relation to personal information records located in British Columbia that are involved in the outsourcing of public services to US-linked service providers.

There is, however, some consensus in the submissions that the FIS Court would find that it has the authority to order a US parent of a Canadian subsidiary to obtain and disclose records located in Canada but controlled by the US parent. We accept this view. We also accept the view expressed in a number of submissions that the FIS Court is likely to consider some or all of the factors in the *Restatement (Third)* in deciding whether to compel production of records located in Canada under a FISA order.

The fact that only two FISA decisions have ever been released—neither of which is relevant here—makes our assessment of how the FIS Court might apply the *Restatement (Third)* factors necessarily somewhat speculative. We can only suggest, applying the approach in cases decided under other US laws, how the FIS Court might apply them.

Specificity of the request for disclosure

The British Columbia government submission refers to cases in which the US court has said that the scope of a disclosure subpoena or order must be reasonable.[35]As we understand this, the British Columbia government is referring to cases in which US courts have restricted the scope of subpoenas to records reasonably related to the investigation or proceeding under way. The government appears to be suggesting that a comparable scope restriction, which depends on the facts of each case, will safeguard British Columbians' personal information in the context of outsourcing because any FISA order that might be issued with effect in British Columbia would be similarly limited.

The ACLU's submission also suggests that the FIS Court might require proposed orders for disclosure of records to be specific. It maintains that FISA allows for broad records requests, but

34 *Restatement (Third) of the Foreign Relations Law of the United States, supra* note 17, § 442.

35 Submission of Government of British Columbia (23 July 2004) p. 12; however, the BC Government acknowledges that it is uncertain whether the FIS court would apply the same legal principles in the context of FISA that an ordinary US court would apply in the context of a grand jury subpoena.

notes that "[c]ourts have struck down sweeping demands for information that could not meet the test of being 'reasonably relevant' to an actual, authorized investigation."[36] We also acknowledge that the US Department of Justice rules governing FISA applications and its FISA minimization requirements, which speak to relevance and minimal collection, could influence the FIS Court to impose a comparable standard of specificity and reasonableness on FISA orders.

Origin of the information sought

We mentioned earlier the prospect that the FIS Court might account for the fact that a US-linked contractor possesses records for the limited purpose of performing services and has no control over the records. In some US cases, the court has considered whether the records in question originated in the US or abroad. It is reasonable to expect a US court to look unfavourably on any attempts to avoid disclosure by removing US records from the country. However, this would not be the case with personal information of British Columbians involved in outsourcing. The records would originate in British Columbia and be in the possession of the US-linked contractor only for the purposes of the outsourcing.

Importance of the records to the US investigation

US courts will consider the importance of the records to the litigation or proceeding for which they are sought. The more important the requested records are to the litigation or other proceeding, the more likely the court will issue an order for disclosure. For example, in *Volkswagen, AG v. Valdez*, applying the balancing test in § 442 of the *Restatement (Third)*, the court held that the records sought were not important to the US litigation because the plaintiffs already had previous versions of the same information.[37] Similarly, in *Minipeco, SA v. ContiCommodity Services, Inc.*,[38] the court was influenced by the fact that much of the information in documents sought from Switzerland was not relevant to the litigation and noted that a great deal of commercial information of third parties not involved in the case would be revealed.

The FIS Court may decline to issue a FISA order for disclosure of personal information records in Canada if it views the records as only marginally relevant to the purpose for which they are sought. Although it has been a factor of influence in some conventional litigation cases, it might be difficult to apply to the more diffuse context of a FISA investigation where no investigation of a specific offence is involved.

Existence of alternative means of obtaining the information

The availability of adequate alternatives for obtaining the information sought can weigh against ordering disclosure in the face of a prohibition under foreign law.[39]We have already dealt with the contention that MLAT is the default information gathering mechanism for US authorities. MLAT provides for the continued use of other agreements, arrangements or practices and, in any event, is not available where US authorities seek to gather information for purposes other than an investigation or prosecution for an offence as defined by MLAT.

We have also noted that Canadian and US authorities can and do use other arrangements to share information for intelligence and national security

36 Submission of American Civil Liberties Union (10 August 2004) p. 11.
37 *Volkswagen, A.G. v. Valdez, supra* note 33.
38 *Minipeco, SA v. ContiCommodity Services, Inc.*, 116 F.R.D. 517 (S.D.N.Y. 1987)
39 See *Volkswagen, A.G. v. Valdez, supra* note 33.

purposes. It is possible that the FIS Court, assuming it was aware of such other arrangements, might decline to order disclosure from Canada where bilateral arrangements could be used to get the information.

Good faith of the person from whom disclosure is sought

US courts have considered the good faith of the US-located person resisting disclosure in trying to get the information being sought. Some courts address this factor only in deciding whether to enforce the disclosure order, while others consider it when deciding whether to order disclosure in the first place.

Good faith is a consideration where foreign law—such as a banking secrecy law—requires the party resisting disclosure to get consents from foreign parties whose information is affected. In *Société Internationale Pour Participations Industrielles Et Commerciales, S. A. v. Rogers*,[40] for example, the US Supreme Court found that the affected party had made extensive efforts to get records from Switzerland but faced criminal prosecution there if it turned the records over in response to the US court order. Similarly, in *Minipeco, SA v. ContiCommodity Services, Inc.*,[41] the court noted that the affected party had made extensive efforts to obtain documents abroad, including by getting consents from third parties that allowed disclosure of their records. Its efforts clearly influenced the court's decision not to order further disclosure.

By contrast, in *Ssangyong Corp. v. Vida Shoes Int'l, Inc.*,[42] the court noted that the party resisting disclosure had, for three months, made no attempt to comply with the disclosure requirement. This weighed in favour of requiring disclosure of banking records despite a common law rule in Hong Kong requiring banking confidentiality.

Competing interests of the US and Canada

As indicated above, the *Restatement (Third)* indicates the court should weigh the interests of the US and the foreign jurisdiction in deciding whether to order disclosure. The following passage from the comments on § 442(1)(c) of the *Restatement (Third)* is helpful in explaining how a US court should assess this factor:

> In making the necessary determination of foreign interests under Subsection (1)(c), a court or agency in the United States should take into account not merely a general policy of the foreign state to resist "intrusion upon its sovereign interests," or to prefer its own system of litigation, but whether producing the requested information would affect important substantive policies or interests of the foreign state. In making this determination, the court or agency will look, [among other things], to expressions of interest by the foreign state, as contrasted with expressions by the parties; to the significance of disclosure in the regulation by the foreign state of the activity in question; and to indications of the foreign state's concern for confidentiality prior to the controversy in connection with which the information is sought. …
>
> In making the necessary determination of the interests of the United States under Subsection (1)(c), the court or agency should take into account not merely the interest of the prosecuting or investigating agency in the particular case, but the long-term interests of the United States generally in international cooperation in law enforcement and judicial assistance, in joint approach to problems of common concern, in giving effect to formal or informal international agreements, and in orderly international relations. …[43]

As this passage indicates, the US court must balance US interests against foreign interests. A

40 *Société Internationale Pour Participations Industrielles Et Commerciales, S. A. v. Rogers,* 357 U.S. 197 (1958).
41 *Minipeco, SA v. ContiCommodity Services, Inc., supra* note 38.
42 *Ssangyong Corp. v. Vida Shoes Int'l, Inc., supra* note 11.
43 *Restatement (Third) of the Foreign Relations Law of the United States, supra* note 17, comment c.

significant issue is whether a foreign legal prohibition against disclosure of the requested records will overcome US interests in disclosure.

Canadian statutory restrictions on disclosure

As noted earlier, the submission of EDS says that where Canadian law restricts disclosure of personal information, a US court will honour that restriction.[44] As the BCGEU points out, however, the case EDS cites as the "closest case on point" in support of its proposition[45] was later disavowed by the same court.[46] Our research discloses that, where competing US interests favour disclosure, a US court may order it despite the existence of a foreign law prohibiting disclosure.[47] As one court put it, "The possibility of civil or criminal sanction [abroad] will not necessarily prevent enforcement of a subpoena."[48]

In fact, US courts have, in the face of foreign laws prohibiting disclosure, been willing to enforce disclosure of records for the purposes of enforcing US criminal fraud laws[49] and securities laws.[50] Even in purely private litigation, where no US government interest is directly involved, US courts have in some cases given more weight to the general US interest in resolving litigation in US courts than to foreign laws prohibiting disclosure of the records.[51]

We do agree, however, with the following statement from the submission of the ACLU:

> The most important portion of the balancing test is the weighing of the interests of the two states involved. Courts have tended to be extremely deferential in cases where the state interest is a criminal prosecution. Because requests involving the Patriot Act apply not only to criminal acts but to terrorism (a crime that all nations have an important interest in resolving and that tends to be international in scope), it is likely that a U.S. court would give significant weight to this interest. Courts have also recognized that the other nations have a legitimate and important privacy interest in their citizens' personal information, but have tended to be sceptical of secrecy laws (general in the context of bank records) when they interfere with criminal investigations or strong state interests.
>
> …
>
> As a practical matter, cases brought by the government (especially those involving violations of criminal law) have tended to favor the disclosure of records because courts accord them great weight under the "significant government interest" prong of the test. While it is difficult to predict the access that U.S. courts will grant to foreign records, it is likely that if the U.S. government claims that its interest lies in preventing terrorist activity and it attempts to limit the amount of the request, a court will find that it has satisfied the prongs of the balancing test and should be granted the records it seeks.[52]

We agree that, although the facts of each case determine the outcome, particularly in the post-September 11 world, the amendments to FISA appear to demonstrate that the scope of what are considered to be vital US national interests in ensuring national security and protecting against terrorism has grown.

44 Submission of EDS Canada Inc. (19 July 2004) p. 31 (legal opinion of Steptoe & Johnson LLP).
45 *Ings v. Ferguson*, 282 F.2d 149 (2d Cir. 1960).
46 *United States v. First Nat'l City Bank, supra* note 31; also see *Minipeco, S.A. v. ContiCommodity Services, Inc., supra* note 38.
47 *In re A Grand Jury Subpoena dated August 9, 2000*, 218 F. Supp. 2d 544 at 554 (S.D.N.Y. 2002). Also see *Compagnie Française d'Assurance Pour le Commerce Extérieur v. Phillips Petroleum Co.,* 105 F.R.D. 16 (S.D.N.Y. 1984).
48 *In re A Grand Jury Subpoena dated August 9, 2000*, 218 F. Supp. 2d 544; 2002 U.S. Dist. LEXIS 16800 (S.D.N.Y., 2002), at para. 23.
49 *United States v. Davis,* 767 F.2d 1025 (2d Cir.1985), where enforcing criminal laws against fraud overcame the Cayman Islands' interest in bank secrecy.
50 *SEC v. Banca Della Svizzera Italiana,* 92 F.R.D. 111 (S.D.N.Y. 1981), compelling production in regulatory action to enjoin violations of US federal securities laws.
51 See, for example, *Ssangyong Corp. v. Vida Shoes Int'l, Inc., supra* note 11.
52 Submission of American Civil Liberties Union (10 August 2004) pp. 10-11.

Since US courts have sometimes found lesser US interests to trump foreign statutes prohibiting disclosure, a Canadian statutory prohibition against disclosure, standing on its own may, but will not necessarily, overcome the vital US interests FISA investigations are said to be aimed at protecting.

Conclusions

We conclude that, although the FIS Court may consider a Canadian statutory prohibition against disclosure, there are no guarantees that the prohibition alone would move the court to decline to issue an order under FISA, particularly when the grounds for the application are cast as vital US interests. Nevertheless, at a minimum, enactment of such statutory provisions in Canada provides US courts with a clear statement of public policy respecting the importance we attach to the privacy of personal information in British Columbia, particularly when it has been generated through necessary use by the public of the many services provided to them by public bodies in British Columbia.[53]

The probability of a Canadian statutory prohibition against disclosure having persuasive effect on decisions of the FIS Court, or any foreign court, could be increased, in our view, if the prohibition were made specific to orders issued by a foreign court, or other foreign authority, and carried considerable penalties for breach, including large fines and imprisonment. Of course, the secrecy of the FIS Court and the fact that only US government lawyers appear before it lessen the probability that British Columbia law and policy will be brought to the court's attention.[54]

Despite any persuasive effect this type of legislation may have on decisions made by foreign courts such as the FIS Court, the most significant value of this legislation could be its practical and legal effect within British Columbia. Regardless of a decision by a US court that records are in the control of a US-linked organization are required for US litigation or relate to a vital US interest, if the records are subject to FOIPPA then, as a matter of law in British Columbia, they cannot be disclosed in response to a US court order. Compliance with FOIPPA must, of course, be a term of all outsourcing contracts and meaningful contractual terms respecting breach of contract would have to complement the direct statutory prohibitions.

Direct statutory prohibitions against disclosure in response to any form of order or request made by a foreign court or foreign authority, accompanied by considerable penalties for breach, provide a substantial incentive for compliance with British Columbia law by a person served with a foreign order for disclosure of personal information records in British Columbia. The threat of prosecution accompanied by a substantial fine or even imprisonment could be expected to be a factor in deterring a person or public body from abiding by the terms of a foreign order and failing to comply with British Columbia law in this regard. Such provisions also provide a defence to the person served with the foreign order and obligate them to notify the public body that it has been made. This is of particular importance in the context of FISA orders (and national security letters), the existence of which would otherwise remain shielded from

53 Statutory provisions intended to counter the effect of foreign orders may be enacted at the provincial or federal level and are not unknown in Canadian law. For example, Canada has occasionally used the Foreign Extraterritorial Measures Act (FEMA), R.S.C. 1985, c. F-29, to block foreign laws, such as the US Helms-Burton Act, that purport to reach into Canadian law in violation of principles of international law and comity.

54 In this respect, there is some suggestion that, in ordinary court proceedings, a US court might be influenced by the fact that the foreign government whose laws are implicated has made the effort to appear as a friend of the court and has resisted disclosure in defence of its laws. See, for example, *Volkswagen, A.G. v. Valdez, supra* note 33, and *In re Uranium Antitrust Litigation, supra* note 15.

attention.

In Chapter 9, we concluded that US authorities engaged in foreign intelligence gathering would not be likely to use the MLAT for a number of reasons. We also concluded that a ban on outsourcing would not be a practical or effective way of ensuring the protection of personal information of British Columbians. In this chapter, we have concluded that there are no assurances that the FIS Court will not grant orders compelling US-linked companies to disclose personal information records located in Canada, particularly when vital US interests are considered to be at stake. The existence of that reasonable possibility warrants other mitigating steps being taken, such as direct statutory prohibitions on disclosure and contractual remedies.

11 CONCLUSIONS AND RECOMMENDATIONS

This chapter builds on conclusions reached in earlier chapters by making recommendations for action. We will begin with a short review of the process undertaken by the Office of the Information and Privacy Commissioner (OIPC) leading up to this report.

The possible implications of the USA Patriot Act for the security of personal information of British Columbians in light of British Columbia government outsourcing initiatives have in recent months been of considerable interest and concern to the public, business and government. The Information and Privacy Commissioner's Request for Submissions, published in late May 2004, therefore initiated a short-term and open process for assessing the privacy issues raised by the USA Patriot Act.

The Information and Privacy Commissioner's objective was to elicit the views of governments, members of the public, businesses, labour organizations and other interest groups and then prepare an advisory report that would be a point of departure for further discussion and action. The number, complexity and intensity of response of submissions received in July and August 2004 was astonishing[1] and clearly demanded an examination of the matter within the larger context of globalization, privacy and national security. In keeping with the openness of the process, some 60 submissions from governments, businesses, interest groups and academics have been posted on the OIPC website (www.oipc.bc.ca).

We studied the submissions and prepared this report over a period of ten weeks. It can only be a step on the road, not an endpoint. The British Columbia government has, since its submission to the OIPC, introduced the FOIPPA amendments[2] that it promised to address the USA Patriot Act. A number of our recommendations below further illustrate the ongoing nature of the dialogue of which this report is a part.

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.

Questions and Answers

We will now recall the specific questions posed in the Request for Submissions and briefly summarize our answers to them:

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?

1 The OIPC received over 500 written responses to the Request for Submissions.
2 Freedom of Information and Protection of Privacy Amendment Act, 2004, 5th Sess., 37th Parl., BC, 2004 (3rd reading 19 October 2004).

2. If it does, what are the implications for public body compliance with the personal privacy protections in the Freedom of Information and Protection of Privacy Act (FOIPPA)? What measures can be suggested to eliminate or appropriately mitigate privacy risks affecting compliance with FOIPPA?

Access to British Columbians' personal information through the USA Patriot Act

On the first question, we have concluded that, if information is located outside British Columbia, it will be subject to the law that applies where it is found, regardless of the terms of an outsourcing contract. Therefore, if an outsourcing arrangement calls for personal information to be sent to the US, that information would be subject to the USA Patriot Act while in the US. The applicability of US law would not be limited to Foreign Intelligence Surveillance Act (FISA) orders for the production of "tangible things". It would also include provisions respecting physical search orders under FISA, national security letters[3] under various US statutes, and other laws that apply to records or information in the US.

Further, we have concluded that it is a reasonable possibility that the US Foreign Intelligence Surveillance Court (FIS Court) would issue a FISA order requiring a US-located corporation to produce records held in Canada by its Canadian subsidiary or, indeed, require any person or corporation within the jurisdiction of that court to disclose records held outside the US that they control because they have the legal or practical ability to obtain the records. It has also been said by some US courts that a US-located corporation will control a foreign corporation if the US corporation can, directly or indirectly, elect a majority of the directors of the foreign corporation. Accordingly, it would not be prudent, in our view, to ignore the fact that control, as a matter of US law, has been found on the basis of corporate relationship alone and there is a reasonable possibility that the FIS Court would take this view regardless of contractual relationships or practical arrangements between a public body, its contractor and corporations related to the contractor.

Some in the information technology industry, notably the Information Technology Association of Canada, have argued that a FISA order is not a concern because Canada and the US have similar anti-terrorism laws. As discussed in Chapters 6 and 7, we agree that the two countries have anti-terrorism laws that share many features. This would not make the application of FISA orders to personal information in British Columbia acceptable or any less invasive.

Others in the information technology industry say a FISA order is not a concern because there is a 'vanishingly small' risk of one ever being made in relation to bulk collections of information or information located in British Columbia. However, US courts and grand juries have over many years made orders in relation to records located in Canada or other countries. This has been a source of friction between the US and Canada and the US and other countries. There is no indication that an extra-territorial FISA order will not be sought by the FBI and issued by a FIS Court or that this has not already happened in relation to personal information in Canada.

We are inclined to the view, for the reasons described in Chapter 10, that there is a reasonable possibility of the FIS Court issuing a FISA order affecting personal information of British Columbians

3 This presupposes that provisions for the issuance of national security letters will continue to exist in US statutes. As discussed in Chapter 6, the decision of Marrero J. in *Doe and ACLU v. Ashcroft*, No. 04-CIV-2614; 2004 U.S. Dist. Lexis 19343 (S.D.N.Y. 2004) has struck down one provision authorizing the issuance of National Security Letters (18 U.S.C. § 2709, relating to electronic communication subscriber, billing and transaction records typically held by Internet service providers) on the ground that it contravenes the First Amendment of the US Constitution. The US government is appealing this decision.

located in British Columbia—a possibility that has increased as a result of the USA Patriot Act amendments to FISA. Section 215 of the USA Patriot Act removed the limits to the types of organizations that can be investigated under FISA orders. Further, ongoing concerns about terrorism increase the likelihood that, when the FIS Court applies a 'balancing test' in reviewing applications for FISA orders, it may give greater weight to US national security concerns than to Canadian concerns about privacy protection.

The FBI, through the US Department of Justice, and the US Department of Homeland Security[4] responded to the Request for Submissions. However, their submissions did not directly address, much less counter, the proposition that the USA Patriot Act might, through US persons or service providers, be used to reach personal information of British Columbians that is located in British Columbia.[5] In the absence of evidence to the contrary—which could take various forms, including unequivocal written assurances from or a formal agreement with the US government—we cannot ignore the history of US courts issuing extra-territorial orders in some circumstances and the evident present day risk with respect to FISA orders (or national security letters that can be issued directly by the FBI under various US statutes).

Implications for compliance with FOIPPA and mitigation of privacy risks

As for the second question posed in the Request for Submissions, we concluded in Chapter 9 that disclosure by a public body or a contractor for the purpose of complying with a FISA order (or a national security letter) is unauthorized disclosure under sections 30 and 33 of FOIPPA. FOIPPA, as we discussed, requires public bodies, directly and through their contractors, to implement reasonable, but not absolute, security arrangements to protect personal information against risks, including risk of unauthorized disclosure in response to an order made under foreign law.

Some submissions to us suggested that unauthorized disclosure in response to an extra-territorial FISA order (or a national security letter) is of little concern because extensive information transfer mechanisms that are recognized by FOIPPA would make an extra-territorial foreign order unnecessary. In our view, US authorities engaged in foreign intelligence gathering would not be likely to 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 to them, or would necessarily use, other information transfer methods—such as information sharing agreements—that are recognized in MLAT and in section 33 of FOIPPA. This raises parallel issues about government transfers of personal information about Canadians to other countries that are important and warrant rigorous study and national dialogue in their own right.

We concluded in Chapter 9 that a ban on British Columbia government outsourcing of the management of sensitive personal information would not be a practical or effective plan of action, but that other measures should be implemented at legislative, contractual and practical levels to mitigate, though probably not eliminate, the risk of unauthorized disclosure in response to a FISA order or national security letter.

4 Submissions of the US Department of Justice, Federal Bureau of Investigation (18 August 2004) and the US Department of Homeland Security (6 August 2004).

5 The Submission of the FBI, *ibid*., alludes to the US Privacy Act prohibiting the FBI from collecting and retaining personal information except for valid law enforcement purposes "which, as a general rule, are established by guidelines issued by the Attorney General". There is no indication that this connotes any restriction on the collection or retention of information located outside US borders and, in the preceding paragraph, the submission refers to the FBI seeking information about a Canadian citizen from a US service provider, without qualification as to the location of that information.

Recommendations

We will now make recommendations with respect to the risks we have identified and just summarized. Some of the recommendations respond directly to the questions in the Request for Submissions. We readily acknowledge that other recommendations are not directly in response to those questions. They flow from suggested answers or justifications in the submissions received in response to the Request for Submissions that, in our view, raise other serious issues about government transfers of personal information in the context of globalization.

In the case of audits of information sharing agreements, our recommendations flow from submissions that the wide extent of authorized information transfer mechanisms in FOIPPA—an important aspect of which is authority to disclose pursuant to sharing agreements—would make an extraterritorial US order unnecessary.

In the case of audits of the data mining activities of governments and government agencies in Canada, our recommendations flow from concerns that data mining is a use to which databases of personal information of Canadians could be expected to be put if they are transferred, unconditionally, into the hands of US government authorities or business organizations. Although data mining technologies are as available to Canadian governments as to their US counterparts, it became clear to us that, unlike the US, where the federal Government Accountability Office has published audit reports in this area, we really have little or no reporting or studies on the incidence of data mining by governments in Canada.

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 other information sharing mechanisms. National dialogue and action are required. Some of our recommendations in that regard are inspired by the government of British Columbia submission or by recommendations proposed by the Privacy Commissioner of Canada in her submission to us and in her office's earlier communications with the government of Canada.

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

Amendments to FOIPPA

On October 7, 2004, the serious government introduced Bill 73, the Freedom of Information and Protection of Privacy Amendment Act, 2004, in the Legislative Assembly of British Columbia.[6] Bill 73 is in general a welcome development, insofar as we understand it is aimed at implementing the government's commitment to introduce legislative amendments to address the USA Patriot Act. We endorse the enactment of direct prohibitions and penal sanctions in FOIPPA against disclosure in response to an order by a foreign court or other foreign authority. A comment letter respecting Bill 73, including whether it adequately meets that objective, will be forthcoming from the Information and Privacy Commissioner.

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

6 Freedom of Information and Protection of Privacy Amendment Act, 2004, *supra* note 2.

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

The next recommendation addresses the fact that US courts, when considering whether to require disclosure of records located outside the US, have been influenced by case-specific opposition from the foreign jurisdiction to disclosure in defiance of a law of the foreign jurisdiction. A published litigation policy for opposition by the British Columbia government to a FISA order or national security letter in respect of personal information in British Columbia may, the US jurisprudence indicates, carry some weight with a US court as an expression of BC public policy respecting privacy of personal information in this province.[7]

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.

Acknowledging that FISA orders and national security letters are issued in secret, express statutory prohibitions against disclosure in FOIPPA, coupled with a requirement to notify the British Columbia government and meaningful penalties for breach, will create new legal and practical incentives for persons in British Columbia to refuse to comply with the foreign order and instead report it to the British Columbia government.

Further protection of personal information from FISA orders

Submissions to us from the US FBI and the US Department of Homeland Security have provided no assurance that FISA orders will not be sought from the FIS Court, or that national security letters will not be issued by the FBI, for access to personal information records in British Columbia. This assurance should be sought to complement the amendments to FOIPPA in Recommendation 1.

7 Doe and ACLU v. Ashcroft, ibid., note 3, a lawsuit brought by the American Civil Liberties Union respecting national security letters, demonstrates that the secret nature of FISA proceedings and national security letter processes does not preclude intervention as contemplated by this recommendation.

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

As discussed in Chapter 9, a public body cannot, by contracting out, relieve itself of its privacy obligations under FOIPPA. This was the case before the USA Patriot Act with respect to all situations, whether or not foreign linked contractors were involved, and it continues to be the case. When a public body contracts out functions, it must ensure there are reasonable security arrangements for the personal information disclosed to the contractor and that the contractor collects or generates in fulfilling the outsourced function. The required standard of security under section 30 is a constant, with or without outsourcing.

OIPC Guideline 01-02 was issued in 2001, and updated in 2003, to assist public bodies in meeting FOIPPA privacy obligations with respect to data services contracts. The OIPC will be updating this guideline again to reflect the new FOIPPA provisions in Bill 73.

The OIPC will also be reviewing the British Columbia government's Privacy Protection Measures announced on October 5, 2004, which is a compilation of technology and business processes, employee strategies, contractual measures and corporate structure considerations for public bodies that are contemplating outsourcing to US linked contractors.

As noted earlier, the Information and Privacy Commissioner wrote in early 2002 to British Columbia government ministers to mark the need for public bodies that outsource functions to ensure they have the expert staff and other resources necessary to actively and diligently monitor contract performance and to punish any discovered breaches. This is particularly important in relation to USA Patriot Act risks. Bearing that in mind, and also that many existing outsource contracts could be subject to USA Patriot Act risk but will not be subject to the new FOIPPA provisions in Bill 73 by virtue of its transitional provisions, we are prompted to make the following recommendations at this time:

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

In Chapter 9, we analyzed the status under FOIPPA of the disclosure of personal information in the custody or under the control of a public body, in response to an order of a foreign court or other foreign authority. Disclosure on that basis would be unauthorized under FOIPPA. We also analyzed, in Chapter 10, the role of direct statutory prohibitions against disclosure in the balancing test that might be expected to be applied by a FIS Court were it asked to issue an extraterritorial FISA order, and the importance, practically and legally, of making unauthorized disclosure under FOIPPA an offence punishable by significant deterrent penalties. The British Columbia government has now proceeded with the introduction of legislation extending FOIPPA to address the USA Patriot Act, in the form of Bill 73.

The next recommendation affirms that it is in the interest of protecting the privacy of British Columbians—whose personal information the government of Canada and its agencies collect directly or indirectly through sharing by public bodies in this province—for these issues also to be considered, and acted on where necessary, at the federal level.

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

We received submissions that US authorities would not resort to extra-territorial FISA orders or national security letters because information sharing under treaties, agreements and arrangements is extensively authorized under FOIPPA and the federal Privacy Act. This raises important parallel issues about government transfers of personal information (issues that have also surfaced, in the context of national security, in the ongoing federal Arar Inquiry referred to in Chapter 9). The extent of information sharing by public bodies under FOIPPA has not been sufficiently or transparently studied and documented and, in our view, this needs to be remedied at the earliest practicable opportunity.

Advanced technologies have enabled the merging of 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 predict future results or behaviour. When personal information is involved, the hidden patterns and subtle relationships that data mining detects are recorded and become new personal information of the individual whose characteristics or habits are being searched and analyzed. A recent audit by the US federal Government Accountability Office (referred to in Chapters 4 and 9) has studied the extent of data mining by US federal agencies. It has

confirmed that this practice is increasingly common and that many 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 this too needs to be remedied at the earliest practicable opportunity.

The adequacy and appropriateness of information sharing and data mining practices at the federal level are important to British Columbians, whose personal information, as already noted, the government of Canada or its agencies collect directly or indirectly through sharing by public bodies in this province. Personal information practices in national security matters, a field in the exclusive jurisdiction of the federal government, are of particular significance in the context of this report on the implications for the privacy of British Columbians of foreign intelligence gathering under the USA Patriot Act.

We commend the Privacy Commissioner of Canada's efforts to date regarding information sharing audits (referred in Chapter 9) and support her recommendation for further work in this area. Audits and ongoing reporting and transparency in respect of information sharing agreements and arrangements and data mining activities are as necessary at the federal level as at the provincial level.

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

In Chapter 9, we described how a disturbing number of British Columbia government ministries do not appear to be living up to the reporting requirements about information sharing agreements

found in section 69 of FOIPPA. This also needs to be corrected promptly.

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

This report has focussed on the implications of the USA Patriot Act for the security of personal information of British Columbians in light of public body outsourcing. However, many submissions to us—including those of the British Columbia government, the Privacy Commissioner of Canada, Professor Michael Geist and Milana Homsi, and the American Civil Liberties Union—observed, and we agree, that transnational personal information transfer issues in respect of government operations are at least as significant in respect of private sector activities.

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 information gathering and use for state purposes

The heightened fear of terrorism provided a catalyst for increased surveillance in North America and elsewhere. The resulting trend appears to be broadened state powers for collection of information for national security purposes (including border and public transportation security), which is then in some cases disclosed for enforcement of unconnected criminal and regulatory laws. The traditional distinction between intelligence gathering for the general purpose of ensuring national security, and policing for the specific purpose of enforcing ordinary laws, is increasingly blurred.

More generous allowances are made for the collection and use of information for security purposes. A more relaxed understanding of the distinction between security and law enforcement purposes then creates risk that traditional law enforcement restraints we rely upon to protect our civil liberties will be eroded. Advancing technology for surveillance and data manipulation compounds that risk. We do not question the importance of national security, but we are concerned that in the implementation of state security initiatives, insufficient attention may be afforded to maintaining necessary distinctions for protecting civil liberties of fundamental importance.

As we noted in Chapter 7, the Attorney General of Canada has said there is no contradiction between the protection of security and the protection of human rights, which we take to include privacy rights. We agree. The task for governments is to ensure that state initiatives reflect as much concern for protection of privacy as for the efficiency of security and law enforcement measures.

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

As discussed in Chapter 4, there is an increasingly complex set of rules and agreements regarding international trade of goods and services. Canada has a stake in ensuring that those rules not only promote international trade but also protect the right of all countries to make independent policy choices. Canada needs to be careful when negotiating international trade obligations that relate to or may affect the delivery of public services to ensure that privacy protections are maintained in accordance with Canadian values.

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

North America appears to be moving towards a continent wide customs free zone with common approaches to trade, energy, immigration and security. The privacy implications of transnational data flows must be taken into account in this process. Privacy values must be given full weight in the multilateral legal, regulatory and administrative solutions that emerge. Rigorous, well-considered privacy protections must be established and must be accompanied by effective continental oversight and accountability mechanisms.

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.

BIBLIOGRAPHY

Canadian Statutory Material and Treaties

Access to Information and Protection of Privacy Act, (Nunavut), R.S.N.W.T. 1994, c. 20.

Access to Information and Protection of Privacy Act, R.S.Y. 2002, c. 1.

Access to Information and Protection of Privacy Act, S.N.L. 2002, c. A-11.

Access to Information and Protection of Privacy Act, S.N.W.T. 1994, c. 20.

Aeronautics Act, R.S.C. 1985, c. A-2.

Anti-terrorism Act, S.C. 2001, c. 41.

Bill 73, Freedom of Information and Protection of Privacy Amendment Act, 2004, 5th Sess., 37th Parl., BC, 2004 (3rd reading 19 October 2004).

Canada Evidence Act, R.S.C. 1985, c. C-5.

Canadian Security Intelligence Service Act, R.S.C. 1985, c. C-23.

Constitution Act, 1982, being Schedule B to the Canada Act 1982 (U.K.), 1982, c. 11.

Criminal Code, R.S.C. 1985, c. 41.

Customs Act, R.S.C. 1985 (2d Supp.) c.1.

Document Disposal Act, R.S.B.C. 1996, c. 99.

Evidence Act, R.S.B.C. 1996, c. 124.

Foreign Extraterritorial Measures Act, R.S.C. 1985, c. F-29.

Freedom of Information and Protection of Privacy Act, C.C.S.M. c. F175.

Freedom of Information and Protection of Privacy Act, R.S.A. 2000, c. F-25.

Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165.

Freedom of Information and Protection of Privacy Act, R.S.P.E.I. 2002, c. F-15.01.

Freedom of Information and Protection of Privacy Act, S.N.S. 1993, c. 5.

Freedom of Information and Protection of Privacy Act, S.S. 1990-91, c. F-22.01.

Inquiries Act, R.S.C. 1985, c. I-11.

Mutual Legal Assistance in Criminal Matters Act, R.S.C. 1985 (4th Supp.), c. 30.

National Defence Act, R.S.C. 1985, c. N-5.

Personal Information Protection Act, S.B.C. 2003, c. 63.

Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.

Privacy Act, R.S.C. 1985, c. P-21.

Proceeds of Crime (Money Laundering) and Terrorist Financing Act, S.C. 2000, c. 17
Public Safety Act, 2002, S.C. 2004, c. 15.
Rules of Court, B.C. Reg. 221/90, as amended.
Security of Information Act, R.S.C. 1985, c. O-5.
Treaty between the Government of Canada and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters (18 March 1985) 1990, Can. T.S. No. 19 (in force 24 January 1990; C.Gaz. 1990.1.953).

Canadian Case Law

Application Under s. 83.28 of the Criminal Code (Re), 2004, S.C.J. No. 40, SCC 42.
Atwal v. Canada, [1988] 1 F.C. 107 (C.A.).
Bell ExpressVu Limited Partnership v. Rex, [2002] 2 S.C.R. 559.
Blencoe v. British Columbia (Human Rights Commission), [2000] 2 S.C.R. 307.
Canada (Information Commissioner) v. Canada (Immigration and Refugee Board), [1997] 4 Admin L.R. (3d) 96 (F.C.T.D.).
Canada (Information Commissioner) v. Canada (Minister of Citizenship and Immigration), [2003] 1 F.C. 219 (C.A.).
Canadian AIDS Society v. Ontario, [1995] O.J. No. 2361 (Gen. Div.); aff'd [1996] O.J. No. 4184 (C.A.); leave to appeal refused [1997] S.C.C.A. No. 33.
Germany (Federal Republic) v. Canadian Imperial Bank of Commerce, [1997] 31 O.R. (3d) 684 (Gen. Div.).
Germany (Federal Republic) v. Ebke, [2001] 159 C.C.C. (3d) 253 (N.W.T.S.C.); aff'd [2003] N.W.T.J. No. 49 (N.W.T.C.A.); leave to appeal refused [2003] S.C.C.A. No. 178.
Gulf Oil Corp. v. Gulf Canada Ltd., [1980] 2 S.C.R. 39.
Hunter v. Southam Inc., [1984] 2 S.C.R. 145.
Morguard Investments Ltd. v. De Savoye, [1990] 3 S.C.R. 1077.
Ontario (Criminal Code Review Board) v. Ontario (Information and Privacy Commissioner) (1999), 180 D.L.R. (4th) 657 (Ont. C.A.).
Purdy v. Canada (Attorney General) (2003), 230 D.L.R. (4th) 361 (B.C.C.A.).
R. v. Colarusso, [1994] 1 S.C.R. 20.
R. v. Collins, [1987] 1 S.C.R. 265.
R. v. Cook, [1998] 2 S.C.R. 597.
R. v. Dersch, [1993] 3 S.C.R. 769.
R. v. Dyment, [1988] 2 S.C.R 417.
R. v. Evans, [1996] 1 S.C.R. 8.
R. v. Harrer, [1995] 3 S.C.R. 562.
R. v. Jarvis, [2002] 3 S.C.R. 757.
R. v. Ling, [2002] 3 S.C.R. 814.
R. v. Mills, [1999] 3 S.C.R. 668.

R. v. O'Connor, [1995] 4 S.C.R. 411.
R. v. Plant, [1993] 3 S.C.R. 281.
R. v. Terry, [1996] 2 S.C.R. 207.
R. v. Tessling (2003), 171 C.C.C. (3d) 361 (Ont. C.A.).
R. v. Wise, [1992] 1 S.C.R. 527.
R. v. Zingre, [1981] 2 S.C.R. 392.
Re Republic of France and De Havilland Aircraft of Canada Ltd. (1991), 65 C.C.C. (3d) 449 (Ont. C.A.).
Re Vancouver Sun, [2004] S.C.J. No. 41, 2004 SCC 43.
Re Westinghouse Electric Corp. and Duquesne Light Co. (1977), 78 D.L.R. (3d) 3 (Ont. H.C.J.).
Rodriguez v. British Columbia (Attorney General), [1993] 3 S.C.R. 519.
Ruby v. Canada (Solicitor General), [2000] 3 F.C. 589 (C.A.); varied [2002] 4 S.C.R. 519.
S*chreiber v. Canada (Attorney General)*, [1998] 1 S.C.R. 841.
Slaight Communications Inc. v. Davidson, [1989] 1 S.C.R. 1039.
Smith v. Canada (Attorney General), [2001] 3 S.C.R. 902.
Tolofson v. Jensen, [1994] 3 S.C.R. 1022.
U.S.A. v. Orphanou, [2004] O.J. No. 622 (S.C.).
U.S.A. v. Ross, [1994] B.C.J. No. 971 (C.A.).
U.S.A. v. Ross, [1995] Q.J. No. 506 (C.A.), leave to appeal refused [1995] C.S.C.R. No. 410.
U.S.A. v. Schneider, [2002] B.C.J. No. 1561 (S.C.).

Orders of the Information and Privacy Commissioner for British Columbia

Order 00-47, [2000] B.C.I.P.C.D. No. 51.
Order 04-19, [2004] B.C.I.P.C.D. No. 19.

Canadian Governmental Documents and Reports

Final Report of the Commission on the Future of Health Care in Canada, *Building on Values: The Future of Health Care in Canada*, Roy J. Romanow, Commissioner, (November 2002).

Government of Canada, *Securing an Open Society: Canada's National Security Policy,* (Privy Council Office, April 2004).

Office of the Information and Privacy Commissioner for British Columbia, Guideline 01-01, *Guidelines for Audits of Automated Personal Information Systems.*

Office of the Information and Privacy Commissioner for British Columbia, Investigation Report 01-01, "Investigation into BC Nurses Union Complaint about Telus-VGH LastWord Contract", (5 October 2001).

Smith, D. and B. Barnard. "Consultations on British Columbia's Information Structure" prepared for the BC Ministry of Employment and Investment (9 November 1994).

US Statutory Material

Department of Homeland Security Appropriations Act, 2005, HR 4567, 108th Congr.
Foreign Intelligence Surveillance Act, 1978, 50 U.S.C. 1801 *et seq.*
Intelligence Authorization Act for Fiscal Year 2004, HR 2417, 108th Cong.
Personal Data Offshoring Protection Act, 2004, HR 4366, 108th Cong.
The Homeland Security Act, 2002, Pub. L. No. 107-296, 116 Stat. 2135.
USA Patriot Act, 2001, Pub. L. No. 107-56, 115 Stat. 272.
US, Rules of the Foreign Intelligence Surveillance Court.

US Case Law

Afros S/P.A. v. Krauss-Maffei Corp., 113 F.R.D. 127, 131 (D. Del. 1986).
Alcan International Ltd. v. S.A. Day Mfg. Co., Inc., 176 F.R.D. 75 (W.D.N.Y. 1996).
Asset Value Fund Ltd. v. The Care Group, Inc., U.S. Dist. LEXIS 19768 (S.D.N.Y. 1997).
Bank of New York v. Meridien Biao Bank Tanzania, 171 F.R.D. 135 (S.D.N.Y. 1977).
Compagnie Française d'Assurance Pour le Commerce Extérieur v. Phillips Petroleum Co., 105 F.R.D. 16 (S.D.N.Y. 1984).
Cooper Indus., Inc. v. British Aerospace, Inc., 102 F.R.D. 918 (S.D.N.Y. 1984).
Dietrich v. *Bauer*, U.S. Dist. Lexis 11729 (S.D.N.Y. 2000).
Doe and ACLU v. Ashcroft, No. 04-CIV-2614, 2004 U.S. Dist. LEXIS 19343 (S.D.N.Y. 2004).
First Am. Corp. v. *Price Waterhouse LLP*, 154 F.3d 16 (2d Cir. 1998).
Griswold v. Connecticut, 381 U.S. 479 (1965).
In re A Grand Jury Subpoena dated August 9, 2000, 218 F. Supp. 2d 544 (S.D.N.Y. 2002).
In re Grand Jury Proceedings (Bank of Nova Scotia), 740 F.2d 817 (11th Cir. 1984).
In re Grand Jury Subpoenas duces tecum addressed to Canadian International Paper Company et al., 72 F.Supp. 1013 (S.D.N.Y. 1947).
In re Investigations of World Arrangements with Relation to the Production, Transportation, Refining and Distribution of Petroleum, 13 F.R.D. 280 (D.D.C. 1952).
In re Marc Rich & Co., A.G., 707 F.2d 663 (2nd Cir. 1983).
In re Sealed Case, 310 F.3d 717 (Foreign Intell. Surv. Ct. Rev. 2002).
In re Sealed Case, 825 F.2d 494; (D.C.C. 1987).
In re Uranium Antitrust Litigation, 480 F.Supp. 1138 (N.D. Ill. 1979).
Ings v. *Ferguson*, 282 F.2d 149 (2d Cir. 1960).
Katz v.United States, 389 U.S. 347 (1967).
Kyllo v. United States, 533 U.S. 27 (2001).
Lawrence v. Texas, 539 U.S. 558 (2003).
Lopez v. United States, 373 U.S. 427 (1963).
Minipeco, S.A. v. ContiCommodity Services, Inc., 116 F.R.D. 517 (S.D.N.Y. 1987).
Olmstead v. United States, 277 U.S. 438 (1928).

Planned Parenthood of Southeastern Pa. v. Casey, 505 U. S. 833 (1992).
SEC v. *Banca Della Svizzera Italiana*, 92 F.R.D. 111 (S.D.N.Y. 1981).
Société Internationale Pour Participations Industrielles Et Commerciales, S.A. v. Rogers, 357 U.S. 197 (1958).
Ssangyong Corp. v. Vida Shoes IntÓl, Inc., 2004 U.S. Dist. LEXIS 9101 (S.D.N.Y. 2004).
United States v. Chase Manhattan Bank, N.A. and F.D.C. Co. Ltd., 584 F. Supp. 1080 (S.D.N.Y. 1984).
United States v. *Davis*, 767 F.2d 1025 (2d Cir. 1985).
United States v. *First NatÓl City Bank*, 396 F.2d 897 (2d Cir. 1968).
United States v. United States District Court, 407 U.S. 297 (1972).
Volkswagen, A.G. v. *Valdez*, 909 S.W.2d 900 (Tex. Sup. Ct. 1995).

Other Governmental Documents and Reports

Report of the Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens*, US Secretary of Health, Education and Welfare (June, 1973).

Bazan, Elizabeth B. "The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions" (Congressional Research Service Report for Congress, 2003).

Council of Europe Convention for the Protection for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108 (Strasbourg: Jan 1981).

Doyle, Charles. "The USA Patriot Act: A Legal Analysis" (Congressional Research Service Report for Congress, 2002).

EC, European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] O.J.L. 281/31.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).

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

UK Report of a Committee of Privy Counsellors, *Review of Intelligence on Weapons of Mass Destruction (Return to an Address of the Honourable the House of Commons)*, Chairman, the Rt Hon the Lord Butler of Brockwell (London: The Stationery Office, 14 July 2004).

UN Conference on Trade and Development, *World Investment Report 2004: The Shift Towards Services* (United Nations: New York and Geneva, 2004).

UN Universal Declaration of Human Rights, G.A. Res 217A(III), UNGAOR, 3d Sess. Supp. No. 13, UN Doc. A/810 (1948).

US Department of Justice, Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (31 October 2003).

US Department of Justice. "Report from the Field: The USA Patriot Act at Work" (July 2004).

US Executive Order 12333—United States Intelligence Activities 46 FR 59941, 3 CFR, 1981 Comp., p. 200.

US General Accounting Office. *Data Mining: Federal Efforts Cover a Wide Range of Uses,* Report to the Ranking Minority Member, Subcommittee on Financial Management, the Budget, and International Committee on Governmental Affairs, U.S. Senate. (May 2004).

US Privacy Protection Study Commission. Personal Privacy in an Information Society (July 1977).
US Senate Judiciary Committee, Senators Patrick Leahy, Charles Grassley and Arlen Specter. *FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures* (Interim Report, February 2003).

Books

6, Perri. *The Future of Privacy*, vol. 1 (London: Demos, 1998).
American Law Institute. *Restatement (Third) of the Foreign Relations Law of the United States* (St. Paul, MN: American Law Institute Publishers, 1987).
Ash, Timothy Garton. *The File* (New York: Random House, 1997).
Bennett, Colin J. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1992).
Bennett, Colin J. and Rebecca Grant, eds., *Vision of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999).
Bennett, Colin J. and Charles D. Raab. *The Governance of Privacy* (Aldershot: Ashgate, 2003).
Brin, David. *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* (Reading, MA: Addison-Wesley, 1998).
Cavoukian, Ann and Don Tapscott. *Who Knows: Safeguarding Your Privacy in a Networked World* (Toronto: Vintage Canada, 1995).
Diffie, Whitfield and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption* (Cambridge, MA: The MIT Press, 1998).
Etzioni, Amitai. *The Limits of Privacy* (New York: Basic Books, 1999).
Flaherty, David H. *Privacy in Colonial New England* (Charlottesville: University Press of Virginia, 1967).
Flaherty, David H. *Protecting Privacy in Surveillance Societies* (Chapel Hill: University of North Carolina Press, 1989).
Hogg, Peter W. *Constitutional Law of Canada* (Toronto: Thomson-Carswell, 2004).
Kindred, H.M. *et al*., *International Law Chiefly as Interpreted and Applied in Canada*, 5th ed. (Toronto: Emond Montgomery, 1993).
Krivel, E.F., Beveridge, T. and J.W. Hayward. *A Practical Guide to Canadian Extradition* (Toronto: Carswell, 2002).
Roach, Kent. *September 11: Consequences for Canada* (Québec: McGill-QueenÓs University Press, 2003).
Rosen, Jeffrey. *The Unwanted Gaze: The Destruction of Privacy in America* (New York: Vintage Books, 2001).
Sieghart, Paul. *Privacy and Computers* (London: Latimer, 1976).
Solzhenitsyn, Alexander. *Cancer Ward (*New York: Farrar, Straus & Giroux, 1969).
Sullivan, R. *Driedger on Construction of Statutes*, 3d ed. (Vancouver: Butterworths, 1994).
Sykes, Charles J. *The End of Privacy* (New York: St. MartinÓs Press, 1999).
Westin, Alan. *Privacy and Freedom* (New York: Antheneum, 1967).
Whitaker, Reg. *The End of Privacy: How Total Surveillance Is Becoming A Reality* (New York: New Press, 1999).

Journal Articles and Commentaries

Brown, Christopher. "Experts Debate Uses, Privacy Concerns Raised by Vast Databases of Personal Info" (2004) 3:13 Privacy and Security Law.

Cockfield, Arthur J. "The State of Privacy Laws and Privacy-encroaching Technologies after September 11: A Two-year Report Card on the Canadian Government", University of Ottawa Law and Technology Journal 1 (2003-2004).

Cotler, the Hon. Irwin, Minister of Justice and Attorney-General of Canada. (Address to the Canadian Bar Association Annual Conference, Winnipeg, 16 August 2004).

Currie, Robert J. "Peace and Public Order: "International Mutual Legal Assistance 'The Canadian Way' " [1998] 7 Dal. J. Leg. Stud. 91.

Feinberg, Joe. "Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution?" [1982] 58 Notre Dame L. Rev.

Freedman, Bradley J. & Gregory N. Harney. "Obtaining Evidence from Canada: The Enforcement of Letters Rogatory by Canadian Courts" [1987] Vol. 21:2 UBCL Rev. 351.

Goldstein, Robert & Nancy, Dennison. "Mutual Legal Assistance in Canadian Criminal Courts" [2002] 45 Crim. L.Q. 126.

La Forest, the Hon. Gérard V., C.C., Q.C., retired Supreme Court of Canada Justice, Legal Opinion for the Privacy Commissioner of Canada (12 November 2002).

Loukidelis, David, Information and Privacy Commissioner for British Columbia "Alternative Service Delivery—Privacy Issues" (Letter to all Ministers, 21 January 2002).

Loukidelis, David, Information and Privacy Commissioner for British Columbia. "Identity, Privacy & Security—Can Technology Really Reconcile Them?" (Speech, Victoria, British Columbia, February 2004).

Rankin, M.T. "The Supreme Court of Canada and the International Uranium Cartel: Gulf Oil and Canadian Sovereignty" [1980] 2 Sup. Ct. L. Rev. 410.

Regan, Priscilla. "American Business and the European Data Protection Directive: Lobbying Strategies and Tactics" in Colin Bennett and Rebecca Grant, eds., *Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999).

Schulhofer, Stephen J. "No Checks, No Balances: Discarding Bedrock Constitutional Principles" in Richard C. Leone and Greg Anrig, Jr., eds., *The War on Our Freedoms: Civil Liberties in an Age of Terrorism* (New York: PublicAffairs, 2003).

Stanley, Jay. "The Surveillance-Industrial Complex: How the American Government is Conscripting Businesses and Individuals in the Construction of a Surveillance Society" (New York: American Civil Liberties Union, 2004).

Tassé, Roger, O.C., Q.C., Legal Opinion for the Privacy Commissioner of Canada (21 November 2002).

Magazine and News Articles

Baron, Madeleine. "Welcome to the Matrix: Inside the Government's Secret, Corporate-run Mega-database" *The*

New Standard (9 July 2004).
Berrington, Craig. "Privacy, Insurance and the Transparent Society" *Privacy in Focus* (February 2001).
Boo, Katherine. "The Best Job in Town: The Americanization of Chennai" *The New Yorker* (5 July 2004).
Bridge, Maurice. "Police Want More Access to Your E-mail" *Vancouver Sun* (24 August 2004) A03.
Bridge, Maurice. "World Is Less Safe Now, Says RCMP's Top Boss" *The Vancouver Sun* (26 August 2004) A05.
Canadian Press, "Census Deal with U.S. Firm Goes Through" *The Globe and Mail* (9 October 2004).
Chester, Simon. "Outsourcing Threat to Privacy Overblown" **Financial Post** (16 August 2004).
Clark, Drew. "Senate Votes for Privacy Study on Agencies' Data-mining Use" *National Journal's Technology Daily* (16 September 2004).
Clarke, Roger. "The Digital Persona and Its Application to Data Surveillance" *The Information Society* 10:2 (June 1994).
Cole, David. "Scalia's Kind of Privacy" *The Nation* (12 July 2001).
Janzen, Leah. "Florida Firm Hawking Stolen St. B. Net Drug List" *Winnipeg Free Press* (5 August 2004).
Kehaulani Goo, Sara. "No Fly List's 'T. Kennedy' irks senator" *The Washington Post* (20 August 2004).
McGregor, Glen. "Biometric Passports Approved" *Victoria Times-Colonist* (6 October 2004) A-1.
McKenna, Barrie. "Offshoring of Jobs Big Benefit for Canada" *The Globe and Mail* (23 September 2004).
Morgan, Dan and Babington, Charles. "Push by GOP Ends Attempt to Scale Back Patriot Act" *The Seattle Times* (9 July 2004).
Recalde, Maria. "Seeking Safe Harbor from European Union Privacy Laws" *New England In-House, Lawyers Weekly USA* (July 2003).
Sallot, Jeff. "Mounties Bungled Arar File" *The Globe and Mail* (25 September 2004) A-1, A-4.
Schecter, Barbara. "Visa Accounts Open to U.S. Law Enforcement Agencies, CIBC Warns" *The National Post* (24 September 2004).
Taber, Jane. "Ottawa Compiles 'No-fly' List of Banned Passengers" *The Globe and Mail* (3 September 2004) A-1.
Ticol, David. "U.S. Patriot Act's Reach Is a Concern for Canadians" *The Globe and Mail* (14 October 2004) B13.
"U.S. Patriot Act Used in Pot Case" *CBC News, British Columbia News Online* (5 August 2004).

Other

Canadian Bar Association Resolution 04-05-A, "Privacy Rights in Canada" (August 2004).
Canadian Bar Association Resolution 04-06-A, "Limiting State Access to Private Information" (August 2004).
Canadian Imperial Bank of Commerce Notice, "Changes to the CIBC VISA Cardholder Agreement" (September 2004).
Public Policy Forum and ITAC Roundtable, "IT Offshore Outsourcing Practices in Canada," (Ottawa, 20 May 2004).

APPENDIX

List of Submissions from Organizations

The following submissions will remain posted on the Information and Privacy Commission website at www.oipc.bc.ca until October 2005. In addition to these, we received about 450 submissions from individuals.

American Civil Liberties Union, (10 Aug 2004), 14 pages.

BC Association of Pregnancy Outreach Programs, "Submission on the USA Patriot Act", (7 Aug 2004), 2 pages.

BC Citizens for Public Power, "Submission on the USA Patriot Act", (Aug 2004), 9 pages.

BC Federation of Labour, "Examination of the *USA Patriot Act* Implications for Personal Information of BC Residents", (20 July 2004), 30 pages.

BC Federation of Retired Union Members, "Submission on the USA Patriot Act", (9 July 2004), 1 page.

BC Ferry and Marine Workers' Union, "Right to Privacy", (5 Aug 2004), 3 pages.

BC Freedom of Information and Privacy Association & BC Coalition of People with Disabilities, "Is Government Outsourcing a Threat to Privacy?", (6 Aug 2004), 19 pages.

BC Government and Service Employees' Union – Part 1, "Submission on the USA Patriot Act", (6 Aug 2004), 42 pages.

BC Government and Service Employees' Union – Part 2, "Submission on the USA Patriot Act", (6 Aug 2004), 50 pages.

BC Health Coalition, "Outsourcing MSP and Pharmacare and the Impact on British Columbians' Privacy Rights", (6 Aug 2004), 5 pages.

BC Hydro, "Examination of USA Patriot Act Implications for Personal Information of British Columbia Residents Involved in Outsourcing of Government Services to US-linked Service Providers", (6 Aug 2004), 2 pages.

BC Library Association, "Submission on the USA Patriot Act and its Impact on the Privacy of BC Citizens' Personal Information in the Context of Government Outsourcing of Data Administration", (6 Aug 2004), 24 pages.

BC Medical Association, (12 July 2004), 3 pages.

BC Nurses' Union, "Submission to the Information and Privacy Commissioner for British Columbia regarding the *USA Patriot Act*", (6 Aug 2004), 10 pages.

BC Persons with AIDS Society, "Submission on the USA Patriot Act", (14 July 2004), 18 pages.

Bearing Point Inc., "Assessing USA Patriot Act Implications", (6 Aug 2004), 3 pages.

British Columbia Civil Liberties Association, "Implications of the USA Patriot Act on Government Outsourcing", (6 Aug 2004), 10 pages.

Canadian Advanced Technology *Alliance,* (6 Aug 2004), 2 pages.

Canadian Internet Policy and Public Interest Clinic, "Submission on the *USA Patriot Act* and its Impact on the Privacy of BC Citizens' Personal Information in the Context of Government Outsourcing of Data Administration", (2 Aug 2004), 27 pages.

Canadian Union of Public Employees, BC Division, "Addendum to the Submission on the USA Patriot Act", (6 Aug 2004), 1 page.

Canadian Union of Public Employees, BC Division, "Submission on the USA Patriot Act", (4 Aug 2004), 22 pages.

Canadian Vehicle Manufacturers' Association, "Submission on the USA Patriot Act", (6 Aug 2004), 2 pages.

Carpenters Union Local 1995, (3 Aug 2004), 1 page.

Comox Valley Chapter Council of Canadians, "Submission to the Privacy Commissioner from the Comox Valley Chapter Council of Canadians", (1 Aug 2004), 1 page.

Council of Canadians, "A Submission on the USA Patriot Act to the Information and Privacy Commissioner for British Columbia", (6 Aug 2004), 6 pages.

Council of Senior Citizens' Organizations of BC, (4 Aug 2004), 2 pages.

Credit Union Central BC, "Submission on the USA Patriot Act", (22 July 2004), 2 pages.

Dutch Data Protection Authority, "Examination of USA Patriot Act Implications", (9 Aug 2004), 2 pages.

EDS Canada Inc., "USA Patriot Act Implications for Privacy Compliance under British Columbia's *Freedom of Information and Protection of Privacy Act"*, (19 July 2004), 46 pages.

Fasken Martineau DuMoulin LLP, "Submission on the USA Patriot Act", (5 Aug 2004), 40 pages.

Federal Bureau of Investigation, "Implications of USA Patriot Act on Information Pertaining to British Columbia Residents", (18 Aug 2004), 3 pages.

Fraser Valley / White Rock Chapter CARP, "Submission on the USA Patriot Act", (5 Aug 2004), 6 pages.

Green Party of BC, "Submission on the USA Patriot Act", (6 Aug 2004), 1 page.

Information and Privacy Commissioner for PEI, "Submission on the USA Patriot Act", (5 Aug 2004), 5 pages.

Information Technology Association of Canada, "Submissions of the Information Technology Association of Canada Regarding the *USA Patriot Act*", (5 Aug 2004), 65 pages.

INTRIA Items Inc., "Submission on the USA Patriot Act", (6 Aug 2004), 2 pages.

MAXIMUS, "MAXIMUS Response to Request for Submissions Assessing USA Patriot Act Implications for Privacy Compliance", (23 July 2004), 32 pages.

Microsoft Canada Co., "Submission on USA Patriot Act", (5 Aug 2004), 2 pages.

MYRA Systems Corp., "MYRA Systems Submission on the USA Patriot Act", (6 Aug 2004), 8 pages.

New Brunswick Ombudsman, (4 Aug 2004), 3 pages.

Office of the Privacy Commissioner of Canada, "Transferring Personal Information about Canadians Across Borders", (16 Aug 2004), 15 pages.

Party of Citizens, "The Patriot Act in a Psychopolitical Context", (31 July 2004), 3 pages.

Privacy International, "Response to British Columbia Information and Privacy Commissioner", (Aug 2004), 7 pages.

Prof. Michael Geist & Milana Homsi, LL.B,. "The Long Arm of the USA Patriot Act: A Threat to Canadian Privacy?" (26 July 2004), 34 pages.

Prof. Reg Whitaker, "Implications of *USA Patriot Act* for Outsourcing of Public Services to US-linked Service Providers", (5 Aug 2004), 7 pages.

Professional Employees Association, "Submission on the USA Patriot Act", (16 July 2004), 2 pages.

Province of British Columbia, "Examination of USA Patriot Act Implications for Personal Information of British Columbia Residents Involved in Outsourcing of Government Services to US-Linked Services Providers", (23 July 2004), 102 pages.

Province of British Columbia (further submission), "Examination of the USA PATRIOT ACT Implications for Personal Information of British Columbia Residents Involved in Outsourcing of Government Services to US-linked Service Providers", (9 Sep 2004), 6 pages.

Public Services International, "Submission on the USA Patriot Act", (14 July 2004), 2 pages.

REACH Community Health Care, "Submission on the USA PATRIOT Act", (6 Aug 2004), 2 pages.

Retail Council of Canada, Canadian Chamber of Commerce and BC Chamber of Commerce, "Submission on the USA Patriot Act", (5 Aug 2004), 4 pages.

Seniors Network of BC, "Submission on the USA Patriot Act", (6 July 2004), 1 page.

Tenough Coalition, "Assessing *USA Patriot Act* Implications for Privacy Compliance", (6 Aug 2004), 12 pages.

The British Columbia Public Interest Advocacy Group, "Assessing 'USA Patriot Act' Implications for Privacy Compliance under British Columbia's *Freedom of Information and Protection of Privacy Act*", (June 2004), 6 pages.

US Department of Homeland Securities, "(6 Aug 2004), 3 pages.

Vancouver Coastal Health Authority & Providence Health Care, "Submission on the USA Patriot Act", (6 Aug 2004), 11 pages.

Vancouver Public Library, "Examination of the *USA Patriot Act* Implications for Personal Information of British Columbia Residents Involved in Outsourcing of Government Services to US-linked Service Providers", (6 Aug 2004), 6 pages.

Vancouver Women's Health Collective, (6 Aug 2004), 1 page.

Women Elders in Action, "A Submission to the Privacy Commissioner From Senior Women in BC", (28 July 2004), 4 pages.