Privacy Implications of the USA Patriot Act

by Jennifer Stoddart

The United States Congress passed the USA Patriot Act soon after the September 11, 2001 terrorist attacks. It gives new investigative powers to law enforcement agencies in the US. Section 215 of the Act allows a special court to secretly issue an order requiring "the production of any tangible things" to the FBI. This can include an individual's personal information. Anyone served with such a secret order is prohibited from disclosing to anyone else that the order exists or has been complied with. When Canadian privacy commissioners met in May 2004 in Victoria, BC, a general consensus emerged that exchange of personal information across borders was becoming increasingly significant in the context of continental economic integration. The British Columbia Information and Privacy Commissioner released his advisory report on the privacy implications of the USA Patriot Act on October 29, 2004. More than 500 representations were received about this issue including the following submission from the Privacy Commissioner of Canada.

We live in a virtual world where the global transmission of information is becoming almost seamless. The operations of governments and corporations are profoundly transformed by the emergence of e-government and e-commerce. Electronic collection, use, sharing and storage of personal information is at the hub of this transformation which modifies not only the way organizations carry out their daily business but also, more fundamentally, the manner by which they communicate with citizens, consumers, clients and stakeholders.

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.

The issue of transfers of personal information across borders goes to the heart of national sovereignty as well as to Canadian identity. As a society, we must think more broadly about the mix of policy instruments that will provide an adequate level of protection of personal information as required by the Personal Information Protection and Electronic Documents Act (PIPEDA), the Privacy Act and equivalent provincial and territorial statutes. This reflection is necessary if Canada is to maintain its leadership in privacy protection.

Jennifer Stoddart is the Privacy Commissioner of Canada. *This article is a slightly edited version of her submission dated August 16, 2004 to the British Columbia Information and Privacy Commissioner on the issue of transferring personal information about Canadians across Borders.*

Governments across Canada have introduced many measures in recent decades to protect the personal information of Canadians. Most significantly, they have developed laws regulating the collection, use and disclosure of personal information by governments and private sector organizations.

At the federal level, the *Privacy Act*, which came into force in 1983, regulates the collection, use and disclosure of personal information in the public sector by about 150 federal institutions. All provinces and territories have similar public sector legislation.

Canada has gone one step further by setting privacy standards for information handling in the commercial private sector. Beginning in stages since 2001, the *Personal Information Protection and Electronic Documents Act* has regulated the handling of personal information in the private sector across the country. Several provinces have enacted similar privacy standards. PIPEDA brings Canada law into line with privacy standards for personal information developed by the European Union, and means that our standards for the protection of personal information, when used by a commercial organization, are among the most stringent in the world. PIPDEA establishes a progressive framework, based on the highest international standards, against which to assess personal information management practices of the public and private sectors in Canada. It provides a framework for benchmarking best practices and encourages organizations that collect and process personal information to emulate those practices.

The Office of the Privacy Commissioner has repeatedly argued over the years that there is no inherent contradiction between the protection of privacy and the promotion of national security and public safety. Others have expressed similar views. Some suggest that a new public policy hybrid needs to emerge — a model that would have Canadians collectively set the terms and conditions by which sensitive personal information (financial, health and judicial, for example) would be shared across organizational and national boundaries. Decision-makers and policy analysts will not be the only ones concerned. Parliamentarians, civil servants, business and union leaders, civil society advocates and service providers also need to be engaged in an informed public dialogue on how to prevent further erosions of privacy.

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 organizational boundaries. It is important for Canadians to understand these flows of information. When is personal information about them transferred outside Canada, to whom, and for what purposes? What rules govern the handling of such information when it has been transferred abroad? Various rules may apply, depending on whether information is held by a government agency or by the private sector, in Canada or abroad, by a Canadian stand alone organization or by an organization whose parent may be in the United States or another foreign country. When and how can personal information held in Canada about Canadians nonetheless be made available to foreign governments? How can Canadians participate in determining the nature of these flows?

This submission highlights some of the most important questions about the transfer of personal information across borders, the application of the federal Privacy Act and PIPEDA and, finally, what Canadians can do about protecting their personal information in this environment.

How is Personal Information about Canadians Transferred Across Borders?

In our world of globalized economies and increasingly interdependent policy environments, personal information is regularly exchanged across borders. Here we explain the many ways in which personal information about Canadians may be transferred outside Canada's borders in many ways incuding:.

1. By organizations in Canada transferring to organizations in foreign countries

"Globalization" has resulted in much more sharing of information held by companies in Canada, including personal information, across borders. This is a fact of contemporary life. Canada's largest single trading partner is the United States (accounting for approximately 85

per cent of the value of Canada's export trade), so it is little surprise that much personal information about Canadians finds its way into the databanks of companies in the United States.

It is to respond to and to attempt to bring some globally recognized privacy standards to this flow of information that PIPEDA states that transfers of personal information can only be made if the requirements of the Act are satisfied — that is to say, if the organization receiving the information promises to protect the information. Organizations transferring personal information must use "contractual or other means" to ensure that a company located in another country provides a level of protection to the personal information comparable to that which it would receive in Canada if the laws in that country do not provide for comparable protection.

Organizations in Canada are also obliged to employ security safeguards to protect personal information against unauthorized access and disclosure. In some cases, this could mean not transferring personal information outside Canada in order to protect it from disclosure to a foreign government.

Note that PIPEDA does not apply to all private sector organizations in Canada. It applies to most commercial organizations in Canada, except where an equivalent provincial law is in force. If an equivalent provincial law is in force, that law would regulate the information handling practices of commercial organizations in the "provincially regulated" private sector.

PIPEDA is focused on commercial organizations only. Organizations that do not have commercial activities are not covered. In such cases, PIPEDA does not pose any obstacle to the transfer of personal information abroad.

Since PIPEDA does not apply to employee records in provincially regulated commercial organizations, this information can be transferred across borders without restriction unless there is corresponding provincial private sector privacy legislation (as in Quebec, and soon Alberta and British Columbia). That means that employee records from some of the largest companies in Canada can be transferred across international borders with little concern for what happens to that information after it crosses those borders.

2. By Organizations in Canada Transferring Personal Information Under Legislative

Sometimes specific legislation overrides PIPEDA and permits commercial organizations to disclose personal information about Canadians to foreign governments. Amendments made to the *Aeronautics Act* in 2001, for example, permit air carriers in Canada to provide to a foreign state certain information in their control about persons on board or expected to be on board the aircraft and that is required by the laws of the foreign state.

3. By Government Agencies in Canada Transferring Personal Information to Foreign Governments

Canadian law often permits government agencies to share personal information that is held in Canada (by government or the private sector) with foreign governments and organizations, even without the consent of the individual to whom the information relates. Several procedures for sharing information are described here.

The federal *Privacy Act* allows personal information to be transferred outside Canada, even without the consent of the individual to whom the information relates. For example, the Act allows personal information under the control of a government institution (for example, information collected to issue passports) to be disclosed for specific purposes under an agreement or arrangement between the Government of Canada and the government of a foreign state. These purposes include administering or enforcing any law or carrying out a lawful investigation.

One such "agreement" is the *Mutual Legal Assistance Treaty* (MLAT) between Canada and the United States (Canada has signed similar treaties with 33 countries, including the United Kingdom, Australia and France, and two multilateral treaties also contain mutual legal assistance provisions). The Canada-US treaty came into force in 1990 and is an important tool for both governments to obtain evidence located in the territory of the other. US authorities might, for example, want information held by provincial, territorial or federal governments, by individuals in Canada, or by companies in Canada, in relation to a broad range of offences. They can rely on the treaty to obtain this information. Numerous tax and other treaties entered into by Canada also permit the transfer of personal information from Canada to foreign governments and agencies.

If United States authorities want to obtain personal information held by a federal or provincial government, a company or an individual in Canada, the usual course of action is to make a request to the Government of Canada under the *Canada-US Mutual Legal Assistance Treaty*. Canada's federal Department of Justice may then apply to a court in Canada for a search warrant to compel the disclosure of the information. Once the information is obtained, the Department of Justice transmits the information to the United States government. Section 7 of PIPEDA permits the company to disclose personal information that is required to comply with a subpoena or warrant issued by a court, or to comply with a court order.

Other legislation sometimes authorizes specific information transfers. The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, amended in 2004, is one example. The Act authorizes the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) to process and analyze reports from financial institutions and other designated entities on suspicious financial transactions. The goal of the legislation is to reduce money laundering and terrorist financing. FINTRAC has access to national security databases, as well as those relating to law enforcement. The activities of FINTRAC clearly involve significant collection and use of personal financial information about individuals. Furthermore, FINTRAC is permitted to enter into agreements with similar institutions or agencies in foreign states for the exchange of information relating to its work.

Another example of legislation authorizing the transfer by government of personal information outside Canada is the *Department of Immigration and Citizenship Act*. The Act permits the Minister to enter into agreements or arrangements with foreign governments and international organizations that involve collecting, using and disclosing personal information relating to programs for which the Minister is responsible.

The *Canadian Security Intelligence Service Act* permits the Service (known as CSIS), if it has the approval of the appropriate Minister, to enter arrangements or cooperate with the government of a foreign state, an institution of that state, or an international organization of states. Clearly, this cooperation could involve the transfer of personal information about Canadians.

In many cases where government departments or agencies transfer personal information abroad, there may be no specific legislation or treaty involved, but simply a Memorandum of Understanding with a government agency in another country allowing for the transfer of personal information.

One important role of the Office of the Privacy Commissioner is to evaluate the privacy impacts of such arrangements and to review the practices in place to see whether or not the terms of any Memorandum are, in fact, respected. These audits and privacy impact reviews are vital functions of the Office.

4. By Government Agencies Transferring Personal Information for Processing by Companies Abroad

Canadian government agencies also sometimes transfer personal information about Canadians to companies in other countries to be processed there – another by-product of our globalized and interdependent economies. Relying on an outside company to process personal information is commonly called "outsourcing."

5. By Canadians Themselves

Canadians themselves give considerable personal information to foreign governments or companies. Canadian travelers are required to provide information to immigration officials when they enter a foreign country by submitting their passports, visas and other records that the country may require them to supply. Canadians may also supply personal information to companies when they do business. Registering for computer software support services, for example, may require supplying information to a company in a foreign country that provides those services.

The USA Patriot Act

Once personal information about Canadians is transferred outside Canada, whether by a Canadian government agency, a private organization or by Canadians themselves, the laws of the country to which the information has been transferred will apply. Those laws will determine when government agencies such as the police, security and tax authorities can obtain access to that personal information. (The same principle also applies in Canada. Foreign companies that operate in Canada must comply with Canadian laws.) In some cases, the foreign law may allow access to personal information about Canadians in situations that many Canadians might find objectionable or inappropriate. This is why the Office of the Privacy Commissioner participates actively in international forums where the rules applying to the circulation of personal information across borders are debated, whether it be for commercial or government purposes, so that the high standards of information protection which Canadians enjoy generally continue to apply whenever possible outside Canada.

The USA Patriot Act, enacted in 2001 by the United States Congress, is just one example of a law enacted in a foreign country that allows access to personal information about Canadians that is held in the United States. The Act enhances access by the Federal Bureau of Investigation (FBI) to records held by companies in the United States. The Act amends the US Foreign Intelligence Surveillance Act of 1978 to permit the Director of the Federal Bureau of Investigation (FBI) to apply to a court in the United States for an order to disclose records, papers, documents and other items for an investigation to protect against international terrorism or clandestine intelligence activities.

If a judge grants an order, a company subject to the order is compelled to provide the information, which could include any personal information about Canadians that it holds. Furthermore, the company would be prohibited

from disclosing to others that the FBI has sought or obtained this information. In other words, the companies cannot tell the individuals that their personal information has been sought or obtained under the order.

The USA Patriot Act is relatively new, but the concept behind the legislation is not. The Act is simply one example of a law that can give the United States government or its agencies access to personal information about Canadians that has been transferred to the United States. Research done by the Office of the Privacy Commissioner and discussions with the Department of Justice suggest that the USA Patriot Act is not likely in the normal course of events to be used to obtain personal information held in the United States about Canadians. It is far more likely that existing means of obtaining such information will continue to be used instead, such as "grand jury subpoenas", "national security letters" and ordinary search warrants issued in criminal investigations.

In addition, US government agencies can rely on other established procedures to obtain information about Canadians that is held by government or the private sector in Canada. Longstanding information sharing agreements between security and law enforcement agencies in both countries, and the mutual legal assistance process, are the most likely vehicles for obtaining access to information held in Canada.

Governments around the globe have long exercised the right to obtain information held by organizations within their borders. Many Canadian laws also enable police, security agencies and government departments generally to obtain access to personal information held in Canada. In short, Canadian government agencies can obtain personal information held in Canada about foreign individuals, just as a foreign government can obtain personal information that may be held in that country about Canadians. Furthermore, Canadian police and security agencies can obtain information held abroad about foreign individuals by using mutual legal assistance procedures and information-sharing agreements.

Whose Laws Apply to Personal Information?

The ongoing discussion about the impact of the USA Patriot Act has highlighted the confusion that exists about the legal obligations of organizations faced with an order made under United States law to provide information they hold. The following sets out the position of the Privacy Commissioner of Canada on these issues.

1. Organizations Operating in a Foreign Country

Organizations operating in a foreign country that hold personal information about Canadians in that country must comply with the laws of that country. For example, if they are presented with an order requiring them to disclose personal information, they must surrender that information.

This has important implications for the "outsourcing" by a company in Canada subject to PIPEDA of data processing to organizations based abroad. For example, if a Canadian company outsources the processing of personal information to the United States, that personal information may be accessible under US law. The broader policy question is whether the Canadian company should outsource personal information when that information will become subject to such laws. At the very least, a company in Canada that outsources information processing in this way should notify its customers that the information may be available to the US government or its agencies under a lawful order made in that country.

2. Commercial Organizations Operating in Canada, and not in any Foreign Country

Organizations in Canada that are regulated by PIPEDA (that is, most commercial organizations in Canada) or equivalent provincial laws such as those in Quebec, and soon British Columbia and Alberta, must comply with PIPEDA or the equivalent provincial legislation. The clearest case is that of a company based only in Canada and that maintains personal information only in Canada. Any order made by a foreign government or court (very unlikely to occur, if the company operated only in Canada) would have no legal force against the company. The Office of the Privacy Commissioner is of the opinion that the company would have no legal duty to provide the personal information to the foreign government, and would violate PIPEDA if it did so without the consent of the individuals to whom the information relates.

However, as noted above, specific Canadian legislation may override PIPEDA and permit Canadian organizations to provide personal information to a foreign agency. Amendments made to the *Aeronautics Act* permit air carriers in Canada to provide to a foreign state certain information in their control about persons on board or expected to be on board the aircraft and that is required by the laws of the foreign state.

3. Commercial Organizations Operating Both in Canada and in a Foreign Country

The situation is more complicated where a commercial organization subject to PIPEDA operates both in Canada and a foreign country. Organizations operating in the foreign country must comply with the law of that country, just as organizations operating in Canada must comply with Canadian law. Therefore, as discussed above,

an organization that operates in the United States and that holds personal information in the United States about Canadians must comply with an order made by a US court to disclose information the organization holds.

If the organization in the foreign country has a related organization in Canada that holds personal information about Canadians in Canada, an order by a foreign court cannot compel the disclosure of the information that is held in Canada. The organization in Canada will be subject to PIPEDA or its provincial equivalent. It is not bound by the order made in the foreign country. Furthermore, it has an obligation under PIPEDA to take appropriate security measures to prevent the unauthorized disclosure of the personal information it holds. This may mean employing technical measures to prevent its related organization in the foreign country from inappropriately getting access to the personal information held in Canada.

4. Outsourcing of Data Processing by Canadian Federal Government Institutions

If a federal government institution hires a company in a foreign country to process personal information about Canadians in that country, the laws of that country will apply to the personal information. A court order made by a court in that country could compel the company to disclose that information.

Unfortunately, the federal *Privacy Act,* now over 20 years old, does not require effective safeguards to be introduced by government institutions against the misuse of personal information about Canadians that has been transferred across borders (However, other legislation or contractual agreements may offer some protection to the information). This is one more reason, among many, for a thorough review of the *Privacy Act*.

What Canadians Can Do to Protect Their Personal Information

Canadians benefit from a reasonable standard of protection of their personal information. They do not want to see that protection vanish when personal information about them is transferred across borders, and they do not want to see governments or organizations in Canada transfer their information across borders if it will be put at risk of inappropriate disclosure, whether for security or for commercial purposes.

The extent to which personal information about Canadians should be made available to foreign governments is a complex issue of continuing concern. Nonetheless, Canadians can take some measures to protect their personal information from inappropriate disclosure to foreign governments:

- By bringing complaints about the handling of personal information (especially outsourcing arrangements) to the Office of the Privacy Commissioner of Canada or provincial and territorial commissioners, depending on the organization whose conduct has raised the concern;
- By relying on the "whistle blowing" provisions of PIPEDA if an organization in Canada regulated by the Act seeks to provide personal information held only in Canada under an order given to its parent or subsidiary in the United States. These provisions would protect the confidentiality of employees who notify the Privacy Commissioner of Canada that a company intends to transfer information abroad in violation of PIPEDA. The provisions also protect employees against retaliation by the employers, such as harassment, dismissal or demotion;
- By letting organizations in Canada that collect personal information about Canadians know that there is a concern about personal information being processed outside Canada;
- By taking advantage of the information rights existing under PIPEDA and provincial private sector statutes which require organizations to follow fair information practices, notably obtaining consent for information use;
- By reminding companies in Canada of their legal obligation to introduce appropriate security measures to prevent their subsidiaries or affiliates in another country from secretly obtaining access to personal information held in Canada to comply with a court order made in the foreign country;
- By raising their concerns about the potential for excessive disclosure of personal information to foreign governments or to foreign companies with their elected representatives; and
- Generally, by being more attentive to what may be happening to their personal information when it crosses borders and to the importance of clear and enforceable international standards on information sharing in democratic countries.

There is no substitute for an informed citizenry that demands of government and corporate leaders the highest standards in privacy protection. While not a panacea for erosion of privacy, civic engagement exerts a compelling force on custodians of personal information to be more vigilant in adhering to privacy standards.

What Can Companies Do?

Companies that are subject to PIPEDA or similar provincial legislation must comply with that legislation. It is important for the management of organizations subject to such laws to understand their responsibilities under the laws – for example, the obligations in PIPEDA to ensure the security of personal information. PIPEDA requires personal information to be protected by security

safeguards appropriate to the sensitivity of the information.

Corporate leaders increasingly recognize that maintaining a high level of public trust in how personal information is handled is vital to achieve customer loyalty. It is also abundantly clear to corporate leaders that personal information holdings are key business assets that need to be protected against misuse.

What Can the Government of Canada Do?

As early as 1987, Canadian Parliamentarians were expressing concern about transfers of personal information across borders. That year, a parliamentary committee reviewing the *Access to Information Act* and the *Privacy Act* recognized the extent to which personal information was crossing borders. It concluded that:

> Personal data on Canadians is routinely being transferred and stored outside of the country by federal or provincial governments and the private sector. … Canadians in particular deserve to know more about transborder data flows of their personal information in such varied fields such as banking, credit information systems, credit card services, health care information, labour unions, personnel and payroll records, airline travel reservations and general government activities. … The Committee has resisted the temptation to ask the Privacy Commissioner to conduct and table in Parliament . . . a special study under section 60 of the Privacy Act, since the resources and expertise needed for such an undertaking are spread across the government. Indeed, a number of major government institutions, especially the Department of External Affairs [now DFAIT] and the Department of Justice, already have significant responsibilities for the privacy aspects, and other important aspects, of transborder data flows. Unfortunately, these oversight roles have not attracted adequate attention and resources in recent years. (Open and Shut: Enhancing the Right to Know and the Right to Privacy, March 1987, p. 80).

The response of the Government of Canada to the Committee's report was promising:

> The government agrees with the Committee that this matter [the transborder flow of data] requires study and has already begun to explore the means by which to determine whether such a problem exists, and if this is found to be the case, the government will move to address it. (Government of Canada, Access and Privacy: The Steps Ahead, 1987, p. 13)

Unfortunately, the promise of the Government's response did not appear to be matched by actions. Now, seventeen years later, after the advent of the Internet, cyber- government and a renewed determination by all liberal democracies to fight terrorism and global crime, it would seem timely, opportune and appropriate to examine the governance of international transfers of personal information. Such a review would need to factor in the three years of implementing PIPEDA, its up-coming legislative review in 2006 and an eventual reform of the *Privacy Act* to ensure that the federal government practices in handling personal data are kept at the highest standards.

The Canadian government, under the aegis of an Assistant Deputy Ministers' Privacy Committee, is currently examining the robustness and comprehensiveness of the federal privacy framework which would extend to both the public sector and private sector activities under federal jurisdiction. As part of the work of this Committee, the Office of the Privacy Commissioner of Canada will advocate that the full spectrum of policy instruments, including public education, contractual agreements and technological solutions be examined to better protect personal information flows both within Canada and outside our borders.

What the Privacy Commissioner is Doing

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 part 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.

In the next few years there are several opportunities for a rigorous and balanced examination and an informed public debate on extraterritorial flow of personal information. The Office of the Privacy Commissioner of Canada will participate as fully as possible in these activities. These include:

- A planned audit in 2004-2005 of the transfer of personal information between Canada and the United States;
- On-going discussions with representatives of the Canadian Department of Public Security and Emergency Preparedness and the US Department of Homeland Security on personal information practices of federal entities;
- The creation of a National Security Committee of Parliamentarians;
- The 2006 legislative review of PIPEDA; and
- An eventual reform of the *Privacy Act*.

The Office will participate actively in coming reviews of anti-terrorism legislation and service delivery initiatives such as E-government (for example, the electronic transfer of health care records and similar initiatives.)

The Office will also maintain its ongoing dialogue with industry leaders and professional associations to ensure that they fully understand their obligations under private sector privacy legislation. It will also seek to better understand the practice of cross-border information transfers. The Office also plans to initiate a dialogue with the private sector in the coming months about the extent and appropriateness of such transfers.

Conclusion

The circumstances under which personal information held by the private sector in Canada should be transferred to organizations in other countries is an important policy issue that needs further examination.

As well, the Government of Canada should reexamine the circumstances under which it allows personal information about Canadians to be processed outside Canada. The Office recognizes that this examination involves more than a simple consideration of the privacy interests of Canadians. It will also involve addressing the important economic benefits that can flow from outsourcing, and Canada's obligations under its trade agreements that may relate to the flow of personal information across borders.

The Commission of Inquiry into the *Actions of Canadian Officials in Relation to Maher Arar* may shed some light on the transfer of personal information about Canadians across borders in national security matters. Other departments and agencies of governments need to perform a similar examination of the transfer of personal information about Canadians to foreign governments and agencies. And they need to explain the nature of these transfers to Canadians. Canadians need to understand the full extent to which their personal information is transferred across borders, and the full extent to which personal information about them can be and is made available to foreign governments and organizations.

Canadians are not alone in wondering what happens to the information they give to their governments or to the private sector in an age of instantaneous global data flow, vigorous international trade, heightened concern about national security, and increased outsourcing. The Office of the Privacy Commissioner of Canada has raised the questions discussed here with its international counterparts. The Office places great importance on fostering appropriate international privacy standards for the transfers of personal information across borders.

If Canadians hope to preserve the fundamental values that they cherish in a democracy, including privacy, they too must ask questions. The security of our personal information is a collective endeavour. Privacy commissioners cannot do the job alone. Canadians need to accept responsibility for informing themselves. Who is using their personal information, and for what purposes? In an environment where privacy values are increasingly under siege, where some see the right to privacy as an unnecessary frill, it is not too much to ask our citizens to stand up for their privacy. In fact, it is essential to ask.