

LEGAL RESTRICTIONS ON TRANSBORDER DATA FLOWS
TO PREVENT GOVERNMENT ACCESS TO PERSONAL DATA:
LESSONS FROM BRITISH COLUMBIA

Fred H. Cate¹

August 2005

¹ **Fred H. Cate** is a Distinguished Professor of Law, Adjunct Professor of Informatics, and director of the Center for Applied Cybersecurity Research at Indiana University. A senior policy advisor to the Center for Information Policy Leadership at Hunton & Williams, he is a member of Microsoft's Trustworthy Computing Academic Advisory Board and of the National Academy of Sciences Committee on Information for Terrorism Prevention. The author gratefully acknowledges the thoughtful comments of Commissioner David Loukidellis, Joe Alhadeff, Jennifer Barrett, Peter Cullen, Brian O'Connor, and Harriet Pearson, and the able research assistance of Elena Dicus. The author alone is responsible for the views expressed herein.

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

Executive Summary

The British Columbia Report. In October 2004, the Information and Privacy Commissioner of British Columbia, Canada, issued a report arguing that there is a “reasonable possibility” that the U.S. government will use section 215 of the USA Patriot Act to obtain access to personal health data about British Columbia residents if those data are outsourced to “US-linked” companies in Canada.² The report concluded that such access would violate provincial privacy law.

As a result, the report recommended that British Columbia prohibit personal information held by the public sector from being transferred to, or accessed from, outside of Canada, and block companies that process personal data for public bodies from complying with other nations’ laws or judicial orders seeking those data “punishable by a fine of up to \$1 million or a significant term of imprisonment, or both.” The report recommended that the Canadian government implement similar requirements on the national level and also “address the implications of the USA Patriot Act for the security of personal information that is entrusted to *private* sector custody or control.”

The British Columbia Privacy Law. The government of British Columbia did not wait for the Commissioner’s report to be published before taking action. In October 2004 the Legislative Assembly adopted a law requiring each public body to ensure that “personal information in its custody or under its control is stored only in Canada and accessed only in Canada.”³

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

The Flaws of the British Columbia Approach. The British Columbia report and privacy law are seriously flawed and have contributed to misfocusing the growing debate over privacy issues in multinational information flows. Among the issues addressed below:

- They ignore the fact that section 215 of the USA Patriot Act has only been used 35 times since being expanded in 2001, is very unlikely to be used to attempt to access Canadian’s records being processed in the United States, and is already governed by the Mutual Legal Assistance Treaty between Canada and the United States if it were to be invoked.
- They ignore the requirement in British Columbia law that privacy protections only be “reasonable,” not perfect or complete, and the exceptions in the law that permit transfers of personal data for important reasons, such as national security or law enforcement.

² Information and Privacy Commissioner of British Columbia, *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing* (Oct. 2004).

³ Bill 73—the Freedom of Information and Protection of Privacy Amendment Act, 2004.

- The report focuses on privacy and downplays security, thereby threatening to compromise the latter by overprotecting the former.
- The report focuses exclusively on U.S. companies with Canadian subsidiaries, thus ignoring the reality that any threat to Canadian data posed by section 215 or other provisions of U.S. law, however slight that may be, is posed equally against Canadian companies with U.S. subsidiaries or service providers.
- The report and privacy law pose real threats to individuals and businesses. Multinational companies are reporting stringent new terms being added to Canadian and provincial government outsourcing contracts forbidding personal data from being transferred to, or accessed from, the United States; prohibiting the involvement of U.S. employees of service providers; and even requiring restructuring of multinational business entities. In the case of the British Columbia health benefits administration contract that sparked the report and the new law, the government required the winning bidder to create a new British Columbia subsidiary to carry out the contract, and required that the stock of the new subsidiary be placed in a trust, with the shares to be handed over to the government—along with a \$35 million penalty—in the event personal data are transferred, or accessed from, outside of Canada.
- Most importantly, the report and the law adopt a provincial solution to a global issue. Prohibiting the transfer of personal data to, or access from, outside of Canada is simply not a workable approach for the information age. It denies the efficiencies and economies of scale that global information flows make possible.

Future Risks and the Need for a New, Multinational Approach. The British Columbia report and law are only a start. Other provinces, the Canadian federal government, and other countries in Europe and Asia are also examining the potential impact of the USA Patriot Act on outsourcing arrangements involving the personal information of their residents. Many other nations, including Canada, have laws similar to the USA Patriot Act that provide limited access to personal data, with judicial authorization, for national security purposes. If the British Columbia approach extends to other nations' laws and spreads across Canada, across sectors, and ultimately across the globe, multinational data flows will be severely threatened.

The harm to individuals and institutions of the British Columbia approach to data protection is already clear. If magnified across provinces and nations, and applied to private- as well as public-sector data processing, the impact could be extraordinary. It will be measured not only in terms of economics and convenience, but jobs, health, and security. Such a serious, multinational issue requires a serious, multinational response, not the unilateral, provincial legislation adopted by British Columbia.

The critical issues highlighted by the British Columbia report and law, and especially the question about how to deal with divergent national legal systems that increasingly come into conflict as data move across national borders, warrant thoughtful consideration. While the concerns are not new, powerful information technologies, global networks, and the multinational commerce, outsourcing, and information sharing they have made possible are inevitably going to

cause new and more frequent conflicts between divergent national (and provincial) approaches to privacy and information management. Those same technologies and activities, our growing reliance on them, and the important values they implicate—including privacy and security—also heighten the urgency of finding multinational, diplomatic solutions that protect global information flows.

LEGAL RESTRICTIONS ON TRANSBORDER DATA FLOWS
TO PREVENT GOVERNMENT ACCESS TO PERSONAL DATA:
LESSONS FROM BRITISH COLUMBIA

The British Columbia Report

In October 2004, the Information and Privacy Commissioner of British Columbia issued a report, *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing*.⁴ The report concluded a six-month inquiry into two issues: (1) whether the USA Patriot Act⁵ would permit U.S. government access to British Columbian health records that had been outsourced to “US-linked private sector service providers”; and (2) if it does, whether this violates the British Columbia Freedom of Information and Protection of Privacy Act (FOIPPA).⁶

The inquiry had been sparked by a lawsuit by the British Columbia Government and Service Employees’ Union. The union had sought to block the provincial government from contracting out administration of its public sector health program. The lawsuit alleged, among other charges, that contracting out the administrative role to a company linked to the United States would threaten the privacy of public sector employees and violate British Columbian law by subjecting their health data to possible seizure under the USA Patriot Act.⁷

The primary focus of the privacy concerns was section 215 of the USA Patriot Act, which amended a 1978 law empowering senior FBI officials to apply to the U.S. Foreign Intelligence Surveillance Court for a secret order requiring the disclosure of certain business records in connection with foreign intelligence and terrorism investigations.⁸ The USA Patriot Act, adopted in the aftermath of the September 11, 2001, terrorist attacks, expanded the scope of those orders so that they could be used to obtain “any tangible thing” from any individual or entity subject to the court’s jurisdiction, as part of “an investigation to protect against international terrorism or clandestine intelligence activities.”⁹

The October British Columbia report was far-reaching and extended well beyond the two questions on which Commissioner David Loukidellis had sought public input. On the first of those questions, however, the report concluded that there is a “reasonable possibility” that the U.S. government will use section 215 of the USA Patriot Act to obtain access to personal health

⁴ Information and Privacy Commissioner of British Columbia, *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing* (Oct. 2004).

⁵ *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, Pub. L. No. 107-56, 115 Stat. 272 (2001).

⁶ *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165.

⁷ *British Columbia Government & Service Employees’ Union v. the Minister of Health Services and the Medical Services Commission*, 2005 B.C.S.C. 446, 2005 B.C.D. Civ. J. 1807.

⁸ Pub. L. No. 107-56, § 215.

⁹ *Id.*

data about British Columbia residents if those data are outsourced to “US-linked” companies in Canada.¹⁰

In response to the second question, the report concluded that such access violates two provisions of provincial privacy law.¹¹ Section 30 of FOIPPA requires the government 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.”¹² Section 33 prohibits disclosure of personal data by the government unless specifically authorized by one of the specified exemptions. At the time the report was written, those exemptions included “in accordance with a provision or a treaty, arrangement or agreement,” “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 the information,” or “to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority.”¹³

The report found that U.S. law—and the law of other Canadian provinces and “possibly” even of Canada itself¹⁴—could never be sufficient to “authorize” disclosure under either section 30 or 33, and that the risk of disclosure under the USA Patriot Act is too great to allow data about British Columbia residents to come within the Act’s reach. According to the report, “sovereignty and territoriality,” as well as “privacy,” demand that for privacy purposes, British Columbia prohibit at least personal data held by or for the public sector from being exported to or even accessed from outside of Canada.

The report concluded with 16 recommendations. The most important and immediate of these would amend FOIPPA to:

- “pending nation-to-nation agreement [see below], . . . 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”;¹⁵
- “pending nation-to-nation agreement [see below], . . . prohibit personal information in the custody or under the control of a public body from being . . . accessed outside Canada”;¹⁶

¹⁰ Privacy and the USA Patriot Act, *supra* at 18.

¹¹ *Id.* at 17, 115-16.

¹² FOIPPA, *supra* § 30.

¹³ *Id.* §§ 33(d), (e), (o). After the report was prepared, FOIPPA was amended to permit disclosure “to comply with a subpoena, warrant or order issued or made by a court, person or body in Canada with jurisdiction to compel the production of information,” *id.* § 33.2(b), and “to a law enforcement agency in a foreign country under an arrangement, a written agreement, a treaty or provincial or Canadian legislative authority,” but only by a “public body that is a law enforcement agency.” *Id.* § 33.1(2).

¹⁴ Privacy and the USA Patriot Act, *supra* at 107.

¹⁵ *Id.* at 134 (Rec. 1(a)).

¹⁶ *Id.* at 134-35 (Rec. 1(a)).

- “require a contractor to a public body to notify the public body of any subpoena, warrant, order, demand or request made by a foreign court or other foreign authority for the disclosure of personal information” about British Columbians, even if doing so violates the national law to which the contractor is subject;¹⁷
- “make it an offense 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”—even if in response to “a subpoena, warrant, order, demand, or request by a court or other authority,” unless “it is a Canadian court, or other Canadian authority”—“punishable by a fine of up to \$1 million or a significant term of imprisonment, or both”;¹⁸ and
- empower the Commissioner to be able to “enter contractor premises, obtain and copy records, and order compliance,” apparently without first obtaining a warrant or other judicial authorization.¹⁹

The report recommended that the federal government implement similar requirements on the national level.²⁰

Although the focus of the report was personal data outsourced by the public sector, the report recommended that 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.”²¹

Finally, the report recommended that “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.”²²

Response to the British Columbia Report

The government of British Columbia did not wait for the Information and Privacy Commissioner’s report to be published before taking action. In October 2004 the Legislative Assem-

¹⁷ Id. at 135 (Rec. 1(d)).

¹⁸ Id. (Recs. 1(b) and 1(g)).

¹⁹ Id. (Rec. 1(f)).

²⁰ Id. at 137-38 (Recs. 7, 8, 11).

²¹ Id. at 139 (Rec. 13) (emphasis added).

²² Id. at 140 (Rec. 16).

bly adopted Bill 73—the Freedom of Information and Protection of Privacy Amendment Act, 2004.²³

The new law anticipated many of the recommendations that were subsequently to appear in the Commissioner’s report. Specifically, the law requires each public body to ensure that “personal information in its custody or under its control is stored only in Canada and accessed only in Canada.”²⁴ The law provides only two exceptions. Personal information may be exported or accessed from outside of Canada with the consent of the data subject or “for the purpose of disclosure allowed under [FOIPPA].”²⁵ The disclosures allowed under FOIPPA include those required or authorized by other British Columbian or Canadian laws; required or authorized by “treaty, arrangement or agreement”; to government officials and bodies for specified uses; to satisfy a debt owed to or by the government; “for the purposes of licensing, registration, insurance, investigation or discipline of persons regulated inside or outside Canada by governing bodies of professions and occupations;” if “compelling circumstances exist that affect anyone’s health or safety”; and “to a law enforcement agency in a foreign country under an arrangement, a written agreement, a treaty or provincial or Canadian legislative authority.”²⁶ In addition, the law allows the “minister responsible for this Act” to “by order, allow disclosure outside Canada . . . in specific cases or specified circumstances, subject to any restrictions or conditions that the minister considers advisable.”²⁷

The law requires a public body or its service provider to notify “the minister responsible for this Act” if it receives “a foreign demand” for personal information, if it receives a request for disclosure that “it has reason to suspect” is for disclosure outside of Canada, or if it “has reason to suspect that unauthorized disclosure of personal information has occurred in response to a foreign demand for disclosure.”²⁸

Finally, the new law explicitly applies the provisions of FOIPPA restricting disclosure of personal information to service providers and their employees.²⁹

The Canadian government also did not wait for the British Columbia Commissioner’s report before issuing a directive to all federal departments last October to conduct a “comprehensive assessment of risks” to Canadians’ personal information provided to U.S. companies carrying out work under contract. The Canadian federal Treasury Board is also leading a working

²³ Bill 73—the Freedom of Information and Protection of Privacy Amendment Act, 2004.

²⁴ Id. § 30.1.

²⁵ Id.

²⁶ Id. §§ 33.1(1)-(2).

²⁷ Id. § 33.1(3).

²⁸ Id. § 30.2(2).

²⁹ Id. § 30.4.

group developing contract clauses to be used in future government requests for proposals and outsourcing contracts.³⁰

Federal Privacy Commissioner Jennifer Stoddart has indicated that she shares the concerns voiced in the British Columbia report.³¹ To date, she has not sought to amend Canadian federal law to follow the British Columbia approach. However, already, as discussed in greater detail below, multinational companies with offices in the United States are reporting stringent new terms being added to Canadian and provincial government outsourcing contracts forbidding personal data from being transferred to, or accessed from, the United States.

There are signs that other countries outside of Canada are concerned as well. South Australia has begun an examination of the potential impact of the USA Patriot Act on outsourcing arrangements involving the personal information of that state's residents.

European Union officials have long expressed concern over U.S. government access to Europeans' data, most recently in the context of U.S. requirements that airlines provide information on all passengers on flights to the United States in advance of their arrival. The **European Court of Justice** is currently reviewing a 2004 case brought by the European Union **Parliament** claiming that the transfer of European passenger records to the United States violates EU law.³² The British Columbia report has prompted European government officials to promise renewed attention to potential access by the U.S. government to data about Europeans.

The Report's Flaws

The British Columbia report, however well-intentioned, is seriously flawed, and has contributed to misfocusing the growing debate over privacy issues in multinational information flows. Ten issues are of particular concern:

1. The report ignores the near impossibility of the USA Patriot Act being used to obtain outsourced information about Canadians

In his report, Commissioner Loukidellis concludes that "there are no assurances that the FIS Court [the U.S. Foreign Intelligence Surveillance Court] will not grant orders compelling

³⁰ Appearance of the President of the Treasury Board before the Special Senate Committee on the Anti-terrorism Act (May 30, 2005).

³¹ Office of the Privacy Commissioner of Canada, Privacy Commissioner of Canada Commends BC Information and Privacy Commissioner for Furthering Public Debate on Sharing of Personal Information about Canadians across Borders (Oct. 29, 2004).

³² Martial Tardy, "Euro Parliament Attempts New Legal Action Against PNR Deal," *Aviation Daily*, June 18, 2004, at 3.

US-linked companies to disclose personal information records located in Canada.”³³ He continues: “The existence of that reasonable possibility warrants other mitigating steps being taken.”³⁴

This conclusion is surprising for a number of reasons. First, it transforms “no assurances” into a “reasonable possibility” without explanation or comment.

Second, it is contrary to the submissions to the Commissioner from the Attorney General of British Columbia and from other legal authorities, all of whom opined that there was little if any possibility of the Foreign Intelligence Surveillance Court issuing such an order. Attorney General Geoff Plant characterized the “risk of access to Canadian information under the Patriot Act” as “minimal.”³⁵ Martin Kratz, head of the Technology Law Practice Group of the Canadian law firm of Bennett Jones LLP, provided an opinion letter describing such access as “highly unlikely.”³⁶ Stewart Baker, former general counsel of the National Security Agency, a partner in the U.S. law firm of Steptoe & Johnson, LLP, and, as of July 14, 2005, President Bush’s nominee as assistant secretary for policy of the Department of Homeland Security, concluded that U.S. law “effectively prevents U.S. authorities from obtaining the personal information of British Columbians without the consent of Canadian authorities or in violation of Canadian law and policy.”³⁷ The possibility of such access, Baker concluded, is “vanishingly small” and “utterly implausible.”³⁸

Third, the Commissioner’s conclusion ignores the evidence about the use of the USA Patriot Act. As of September 2003, not one section 215 order had been sought or issued in the almost two years since the Act had expanded the scope of those orders.³⁹ Since then, according to the April 27, 2005, testimony of the U.S. Attorney General, section 215 has been used only 35 times and never to obtain medical records.⁴⁰ It is simply not credible to believe, as the British Columbia Commissioner asserts, that the use of such a provision to obtain data from Canada is a “reasonable possibility.”

³³ Privacy and the USA Patriot Act, *supra* at 129.

³⁴ *Id.*

³⁵ The Hon. Geoff Plant, Attorney General of the Province of British Columbia, Submission to the Information and Privacy Commissioner for British Columbia ¶ 4.08 (2004).

³⁶ Ross Breckon, Vice President of EDS Canada Inc., EDS Canada Submission on the USA Patriot Act at 21 (2004) (letter from Martin Kratz, Bennett Jones LLP, to Ross Breckon, July 19, 2004).

³⁷ *Id.* at 24 (letter from Stewart A. Baker, Steptoe & Johnson, LLP, to Ross Breckon, July 19, 2004).

³⁸ *Id.* at 29, 35 (letter from Stewart A. Baker).

³⁹ Richard B. Schmitt, “Ashcroft Says Patriot Act’s Search Clause was Never Used,” *Los Angeles Times*, Sept. 19, 2003, at A30.

⁴⁰ *Hearing on the USA Patriot Act of 2001*, Senate Select Committee on Intelligence, U.S. Cong., Washington, DC, April 27, 2005 (testimony of Attorney General Alberto Gonzales).

Finally, the report discounts the impact of the Mutual Legal Assistance Treaty, which governs the transborder collection of information between Canada and the United States.⁴¹ The countries signed the treaty in 1985 largely in response to concerns about the use of U.S. subpoenas to obtain access to data in Canada. Under the treaty, as the British Columbia Attorney General informed the Commissioner, “U.S. authorities *must* first try to obtain records located in Canada through the assistance of Canadian authorities.”⁴² Article IV states that “[a] Party seeking to obtain documents, records or other articles known to be located in the territory of the other Party *shall* request assistance pursuant to the provisions of this Treaty,” except when the parties otherwise agree.⁴³ The United States understood and acknowledged this requirement in the Senate report that accompanied the treaty when it was ratified: “a Party needing documents, records, or articles located in the territory of the other and not available under any cooperative agreement or arrangement must use the treaty to obtain them.”⁴⁴ The use of the USA Patriot Act or any other provision of U.S. law to obtain records located in Canada without first seeking access through the treaty is prohibited.⁴⁵

2. The report ignores the exceptions in British Columbian privacy law

Even in the highly unlikely event that the U.S. government sought to use the USA Patriot Act to obtain access to personal information concerning British Columbia residents from U.S.-linked companies, it is not at all clear that this would violate British Columbian law. The Commissioner’s report’s conclusion to the contrary is unsupported by law.

The version of FOIPPA in effect at the time the report was written provided specific conditions under which the government could—in fact, might be required to—disclose personal information within its control. Those exemptions included “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 the information.”⁴⁶ The Commissioner’s report concludes that this exemption applies only to a *Canadian*—or perhaps even only to a *British Columbian*—“court, person or body,” but the exemption certainly does not say so, the report cites to no legislative history supporting this interpretation, and no decision by the British Columbia Information and Privacy

⁴¹ Mutual Legal Assistance Treaty Between United States and Canada, reprinted in S. Treaty Doc. 100-14, 100th Cong., 2d Sess. (1988).

⁴² The Hon. Geoff Plant, *supra* ¶ 2.07.

⁴³ Mutual Legal Assistance Treaty, *supra* art. iv.

⁴⁴ Senate Report, Treaty with Canada on Mutual Legal Assistance in Criminal Matters, reprinted in S. Treaty Doc. 100-14, 100th Cong., 2d Sess. (1988).

⁴⁵ The British Columbia report acknowledges the existence of the Treaty, but concludes that because it only applies to requests for assistance in relation to the investigation or prosecution of an “offence,” it would not apply to “intelligence gathering or surveillance where no investigation or prosecution of an ‘offence’ is involved.” *Privacy and the USA Patriot Act*, *supra* at 102. Under U.S. law, section 215 orders can only be issued as part of “an investigation to protect against international terrorism or clandestine intelligence activities,” both of which constitute offenses under U.S. and Canadian law. Pub. L. No. 107-56, § 215. It therefore seems unlikely that U.S. authorities would be able to invoke section 215 without also triggering the Mutual Legal Assistance Treaty.

⁴⁶ FOIPPA, *supra* § 33 (e).

Commissioner has ever described the provision in this restrictive light. The broad, inclusive language of the exemption, especially when viewed in the context of the other exemptions, is more logically read as applying to a “subpoena, warrant, or order” issued by *any* “court, person or body with jurisdiction to compel the production of the information.”

After the Commissioner’s report was written, British Columbia amended the FOIPPA to limit disclosure “to comply with a subpoena, warrant or order” only to those “issued or made by a court, person or body *in Canada* with jurisdiction to compel the production of information.”⁴⁷ This amendment suggests that the prior version of FOIPPA had not been limited to Canadian subpoenas, warrants, or orders.

The version of FOIPPA in effect while the Commissioner was writing also permitted disclosure “to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority.”⁴⁸ This would have permitted the United States to seek information through the Mutual Legal Assistance Treaty or other treaty or agreement, and might well be read as permitting access under the USA Patriot Act—a U.S. “legislative authority.” The British Columbia legislature lent credence to this interpretation when it subsequently amended the provision to restrict it “to a law enforcement agency in a foreign country under an arrangement, a written agreement, a treaty or *provincial or Canadian* legislative authority,” and even then only by a “public body that is a law enforcement agency.”⁴⁹ At the same time, by anticipating the changes recommended by the report in the FOIPPA amendments, the British Columbia legislature heightened the movement towards provincial restrictions on global information flows.

3. The report ignores the concept of “reasonableness” enshrined in British Columbian and Canadian law

Privacy, even in British Columbia, is not protected absolutely. FOIPPA requires only that the government make “*reasonable* security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal” of personal information under its control.⁵⁰ In fact, the term “reasonable” appears 17 times in the law.

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

The importance of the right to privacy . . . cannot be minimized. Those fundamental rights are contained in the Charter for the benefit of all Canadians. However, those rights, as previously stated, are not absolute. There is a *reasonable* expectation of privacy and the language [of the Charter] emphasizes that in-

⁴⁷ Id. § 33.2(b) (emphasis added).

⁴⁸ Id. § 33 (o).

⁴⁹ Id. § 33.1(2) (emphasis added).

⁵⁰ Id. § 30 (emphasis added).

dividuals should be secure against *unreasonable* search and seizure. In the case at bar . . . [t]he *reasonable* expectations of privacy are satisfied by statute and by contract. . . . A *reasonable* expectation of privacy is protected.⁵¹

The British Columbia Information and Privacy Commissioner's report ignores this reasonableness requirement by seeking to impose obligations on the government to guard against *any* unauthorized access. As a result, in the Commissioner's view, even the slightest risk of the U.S. government seeking access to Canadian data through section 215 or other means appears to be too much. This creates an impossible barrier to reconciling national data protection regimes and an unworkable approach to privacy and therefore undermines both meaningful privacy protection and multinational information flows.

This also undervalues the important competing values that may conflict with information privacy. David Flaherty, the previous British Columbia Information and Privacy Commissioner and a leading scholar of privacy law, has stressed the need for balance in privacy protection in many of his writings, including a 1998 report on the British Columbia Cancer Agency: "[F]air information practices need to be consciously fashioned, by written policies, to the needs of public bodies and their clientele to deliver services effectively. Privacy protection is all about balancing competing interests."⁵²

4. The report focuses on privacy and downplays security

One of the vital competing interests that the report downplays is the security of Canada and the United States. This is surprising because it is impossible to balance privacy with competing interests, or to determine whether a potential incursion into privacy is justified, without knowing why the data are necessary.

Section 215, by its own terms, is limited to an investigation "to protect against international terrorism or clandestine intelligence activities."⁵³ On September 11, 2001, and in the days afterwards, the world learned something about the reality and magnitude of the threat of international terrorism. In the words of noted U.S. attorney and civil liberties advocate Floyd Abrams:

The threat of nuclear, biological, or chemical attacks within the United States by terrorists who are, at one and the same time, technologically skilled and suicidally oriented, may well pose the greatest threat to our people that we have ever faced before. The threat is not only real; it is long-term in nature, with no end in sight and, quite possibly, with no end at all. It may be the fate of our children and grandchildren always to be at risk.

⁵¹ BC Government & Service Employees' Union v. British Columbia (Minister of Health Services), 2005 B.C.S.C. 446 ¶¶ 68-70 (appeal pending) (emphasis added).

⁵² Information and Privacy Commissioner of British Columbia, The British Columbia Cancer Agency: The Results of a Privacy Check-Up (1998).

⁵³ Pub. L. No. 107-56, § 215.

Given the level of this threat, it is not only understandable but necessary that our government seek out new and creative ways to prevent acts of terrorism.⁵⁴

As post-September 11 amendments to Canadian laws have demonstrated, the Canadian government, like that of the United States, recognizes that some personal information will be necessary to protect against terrorist threats and secure critical infrastructures, such as the airways and national borders. Other nations have adopted similar laws to enhance national security. By focusing more on privacy than security, the report seriously undermines its conclusions about how the demand for privacy should be balanced against the need for the information.

Moreover, a more reasonable examination of the statutorily provided purpose for which section 215 may be used to access information might have led the Commissioner to recognize how unlikely it was that the U.S. government would invoke section 215 to obtain access to British Columbia's public health payment and administration records. As Stewart Baker wrote in his opinion letter: "it is hard to imagine a set of facts under which investigators could persuade the FIS Court [Foreign Intelligence Surveillance Court] that any British Columbian health records—let alone an entire database—are relevant to an investigation to protect against international terrorism or clandestine intelligence activities. The request would not withstand judicial review."⁵⁵

5. The report focuses on the USA Patriot Act, despite the reality that other longstanding legal provisions are far more likely to provide foreign government access to Canadian data

One of the ironies of the British Columbia report and the debate it has created is the focus on the USA Patriot Act, and especially section 215. While the Act is comparatively new and therefore perhaps more likely to be newsworthy, it is far less likely to be used as an effective tool to obtain access to Canadians' data than other provisions of U.S. and other nations' laws. In fact, while the most recent data available indicates that section 215—the focus of the British Columbia report—is rarely used to obtain access to anyone's data, other tools such as National Security Letters, administrative subpoenas, and grand jury subpoenas are routinely used to obtain personal information including data held in other countries. Moreover, like section 215 orders, these are usually issued and executed in secret, but unlike those orders, these do not all require the involvement of a court.

While the details of these other provisions are beyond the scope of this document, their existence and track record of use as means of obtaining data from abroad are critical for three reasons. First, they remind us that the issue at the heart of the British Columbia report is not new. It has been dealt with by Canada, the United States, and other nations for decades and, in fact, it was concern about how data were being accessed that led to adoption of the Mutual Legal Assistance Treaty in 1985—20 years ago.

⁵⁴ U.S. Department of Defense, Technology and Privacy Advisory Committee, *Safeguarding Privacy in the Fight Against Terrorism* 63 (2004) (separate statement of Floyd Abrams).

⁵⁵ EDS Canada Submission on the USA Patriot Act, *supra* at 28 (letter of Stewart A. Baker).

Second, not only are these issues not new, they are not limited to U.S. law either. Canada, too, like many other countries, has legal provisions for issuing subpoenas and other judicial orders to collect and disclose personal information, even across national borders. We have already seen the exceptions to FOIPPA for complying “with a subpoena, warrant or order” and to allow Canadian law enforcement agencies to disclose personal information to foreign law enforcement agencies “under an arrangement, a written agreement, a treaty or provincial or Canadian legislative authority.”⁵⁶ A neutral reading of the British Columbia report and law would affect most global businesses because of their inevitable links to one or more of the dozens of countries with laws permitting government access to personal data, under limited circumstances, for national security purposes.

Canada and the United States have for years sought personal information from each other’s territories, shared information across their borders, and negotiated when efforts to obtain that information conflicted with the values of either nation. Moreover, like the United States, Canada amended its federal laws post-September 11 to expand the power of the government to collect and disclose information regarding its citizens.⁵⁷ In fact, Michael Geist, Canada Research Chair in Internet and E-Commerce Law at the University of Ottawa Faculty of Law, noted in his submission to the British Columbia Commissioner that section 21 of the Canadian Security Intelligence Act is remarkably similar to section 215 of the USA Patriot Act. Both provide for warrants to be issued in secret by federal courts empowering law enforcement officials to seize tangible things.⁵⁸

Finally, the existence of these other tools reminds us that the issues surrounding transborder access to personal information are not likely to go away any time soon. Even if section 215 is not the threat the British Columbia report portrays it to be, the issues raised by the discussion of section 215 remain relevant and timely.

6. The report fails to define “US-linked” and “US-located” companies and then focuses exclusively on U.S. companies with Canadian subsidiaries

The British Columbia report focuses on a single group of service providers: “US-linked” or “US-located” companies, terms the report uses 40 times. Despite the obvious importance of these terms, they are never defined. A careful reading, however, shows that the report is focused only on U.S. companies doing business in Canada or with Canadian subsidiaries, as if only such companies present the USA Patriot Act issues that the report fears. For example, every time the report refers to parent-subsidiary relationships the parent is a U.S. company and the subsidiary is Canadian. The implication is that U.S. companies and their Canadian subsidiaries are uniquely vulnerable to the USA Patriot Act. For example, the report notes that “[a]s long as the court has jurisdiction over a US corporation that controls records located abroad, the court can order dis-

⁵⁶ FOIPPA, supra §§ 33.2(b), 33.1(2).

⁵⁷ See, e.g., An Act to amend certain Acts of Canada, and to enact measures for implementing the Biological and Toxic Weapons Convention, in order to enhance public safety, SC 2004, C.15.

⁵⁸ Michael Geist & Milana Homsy, *The Long Arm of the USA Patriot Act: A Threat to Canadian Privacy?* 24 (2004).

closure.”⁵⁹ But exactly the same thing can be said of a Canadian corporation: as long as a U.S. court has jurisdiction, it can order disclosure even of records located abroad.

The threat that the USA Patriot Act presents to data about Canadians, slight though it is, is shared equally by any entity—Canadian or U.S.—with ties to the United States. Those ties could be a U.S. office, a U.S. parent, a U.S. subsidiary, a U.S. consultant, or a U.S. service provider. The Attorney General of British Columbia, for example, noted that whatever risks exist under the USA Patriot Act, they exist equally for “Canadian companies with U.S. connections,” “Canadian airlines,” “Canadian or British Columbian unions that have connections with U.S. unions,” Canadian retail companies with U.S. connections,” and “Canadian internet service providers with U.S. connections.”⁶⁰

Similarly, Professor Geist wrote:

Moreover, the application of these laws is not limited to U.S. companies but actually applies to any company with sufficient U.S. connections such that it could find itself subject to the jurisdiction of the U.S. courts. This is true both for U.S. companies operating subsidiaries in foreign countries as well as for foreign companies with U.S. subsidiaries.⁶¹

The restrictions, then, that the report would impose on U.S. companies and their Canadian subsidiaries, to be effective, would need to apply equally to all Canadian companies with U.S. connections, whatever their form. Multiplied across the global context, those restrictions would have to apply to virtually all non-Canadian companies with Canadian operations and Canadian companies with non-Canadian operations—an extraordinary impediment to global information flows and trade in information services, as discussed in greater detail below.

7. The report substitutes sovereignty for privacy

Although the British Columbia Information and Privacy Commissioner’s report is ostensibly about privacy, it appears to be equally concerned with sovereignty. For example, the report notes 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.”⁶² The report also concludes that “[u]sing the long arm of the USA Patriot Act to extend American legislation and American principles onto foreign soil offends our basic understanding of sovereignty.”⁶³

⁵⁹ Privacy and the USA Patriot Act, *supra* at 119.

⁶⁰ The Hon. Geoff Plant, *supra* ¶ 9.02.

⁶¹ Geist & Homsy, *supra* at 34.

⁶² Privacy and the USA Patriot Act, *supra* at 82.

⁶³ *Id.* at 88 (quoting Submission of Public Services International 2 (July 14, 2004)).

Sovereignty is, of course, very important, but its prominence in the report is noteworthy given that the report is ostensibly about privacy and emanates from an independent government office concerned with privacy and access to information. That lack of experience with issues involving sovereignty may help explain the nationalist way in which the term is used in the report.

The report notes in passing that Canada has adopted provisions similar to those contained in the USA Patriot Act and that both Canadian and British Columbian laws expressly permit collecting data for national security and law enforcement purposes, but it draws the line at the U.S. government engaging in similar activities. Moreover, the report presumes that U.S. government officials would not seek information in a straightforward manner from their Canadian counterparts and pursuant to the Mutual Legal Assistance Treaty, even though the only examples of failing to follow privacy law to which the report cites are Canadian. The report refers repeatedly to the “rule of law” and its paramount importance in a democratic society, but then intimates that it only works in Canada. In fact, the report goes so far as to make recommendations that could cause U.S. companies with Canadian connections to violate the “rule of law” in the United States.⁶⁴

Faced with the similarities between the national security threats, the legitimate need for information, and the importance of the rule of law in Canada, the United States, and other nations, the report might very well have concluded that sovereign nations must find a principled way of accommodating their mutual needs when they affect the transborder flow of information. Instead, the report opted for protecting the rule of law and sovereignty in Canada without regard for the impact elsewhere.

8. The report recommends a provincial solution to a global issue

Faced with a fundamentally global problem about the inevitable conflict between national legal systems when applied to global information flows, the British Columbia report takes a surprising turn by focusing on a provincial approach. This might be explained partially by the fact that the British Columbia Information and Privacy Commissioner is an independent office of a provincial government, but, at least as a near-term step, the report actually seems to advocate a local approach to national and global issues.

In discussing the scope of exemption 33(e) under the FOIPPA, permitting disclosures of personal information “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 the information,” the report concludes that “with jurisdiction” would include only subpoenas, warrants, or orders issued “in British Columbia or *possibly* elsewhere in Canada,” but in no event “under the authority of a provincial law of another province.”⁶⁵ This doubt as to whether British Columbia would recognize subpoenas, warrants, or orders issued by Canadian federal courts, combined with a firm resistance to recognizing such documents issued by other provincial courts, is striking.

⁶⁴ Id. at 135 (Rec. 1(d)).

⁶⁵ Id. at 107 (emphasis added).

In the face of the report's conclusion that the law of no Canadian province other than British Columbia could ever be sufficient to "authorize" disclosure under section 30 or 33, and that only "possibly" might federal Canadian law suffice, it is clear that U.S. law and the laws of other sovereign nations never had a chance. In short, the report articulates a view of British Columbia, at least for privacy purposes, as a legal island, separated not only from other countries but from other provinces as well. This stands in stark contrast to the growing reliance over the past two decades on supra-national regional political institutions, such as the European Union, the North American Free Trade Area, and the Asia-Pacific Economic Cooperation.

9. The report highlights vital issues, but fails to address them meaningfully

The British Columbia Information and Privacy Commissioner's report on privacy and the USA Patriot Act highlights two important sets of issues. The first concerns how to balance privacy with security. This is a question that all developed countries are facing and will undoubtedly continue to face for the foreseeable future. The second set of issues concerns how to deal with divergent national legal systems that increasingly come into conflict as data move across national borders. This is by no means a new concern, but global information technologies, like the World Wide Web, and the multinational commerce, outsourcing, and information sharing they have made possible are causing new and frequent conflicts between divergent approaches to privacy and information management.

The British Columbia report focuses new attention on both sets of issues, but then adopts a nationalistic (even provincial), authoritarian solution that asserts the primacy of the law of one province over that of all other nations. This approach may work, at least temporarily, for Canada or British Columbia, but it is no solution. The report recommends, and the British Columbia legislature contemporaneously adopted, requirements that prevent transmitting or even accessing personal data held by the public sector from outside of Canada. As a practical matter, only businesses incorporated in British Columbia can even bid on outsourcing contracts involving personal data.

In the case of the British Columbia health benefits administration contract, the government ultimately granted the contract to Maximus BC Health Benefit Operations Inc., a wholly owned subsidiary of Maximus BC Health, which in turn is owned by Maximus Canada Inc., which is owned by Maximus Inc., a U.S. company. Even these four levels of separation were not sufficient for the British Columbia government, which required that the stock of Maximus BC Health be placed in a trust, with instructions that the shares are handed over to the government if Maximus BC Health fails to abide by the terms of the service contract. In addition, Maximus agreed to pay a stipulated \$35 million penalty if it breached the confidentiality provisions in the contract.⁶⁶

This is simply not a workable approach for the information age. It denies the efficiencies and economies of scale that global information networks make possible. By adopting this ap-

⁶⁶ BCGSEU v. British Columbia, *supra*.

proach, the report misses a valuable opportunity to have advanced our thinking about vexing but critical issues, rather than merely our awareness of them.

10. The report's recommendations pose real threats to individuals and businesses in Canada and elsewhere

The ability to move information across borders offers real benefits to individuals and real opportunities to businesses. Customer service can be provided around the clock without employees having to work through the night and without companies having to pay overtime. Efficiencies and specialization that global information networks support expand the range of products and services available to consumers and reduce the prices consumers pay for them. The ability to access data from abroad decreases the need for redundant sales and service forces, further reducing costs. It increases the mobility of labor and facilitates travel and commerce across borders.

The British Columbia report and legislation are already having significant effects on individuals and businesses in both public and private sectors in Canada and elsewhere.⁶⁷ For example, the requirement that personal data not be transferred out of British Columbia eliminates the ability of businesses to provide centralized data storage, back-up, or processing. One of the world's largest issuers of affinity credit cards has been told that it can no longer service cards provided to support public sector institutions in British Columbia, such as public universities, from anywhere other than British Columbia. This not only eliminates important efficiencies and drives up the cost of providing services, it will likely eliminate some services and competition from some service providers altogether because of the economic impossibility of creating data centers just for British Columbia.

The inability to move public sector data outside of the province also greatly restricts the ability of service providers to match those data with information from other sources in an effort to identify fraud, protect national security, trace missing persons, enhance the accuracy of records, or provide more personalized service. Such matching will only be possible with data that can be moved to British Columbia, which may be impossible for economic reasons or legal prohibitions as other provinces, states, and nations adopt similarly restrictive laws.

Video conferencing, Internet-based meeting services, even the routing of telephone and Internet traffic (which often is done through the United States to take advantage of lower tariff rates) will be restricted at least in the public sector if they involve sending personal information outside of the province.

The requirement that personal data from British Columbia's public sector not even be accessible outside of the province exacerbates these concerns and adds new ones. For example, non-British Columbia call centers that provide service, instruction, or other support are impossible if they involve personal data. As a result, the increasingly common practice of providing

⁶⁷ The examples in this section are extracted from confidential information provided to the author by member companies of the Center for Information Policy Leadership that operate in Canada.

benefits information and options on a 24x7x365 basis using foreign call centers and Internet service providers is prohibited because these require that the foreign operations have access to personal data.

The absolute prohibitions recommended in the British Columbia report and contained in the amended law restrict even incidental links to provincial data from outside the country. For example, manufacturers of medical imaging and other diagnostic equipment have been informed that they can no longer provide remote service because such service inevitably involves the technician temporarily accessing patient information. As a result, the prices for equipment provided to British Columbia hospitals, which operate in the public sector, are anticipated to rise 10-15 percent just to cover the additional costs of servicing it. Moreover, suppliers are warning of substantial delays to allow time for senior technicians to be flown into British Columbia since they cannot consult about maintenance issues from outside of the province. Patient care and convenience are certain to suffer, all to protect against the USA Patriot Act being used to access patient data that might be stored in a malfunctioning piece of equipment. The same will be true of warranty service, computer support, and similar services that cannot be provided remotely because of the likelihood that personal information might be disclosed during the transaction.

The British Columbia report and legislation pose special challenges for multinational organizations, which can no longer take advantage of the efficiencies of their size and structure to provide centralized computer support, payroll processing, hiring and promotion evaluation, risk management, or even internal audit if personal information from the public sector would be involved.

In addition to the restrictions on transferring data or accessing it from outside of British Columbia, the report and legislation include other requirements that are being implemented and often amplified in practice. For example, non-British Columbian companies are being required to create separate British Columbian subsidiaries and then to take extraordinary steps to separate those entities from Canadian or U.S. parent companies. This is an expensive and burdensome process that can result in enormous inefficiencies as well as significant risk to the parent company because of its inability to oversee its subsidiaries effectively.

The requirement that service providers notify the provincial government if any non-British Columbia government agency seeks access to data creates a real dilemma for affected businesses. For example, a Canadian company that receives a subpoena under either Canadian or U.S. law is likely to be prohibited by the terms of subpoena from disclosing its existence to anyone other than its counsel. However, if that subpoena concerns personal information that has been obtained from, or is being processed for, a British Columbia government agency, provincial law requires that the company disclose the existence of the subpoena or face stiff civil and even criminal penalties for failing to do so. Neither the Information and Privacy Commissioner's report nor the British Columbia law permits any exceptions, even for compliance with other legal obligations.

Increasingly multinational businesses are finding that service contracts and outsourcing agreements with British Columbia government agencies are including harsh stipulated penalties for disclosing information in violation of the contract, even if the violation was inadvertent, re-

sulted in no tangible harm, or was compelled by a higher law. Provisions for stipulated penalties such as the \$35 million that Maximus faces will inevitably cause some companies to stop doing business with the province and may well result in subjecting those that do continue to work in British Columbia to unconscionable punishment. Moreover, such penalty provisions threaten to distort the market if they are required only of entities owned by companies outside of British Columbia.

British Columbia public agencies are also including in service contracts provisions prohibiting the involvement of U.S. employees of service providers or condition their involvement on prior agency permission. This wreaks havoc on a business' ability to manage its work force and deliver the best service at the lowest cost possible. It can interfere with union contracts and succession planning, and it denies British Columbian residents and government the benefit of access to the best talent available.

These and other risks are not just conjecture. Already we are seeing the impact of the British Columbia Information and Privacy Commissioner's report and the related legislation reflected in onerous contract terms and the exclusion of U.S. and other non-British Columbian enterprises from the opportunity to bid on government contracts. As serious as these restrictions are, the greater risk is that they spread.

The Future Threat

The British Columbia report and law are only a start. They and other developments and concerns are causing ripples throughout Canada and in other countries. As we have seen, the Canadian federal government has issued a directive to all federal departments to conduct a "comprehensive assessment of risks" to Canadians' personal information provided to U.S. companies carrying out work under contract. The Canadian federal Treasury Board is also leading a working group developing contract clauses to be used in future government requests for proposals and outsourcing contracts. And other Canadian provinces are watching the experience with the British Columbia law to see whether they should adopt similar restrictions. In the meantime, individual federal and provincial government agencies are adding stringent new terms to outsourcing contracts with multinational companies with offices in the United States, forbidding personal data from being transferred to, or accessed from, the United States.

The risk that British Columbia-style laws will spread throughout Canada was heightened by a March 2005 survey showing that 92 percent of Canadians surveyed have moderate or high concern that Canadian government agencies will outsource processing of personal data to companies in the United States.⁶⁸ Ninety-two percent believe that they should receive notice of such transfers, and 94 percent consider it of moderate or high importance that such transfers be conditioned on individual consent.⁶⁹

⁶⁸ EKOS Research Associates, *Canadians, Privacy, and Emerging Issues 12* (2005).

⁶⁹ *Id.* at 13-14.

The survey also provides a useful insight into the political environment in Canada and elsewhere surrounding transborder data flows. The Privacy Commissioner of Canada, Jennifer Stoddart, who commissioned the survey, issued a press release entitled: “Majority of Canadians demand informed consent on cross-border sharing of their personal information.”⁷⁰ The Commissioner neglected to note, however, that 90 percent of Canadians surveyed have moderate or high concern about Canadian government agencies outsourcing processing of personal data to companies *in Canada*; 94 percent want notice of such transfers; and the survey failed to ask whether Canadians thought such transfers should be conditioned on consent.⁷¹ Commissioner Stoddart issued a statement saying that the survey showed “[t]here is a growing lack of confidence by Canadians in the protection of their personal information being transferred across borders” and calling on the government to “protect Canadians’ personal data in any outsourcing or contract arrangements with foreign governments or companies.”⁷² Her statement reflected only half of the story, however, because what the survey showed was that Canadians are equally concerned about outsourcing of personal data in Canada, a fact overlooked in both the Commissioner’s publicity efforts and the resulting press coverage of the survey.

The risk is not only that unilateral restrictions spread throughout Canada, but that they are adopted by other countries and provinces either to emulate the British Columbia law or to retaliate against it. South Australia has begun an examination of the potential impact of the USA Patriot Act on outsourcing arrangements there. European Union officials, who have long expressed concern over data flows to other countries in general and U.S. government access to European data in particular, are watching developments in British Columbia with great interest.

Restrictions on public-sector data flows may be just the beginning. If British Columbia-style restrictions are portrayed as necessary to protect individuals’ data held by the public sector from access by the U.S. government during processing, wouldn’t similar restrictions be necessary to protect data held by the private sector? After all, unlike in the United States, data protection laws in Canada, Europe, and much of the rest of the world apply equally to public and private sectors. There is no bright dividing line.

The British Columbia Information and Privacy Commissioner’s report explicitly recommends that 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.”⁷³ The restrictions on transferring or accessing personal data from abroad recommended by the Commissioner and enacted by the provincial legislature could spread from the public sector to the private sector.

⁷⁰ Office of the Privacy Commissioner of Canada, *Majority of Canadians Demand Informed Consent on Cross-border Sharing of Their Personal Information* (June 20, 2005).

⁷¹ *Canadians, Privacy, and Emerging Issues*, *supra* at 12-13.

⁷² *Majority of Canadians*, *supra* at 1.

⁷³ *Privacy and the USA Patriot Act*, *supra* at 139 (Rec. 13) (emphasis added).

Finally, it seems inevitable that if the British Columbian unilateral approach to transborder data flows becomes more widespread, other provinces and nations will feel compelled to adopt similar or other data flow restrictions to protect local industry and ensure a level playing field. Restrictions on transferring information to, or allowing it to be accessed from, other countries and special conditions on service providers with connections to other countries constitute barriers to trade and are likely to provoke retaliatory responses.

This is the real risk: that the threat to multinational data flows posed by the British Columbia report and law spread across Canada, across sectors, and ultimately across the globe. The harm to individuals and institutions of the British Columbia approach to data protection is already clear. If magnified across provinces and nations, and applied to private- as well as public-sector data processing, the impact could be extraordinary. It will be measured not only in terms of economics and convenience, but jobs, health, and security. Such a serious, multinational issue requires a serious, multinational response, not the unilateral, provincial legislation adopted by British Columbia.

The critical issues highlighted by Commissioner Loukidellis' report and the British Columbia law, and especially the question about how to deal with divergent national legal systems that increasingly come into conflict as data move across national borders, warrant serious, thoughtful consideration. While the concerns are not new, powerful information technologies, global networks, and the multinational commerce, outsourcing, and information sharing they have made possible are inevitably going to cause new and more frequent conflicts between divergent national (and provincial) approaches to privacy and information management. Those same technologies and activities, our growing reliance on them, and the important values they implicate—including privacy and security—also heighten the urgency of finding multinational, diplomatic solutions that protect global information flows.