“O, PRIVACY”
CANADA’S IMPORTANCE IN THE DEVELOPMENT OF THE INTERNATIONAL DATA PRIVACY REGIME

JENNIFER MCCLENNAN* & VADIM SCHICK**

INTRODUCTION

As e-commerce and international outsourcing rapidly expands, the governments of the leading Western industrial nations are making every effort to balance protection of their citizens’ personal information with governmental interests in national security and promotion of commercial competitiveness. A continuously developing body of international law—to which we refer as the International Data Privacy (IDP) regime—attempts to reconcile the rights and conduct of the three major actors in this regime: governments, businesses, and individuals whose information is gathered, stored or traded. Famously, Europe and the United States have drastically different notions of what constitutes the proper balance of rights and responsibilities of the three actors, and approaches to achieving that balance. On the one hand, European governments are focused on protecting their citizens’ privacy and ensuring that those individuals have enough faith in the safety of the international system to freely engage in commerce, especially e-commerce. On the other hand, national security concerns in the United States, particularly after September 11, 2001, push the limits of civil rights such as privacy in order to satisfy the State’s duty to protect its citizens. Canada has traditionally taken a middle-of-the-road approach to this cross-Atlantic divide. However, since the enactment of the EU Data Privacy Directive of 1995 (“EU Directive”), Canada has been moving closer toward the European model of the IDP regime, and will

* Jennifer McClennan is a partner in Pillsbury Winthrop Shaw Pittman’s Global Sourcing practice. Ms. McClennan has more than 13 years experience in structuring and negotiating information technology and business process outsourcing agreements and technology transactions. Ms. McClennan graduated from Notre Dame Law School and the University of Virginia School of Engineering and Applied Science. Ms. McClennan serves on the board of the Ballston Science and Technology Center and is active in Leadership Washington.

** Vadim Schick is an associate in Pillsbury Winthrop Shaw Pittman’s Global Sourcing group, focusing on technology transactions and outsourcing on behalf of large corporate clients, particularly in the financial services industry. Mr. Schick also advises a group of retail companies with regard to its privacy policies. Mr. Schick is a graduate of the University of California, Berkeley, School of Law (Boalt Hall) and The Johns Hopkins University, where he served on the Board of Trustees from 2001 through 2005. © 2007, Jennifer McClennan and Vadim Schick.
likely continue to make its data protection laws increasingly restrictive.¹

No single document was as instrumental to the development of the IDP regime as the EU Directive. The Directive tied together the rights and responsibilities of the three major actors in a way that was most secure for the individual, and most burdensome for the corporation. Perhaps even more importantly, the EU Directive set out major requirements for the export of data from the European Union, effectively passing judgment on the status of data privacy protection outside the EU. The EU Directive pushed boundaries almost literally, causing numerous other nations to reconsider, or even consider for the first time, their positions and attitudes towards data privacy.

The United States has taken a more laissez-faire approach toward international data privacy protection law. Despite participating in shaping the original international framework for data protection in the 1970s, the United States now occupies the opposite end of the spectrum from its Western industrialized counterparts and is reluctant to play by the EU’s rules. The United States has developed what has been widely referred to as a “sectoral” regime,² enacting legislation that affects only specific industries, such as healthcare or financial services. The U.S. government otherwise participates in the IDP regime tangentially, such as by negotiating Safe Harbor provisions for U.S. companies to do business abroad.³ Nonetheless, U.S. companies doing business in Europe have little choice but to assent to the EU Directive’s requirements. They can comply by either enrolling in the Safe Harbor program (subject to eligibility requirements discussed in Part II, infra) or by adopting other self-regulatory mechanisms, such as standard clauses or binding corporate rules.⁴


⁴. After the EU Directive was enacted in 1998, the U.S. Department of Commerce and the EU Commission negotiated a set of data privacy protection principles, commonly referred to as the Safe Harbor. See Export.gov, Safe Harbor Overview, http://www.export.gov/safeharbor/SH_Overview.asp (last visited May 7, 2007). Safe Harbor is a voluntary regime, but the organizations that choose to sign up and comply with its requirements (which roughly correspond to the OECD principles of data protection described in Section I, infra), are deemed “adequate” by the EU data privacy authorities, and may import personal information from the EU to the U.S. without prior approval of data subjects. See id. Standard clauses and binding corporate rules are
Development of Canadian privacy law has been largely influenced by two radically different approaches within the IDP regime—the strict, protectionist EU approach, and the targeted, sectoral U.S. approach. The EU Directive doubtlessly had a major transformational impact on the development of data privacy law in Canada. Data privacy legislation existed in Canada before 2000, in the form of the Privacy Act, enacted in 1985, which regulated public entities’ treatment of personal information.\(^5\) Several Canadian provinces—led by Quebec, after 1994—enacted their own data privacy legislation, increasing or creating protections for individuals. None of these measures, however, were enough for the European Union to deem Canada a “safe” country for export of the Europeans’ data. That attitude changed after Canada passed the Personal Information Protection and Electronic Documents Act (PIPEDA) in 2000 and gradually implemented it by 2004.\(^6\) PIPEDA offered a national standard for protection of individuals’ data across virtually all private industries, not just in a few individual sectors. The new law also showed the federal government’s commitment to securing Canadian citizens’ personal information. As of 2002, the European Union has deemed Canada a “safe” country for transfer of data. Canada has thus effectively joined the European mold of the IDP regime despite remaining more sympathetic than the European Union, so far, to American national security and business interests.

On the business front, the EU approach is prevailing: corporate America has accepted, albeit reluctantly, the high costs of compliance with the various international IDP rules. This is particularly true in the outsourcing industry, where much attention has been given to the location—and, therefore, safety—of personal information, and where statutorily-sanctioned data privacy provisions have become a significant part of outsourcing agreements.

---

The story is different, however, when it comes to issues of national security, which pose a serious questions as to the future direction of the IDP regime. The United States has been able to force the Europeans’ hand on at least two occasions. First, U.S. national security interests trumped the European data privacy concerns when the U.S. Department of Homeland Security (DHS) required European airlines to transfer passenger information for all travelers entering the United States. The Passenger Name Records (PNR) controversy resulted in a negotiated agreement between the European Commission and DHS, which, ultimately, was favorable to the United States’ position. Second, the United States also prevailed in getting protected information regarding financial transactions from the Society for Worldwide Interbank Financial Transactions (SWIFT), the Belgium-based nonprofit banking clearinghouse, causing an uproar among the European data privacy watchdogs. The EU Commission and the U.S. Department of the Treasury are now seeking a political solution that would satisfy U.S. national security needs while alleviating European data privacy concerns.

Canada may become the bellwether of the IDP regime’s development as the nation either becomes progressively stricter or stalls under pressure from the United States. Canadians are generally uneasy about infringement of their privacy rights in order to protect national security interests. The Canadian government, and its Privacy Commissioner in particular, are keenly aware of and deeply concerned with maintaining a balance between national security interests and the likely subsequent infringements on individuals’ privacy rights, or as one privacy official put it, “secur[ing] democracy . . . without destroying democracy in the pro-

---


8. Glenn R. Simpson, U.S., EU Seek to Ease Banking-Privacy Concerns, WALL ST. J., Nov. 21, 2006, at A6. The SWIFT controversy centered around the U.S. government’s attempts to obtain information from private European businesses. European governments are not bound by the same rules, and have fewer restrictions that would prevent them from turning such information to the U.S. government, especially if such information is transferred for national security reasons. See STEWART ROOM, DATA PROTECTION COMPLIANCE IN CONTEXT 160-61 (BCS Pub’g 2002); see also Francesca Bignami, Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network, 26 MICH. J. INT’L L. 807, 819 (2005) (“extensive exceptions [to the EU Directive’s requirements] are carved out for government use of personal information in areas such as national security, domestic policing, foreign affairs, and defense.”).


10. For brief description of the Office of the Privacy Commissioner, see Part II infra.
The Privacy Commissioner has repeatedly expressed concern about the USA PATRIOT Act. She recently suggested that the Canadian government should consider tightening its requirements for export of its citizens’ personal information—particularly to the United States—perhaps along the lines of the EU Directive’s limitations on transferring personal information to countries without adequate data privacy protections.

U.S. and Canadian businesses, particularly those seeking outsourcing solutions in Canada requiring transfer of personal information outside Canada, will have to abide by the strict pro-privacy Canadian laws. Despite creating a few significant and durable national security exceptions to this regime, such as the Passenger Protect Program, Canada will likely follow Europe in adopting even stricter data privacy protection standards, including, possibly, an “adequacy” standard for export of personal information abroad.

Part I of this paper briefly surveys the data protection legislation in the United States, European Union and Canada, focusing specifically on each country’s definition of personal information and rules governing its transfer abroad. Part II examines the current state of data privacy law in Canada, including provincial laws of Quebec, British Columbia, and Alberta, and how Canadian data protection law has developed so far. Part III suggests a few necessary steps that U.S. companies doing business in Canada, or any company collecting, using or disclosing Canadians’ personal information, should take in regards to data privacy compliance. Particular attention is paid to outsourcing transactions originating in or affecting Canada. Finally, Part IV discusses the future development of Canadian privacy legislation and the progress of the IDP regime.

I. Global Overview

The groundwork for the IDP regime was laid in the 1970s, with the development and adoption of the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the Guidelines) promulgated by the Organization for Economic Cooperation and

---


13. See Shaw, supra note 2; Annual Report, supra note 11, at 19-20.
The United States participated in creation of the Guidelines, which were adopted in 1980. While not binding or mandatory, the Guidelines were nevertheless an important precursor to subsequent IDP legislation, including Canada’s PIPEDA, discussed in Section III, infra, because the OECD Guidelines included provisions regarding notice, consent, transfers, access, integrity, and safety of personal information.

In 1995, the EU Parliament passed the EU Directive, which set a minimum standard for EU member states’ comprehensive legislation on data privacy protection. Broadly, the EU Directive allows private companies to collect only a limited amount of protected personal data and only for a specific permitted purpose. Further, such companies are required to provide notice to data subjects regarding the purpose for which the information is being gathered, and also may be required to obtain consent from the data subjects in order to use or disclose the information to a third party. Finally, the EU Directive closely regulates transborder transfers of protected data, and allows for imposition of serious sanctions against violators.

The Directive proved to be a controversial measure even within the EU. Only a few member states complied with the 1998 implementation deadline. In fact, the EU Commission had to take France, Ireland, Germany, Luxembourg, and the Netherlands to the European Court of Justice in order to compel them to implement the acceptable privacy standards. Nevertheless, as of early 2007, most member states have complied or substantially complied with the EU Directive.

Canada has traditionally occupied the middle ground between the strict regulation in Europe and the laissez-faire approach in the United States. Like its neighbor to the south, Canada has enacted privacy legislation, beginning with the Privacy Act in 1985, directing its public entities to implement protections for the privacy of Canadians. In 2000, no doubt influenced by the EU Directive, Canadian Parliament
passed PIPEDA, which binds most private Canadian entities to stricter privacy protection for their data subjects. Canada also enacted legislation regarding health care and financial services related information. Like the United States, Canada places fewer restrictions on transborder flow of data than the European Union (particularly avoiding the European “adequacy” export standard). Unlike their European counterparts, Canadian airlines and transportation authorities have consistently and willingly relayed requested passenger information to the United States.20 On the other hand, Canadian citizens seem to be more concerned about protection of their privacy than their American neighbors. Privacy protection is a right guaranteed to Canadians under the Canadian Charter of Rights and Freedoms.21 Moreover, the Supreme Court of Canada deems individual privacy a fundamental right, the violation of which constitutes a tort.22 Canada also has a functioning—if overwhelmed—Privacy Commissioner, charged with the task of enforcing companies’ compliance with the law.

The United States has adopted a much less regulated approach to data privacy protection. In 1974, Congress passed the Privacy Act, regulating the federal government’s use and disclosure of personal information.23 The Privacy Act is the closest the United States came to comprehensive, omnibus privacy legislation. It requires, in part, that federal agencies: obtain the consent of data subjects before disclosure unless certain exemptions apply; track such disclosures; and allow subjects to access their data.24 Unlike the EU Directive, the Privacy Act does not apply to state or local public entities, and its enforcement mechanisms proved to be ineffective.25

Since the OECD Guidelines were passed in 1980, Congress has been reluctant to enact comprehensive legislation protecting all of an individual’s private information. Instead, federal authorities focused on a few industries and sectors. Most notable are health care, with the passing of

20. Tonda Maccharles, PM Backs Off Pledge to Beef Up Laws, TORONTO STAR, June 6, 2006, at A14 (“But when asked if there is any chance Canadian airlines would no longer give data to the Americans, [Transport Minister Lawrence Cannon] replied, ‘No.’”).
Health Insurance Portability and Accountability Act (HIPAA) in 1996, and financial institutions, with the enactment of the Graham-Leach-Bliley Act (GLB) of 1999.\textsuperscript{26} In 1996, Congress also passed the Telecommunications Act, which with very limited scope requires telecommunications carriers to protect consumer information, such as calling patterns, billing information, and home addresses of subscribers.\textsuperscript{27}

In many ways, Congress has been reactive, rather than proactive, in passing data privacy legislation.\textsuperscript{28} The Video Privacy Protection Act of 1988 was passed after reporters gained access to titles of videos rented by Supreme Court nominee Robert Bork, which led some critics to joke that in the United States “video rentals are afforded more federal protection than are medical records.”\textsuperscript{29} The murder of Hollywood actress Rebecca Shafter by a stalker who got her address from the California Department of Motor Vehicles led to the enactment of the U.S. Driver’s Privacy Protection Act of 1994.\textsuperscript{30} Consumer concerns over misuse of their phone numbers by telemarketers led to the Do-Not-Call Implementation Act of 2003, establishing the Do-Not-Call Registry administered by the Federal Trade Commission.\textsuperscript{31} Similarly, growing concerns from Internet Service Providers (ISPs) and consumers regarding e-mail spam resulted in the Controlling the Assault of Non-Solicited Pornography And Marketing Act (CAN SPAM) of 2003.\textsuperscript{32}

The ongoing “War on Terror” has produced another set of reactionary congressional legislation that significantly affects citizens’ privacy rights, most notably the USA PATRIOT Act of 2001.\textsuperscript{33} While the details of this and other anti-terrorism-related legislation are mostly outside of the scope of this article, it is important to note that these provisions affect the basic privacy rights of both American citizens and non-U.S. citizens whose data is stored in the United States. In this respect, the United States is moving in the opposite direction from Europe and Canada, the latter of which is considering ways to impose further restrictions on transferring data into the United States.

Unlike the European and Canadian approaches, the U.S. data privacy approach relies in great measure on self-regulation, largely

\textsuperscript{27} Nova, supra note 22, at 779.
\textsuperscript{28} Id.
\textsuperscript{29} Shaw, supra note 2, at 3; Nova, supra note 22, at 780.
\textsuperscript{30} Bignami, supra note 8, at 813.
based on company or industry-wide self-imposed or aspirational standards. After the EU Directive was passed and the European Union deemed U.S. data privacy protections inadequate, the U.S. Department of Commerce negotiated a set of “Safe Harbor” provisions, which bound participating U.S. companies to offer stricter privacy protections, while allowing them to transfer protected data of Europeans into the United States.\textsuperscript{34} The Federal Trade Commission (FTC) also pro-

\begin{table}

<table>
<thead>
<tr>
<th>Relevant Statutes</th>
<th>United States</th>
<th>Canada</th>
<th>European Union</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Relevant</strong></td>
<td>No overarching data privacy legislation or scheme</td>
<td>PIPEDA (2000) and “substantially similar” provincial laws</td>
<td>The EU Directive (1995) and member states’ laws</td>
</tr>
<tr>
<td><strong>Enforcing</strong></td>
<td>FTC is responsible for enforcement of businesses’ compliance with the Safe Harbor provisions and relevant privacy legislation.</td>
<td>Administered by the Privacy Commissioner (established in 2000); Office of the Superintendent of Financial Institutions (OSFI) supervises offshoring of data during outsourcing transactions for financial institutions.\textsuperscript{38}</td>
<td>Administered and enforced by the member states’ commissions and by the European Data Protection Supervisor on the Union level.</td>
</tr>
<tr>
<td><strong>Agencies</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Relevant State and Province Legislation</strong></td>
<td>Many States, including California and Georgia, adopted more stringent data privacy legislation</td>
<td>Alberta, British Columbia, and Quebec have their own data privacy legislation that was recognized to be substantially similar to PIPEDA. PIPEDA still applies in other provinces, and applies to all inter-provincial data transfers.</td>
<td>Each member state has adopted its own data privacy legislation, which must be in accord with the EU Directive.</td>
</tr>
</tbody>
</table>

\textsuperscript{34} See 56 Fed. Reg. 56,534 (Sept. 19, 2004).
\textsuperscript{35} See Safe Harbor Overview, supra note 4.
\textsuperscript{36} Fair Credit Reporting Act, 15 U.S.C. § 168 et seq.
\textsuperscript{37} Children’s Online Privacy Protection Act, 15 U.S.C. §§ 6501-06.
\textsuperscript{38} George Takach, Canada: Outsourcing and Offshoring: Myths, Realities, The Hurdles and How to Do It Right, MONDAQ BUS. BRIEFING, July 20, 2006, available at http://www.mondaq.com/
vides an enforcement mechanism for violations of the Safe Harbor regime. However, Safe Harbor has a very limited reach, because it only applies to EU-U.S. transfers and only to U.S. corporations under the jurisdiction of the Departments of Commerce and Transportation.\textsuperscript{35}

The EU Directive and Canada’s PIPEDA both adopt extraordinarily broad definitions of “personal information.”\textsuperscript{39} The EU Directive covers all information “relating to an identified or identifiable natural person.”\textsuperscript{40} Under Section 2(1) of PIPEDA, personal information means “information about an identifiable individual.”\textsuperscript{41} The similarity of these broad definitions of protected personal information is a main indicator of Canada’s adoption of an EU Directive-driven IDP regime. The United States, for its part, has no single definition for protected personal information, only definitions specific to individual statutory and self-regulatory regimes.\textsuperscript{42}

**Table 2:**
**Definition of Protected Personal Information in Canada and the European Union**

<table>
<thead>
<tr>
<th>European Union</th>
<th>Canada</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Personal data” shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.\textsuperscript{43}</td>
<td>“Personal information” means “information about an identifiable individual,” excluding “the name, title or business address or telephone number of an employee of an organization.”\textsuperscript{44}</td>
</tr>
<tr>
<td>NB: Business e-mail is not included in the Act, and is considered personal information.</td>
<td></td>
</tr>
</tbody>
</table>

Despite these broad definitions, it is important for businesses to consider what kinds of data these definitions encompass. Table 3 does not provide a complete list of protected data, but gives an impression of


\textsuperscript{39}. See EU Directive, supra note 1, art. 2(a); PIPEDA, 2000 S.C., ch. 5 § 2(1) (Can.).

\textsuperscript{40}. See EU Directive, supra note 1, art. 2(a); see also ROOM, supra note 8, at 36.

\textsuperscript{41}. PIPEDA, 2000 S.C., ch. 5 § 2(1) (Can.). Notably, this definition is different from Quebec’s privacy legislation, which will be discussed subsequently in Part II.

\textsuperscript{42}. See Nova, supra note 22, at 777-81.

\textsuperscript{43}. See EU Directive, supra note 1, art. 2(a).

\textsuperscript{44}. PIPEDA, 2000 S.C., ch. 5 § 2(1) (Can.).
just how far the various data protections laws of the European Union, Canada, and the United States can reach. 45

Unlike Canada and the United States, the EU places unique and severe restrictions on the export of personal information from the European Union by private actors. 46 Protected data may be transferred

46. Public actors are allowed much more leeway in using or disclosing personal information to a third party for diplomatic or national security reasons. See EU Directive, supra note 1, arts. 25-26; see, e.g., Bignami, supra note 8, at 807, 819.
outside of the European Union only to a country with “adequate” data privacy protections, meaning protections substantially similar to or greater than those offered by the EU Directive. In 2002, the EU Data Protection Working Party had deemed Canada “adequate” and lifted the previously imposed restrictions on European Union-Canadian transfers of data.\(^47\) To date, the U.S. companies must still either adopt Safe Harbor principles or use additional “contractual or other binding provisions,” such as the EU Directive’s Binding Corporate Rules in order to transfer EU citizens’ personal information into the United States (or another “inadequately” safe country).\(^48\)

The EU Directive allows for transfers of personal information to an entity in country that does not guarantee an adequate level of privacy protection and that has not assented to Safe Harbor or implemented binding corporate rules if: (1) the data subject unambiguously consents to the transfer; (2) transfer is necessary for the performance of a contract between the data subject and the business; (3) transfer is necessary for the entry and/or performance of a contract between the business and a third party for the data subject’s benefit; (4) transfer is justified on “important public interest grounds” or for purposes of a lawsuit; (5) transfer is necessary to protect the vital interests of the data subject; or (6) information is from a database to which the public has routine access because of national laws on access to documents.\(^49\) EU member states may create other exceptions to the transborder transfer restrictions, but they must notify the European Commission and other member states of any such exemptions.\(^50\)

Similar to EU law, Canadian law provides for a few exceptions to the laws governing the collection, use, and disclosure of protected personal information,\(^51\) which may—depending on contractual arrangements—apply to transfers of protected information abroad. For example, as in the European Union, Canadian law does not require consent for collection, use or disclosure of protected information: in case of emergencies threatening the individual’s life, health or safety; that is already publicly available; for purposes of law enforcement; and for other public policy reasons.

---

49. See Bignami, supra note 8, at 826; see also EU Directive, supra note 1, art. 7.
50. One example of an exception is allowing a transborder transfer if a contract between the corporation and the receiving party outside the EU—specifically, not a “safe” country for personal information—renders that party liable in tort for any loss or theft of the personal information. See Bignami, supra note 8, at 826.
51. Described in detail in Part II, infra.
Meanwhile, Canadian law is somewhat ambiguous about private firms’ transfer of protected information out of Canada. U.S. companies may be contractually compelled by their Canadian partners to provide the same level of protection to Canadians’ personal information as is required by Canadian law. However, once the information is exported or is stored in the United States, U.S. law applies and the policing and enforcement of data privacy compliance leave the jurisdiction of the Privacy Commissioner and, more broadly, the Canadian judiciary. Thus, PIPEDA’s extra-territorial reach is an open question. It remains unclear whether U.S. courts would apply foreign standards of data privacy protection against domestic defendants, or whether Canadian courts would be able to require companies located in the United States but doing business in Canada to comply with Canadian law.52

Regardless, both Canadian and European authorities take data subjects’ complaints and corporate compliance in general very seriously. “The EU nations have assessed millions of dollars in fines for noncompliance with the EU Data Protection Directive and applicable country privacy laws,” writes Rebecca Herold, “with a couple of the highest to date running at 840,000 Euros (approximately US$900,000) and 1.08 million Euros [(approximately US$1.16 million)] . . . [and many] of these actions have been related to moving data over country borders to a receiving country that is not considered as having adequate data protection requirements, such as the United States.”53 For example, in 2001 Spain alone imposed fines against 500 companies totaling over $13 million, and the EU member states plan to conduct joint audits of data protection in health insurance companies.54 In 2003, Canada completed 278 PIPEDA compliance investigations, and the number

<table>
<thead>
<tr>
<th>United States</th>
<th>Canada</th>
<th>European Union</th>
</tr>
</thead>
<tbody>
<tr>
<td>No federal statutory restrictions</td>
<td>PIPEDA’s impact unclear</td>
<td>The European Union approves only transfers to countries with “adequate” privacy protection regimes including, since 2002, Canada, but not the United States. Certain exceptions apply (see above)</td>
</tr>
<tr>
<td>PIPEDA requires contractual clauses ensuring that third parties outside of Canada will protect personal information. It is not clear, however, how it is or can be effectively enforced. Certain exceptions apply (see Part II, infra)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

52. See Spaeth et al., supra note 15, at 39.
53. Herold, supra note 45, at 1.
54. Id.
went up to 379 investigations in 2004.\textsuperscript{55} However, the Privacy Commissioner in Canada is significantly under-funded.\textsuperscript{56} If the Canadian Parliament gives the Privacy Commissioner greater funds, as requested in her 2005-06 Annual Report, the Commissioner will likely increase the number of audits and investigations.\textsuperscript{57}

II. Overview of Canadian Privacy Law

Canadian privacy law is a crucial subject for a U.S. business to consider. U.S. trade with Canada is greater than with any other country, “roughly equivalent to [U.S.] combined trade with China, Japan, Germany, and the United Kingdom.”\textsuperscript{58} Therefore, changes in the data privacy protocol north of the border will affect most large domestic companies with operations and other relationships in Canada. Any such developments will certainly have an impact on structuring outsourcing agreements regarding protected data exported out of, or imported into, Canada.

As mentioned above, at the time of passage of the EU Data Directive, Canada occupied the middle of the spectrum of data privacy protection, somewhere between the laissez-faire approach of the United States, and the strictly regulated European model. However, Canada has been gradually moving closer and closer to the European Union. With PIPEDA’s passage in 2000, and its full implementation in 2004, the European Union recognized Canada as providing “adequate” data privacy protection, which connotes protection at least equal to the one afforded by the EU Directive.

Prior to enactment of PIPEDA, Canadian law provided significant protection of its citizens’ personal information. Beginning in the 1970’s, Canadian courts recognized individuals’ control over their personal information as a “human right.”\textsuperscript{59} Federal and provincial common law in Ontario allowed Canadian citizens to assert their right to privacy by bringing a tort claim against violators, while New Brunswick, British Columbia, Manitoba, Newfoundland and Saskatchewan enacted legislation to allow such tort actions.\textsuperscript{60} The Privacy Act of 1985 provided a broad slate of protections for collection and use of personal information by the federal government and its agencies. After 1994, the

\textsuperscript{55} Id.
\textsuperscript{56} \textit{Annual Report}, supra note 11, at 5.
\textsuperscript{57} Id. at 6; see also Herold, supra note 45, at 1 (“privacy enforcement authorities have stated that they are just getting started and expect enforcement to increase markedly”).
\textsuperscript{58} Spaeth et al., supra note 15, at 29.
\textsuperscript{59} Id. at 31.
\textsuperscript{60} Id.
provinces, with Quebec leading the way, enacted their own data protection laws, aimed at either private or public entities, or both. Finally, the Canadian Standards Association ("CSA") Model Code for the Protection of Personal Information, which, while not mandatory, nevertheless provided necessary guidance to Canadian companies interested in self-regulation and seeking to comply with higher standards of data privacy protection. PIPEDA’s famous ten principles were based on the CSA Model Code.

The Privacy Commissioner of Canada oversees application and compliance with Canada’s two major privacy laws—the Privacy Act of 1985, which covers the public sector, including 160 federal government agencies and departments, and PIPEDA, which covers private businesses. The Privacy Commissioner is independent of the Prime Minister’s cabinet and reports directly to the Canadian House of Commons and the Senate. The Commissioner has the power to investigate complaints and conduct audits under the two federal laws, as well as publish reports about personal information handling practices in the public and private sector. The Privacy Commissioner is also empowered to conduct research into privacy issues so as to inform Parliament and the public, promote awareness and understanding of privacy issues by the public, and review and comment on the Privacy Impact Assessments (PIAs) completed by the federal government.

PIPEDA brought significant changes to how businesses use Canadians’ personal information. As mentioned in Part I above, PIPEDA’s definition of protected personal information is extremely broad. PIPEDA applies to entities using or disclosing such information during the course of a "commercial activity." Canadian law gives an equally broad scope to the definition of commercial activity, defining it as “any particular transaction, act or conduct that is of a commercial character, including selling, bartering or leasing of donor, membership or other fundraising lists.” For example, Centurion, a security company, installed four cameras to monitor incidents at an intersection in downtown Yellowknife, Northwest Territories, in 2001.

---


62. See infra Part III; see also *Canadian Standards Association Model Code for the Protection of Personal Information* Q830-96 (1996).

63. See Canada Privacy Act, R.S.C., ch. P 21 (1985); see also PIPEDA, 2000 S.C., ch. 5 § 4 (Can.).

64. Shaw, supra note 2.

65. PIPEDA, 2000 S.C., ch. 5 § 4 (Can.).


67. Racicot & Morgan, supra note 21, at 7.
was not making recordings but merely monitoring the events live, 24 hours a day, seven days a week. Centurion then reported incidents at the intersection to local police. Centurion supplied police the information without charge, in order to demonstrate its surveillance capabilities and thus generate business. The Information and Privacy Commissioner of Northwest Territories filed a complaint against Centurion for violating PIPEDA. The Privacy Commissioner agreed with the claimant, holding, in part, that Centurion did capture protected personal information and its actions represented “commercial activity” within the meaning of PIPEDA.68

The term “record” is similarly broad, including “any correspondence, memorandum, machine-readable record, or any other documentary material, regardless of physical form or characteristics, and any copy thereof.”69 Therefore, in order to comply with PIPEDA, businesses must “monitor all of their files, regardless of the form of storage which may contain personal information.”70 For example, in the Yellowknife case, Centurion’s actions violated PIPEDA because their cameras were capturing drivers’ personal information. Even though Centurion was not permanently recording surveillance on tapes, capturing their actions on camera was deemed to satisfy the “recording” language in the statute.71 PIPEDA also applies to information gathered prior to its enactment, and applies to non-Canadian businesses gathering information about Canadians.72 However, non-Canadian businesses’ obligations under PIPEDA are unclear once the information is transferred and then stored outside of Canada. American businesses gathering information are certainly affected by PIPEDA while collecting the information in Canada, or acquiring it from a Canadian partner, because PIPEDA’s secondary data transfer requirement forces Canadian businesses to include PIPEDA’s privacy requirements in all contracts contemplating transfer of Canadians’ personal information abroad.73

Specifically, PIPEDA requires compliance with ten data protection principles. Some of these “Ten Commandments” are mandatory obligations, and some are recommended practices that the legislature urges businesses to comply with. Critics fault PIPEDA because of the lack of clarity resulting from its intermittent use of “shall” and “should.”74

68. Id.
69. See PIPEDA, 2000 S.C., ch. 5 § 4 (Can.); see also Spaeth et al., supra note 15, at 33.
70. Spaeth et al., supra note 15, at 33.
71. Racicot & Morgan, supra note 21, at 8.
72. See PIPEDA, 2000 S.C., ch. 5 § 4 (Can.).
73. Id.
74. Keith, supra note 2, at 45 (referring to PIPEDA as a “Frankenstein’s monster.”).
Nevertheless, an outline of these ten principles is important to helping businesses understand what they should at least aspire to achieve. Part III provides a brief guideline for businesses seeking to comply with

| Ownership of information affects the applicable protections (some information belongs to the individual, some to the organization). | No such ownership distinction. The Privacy Commissioner specifically found that PIPEDA applies to information "about an individual," regardless of how it was generated. | No such ownership distinction. |
| GLB imposes notice requirements for disclosing "nonpublic" personal information. | No distinction between public and nonpublic information, with the exception of "business information." Exception for publicly available information, but must be used for the purpose such information was made public (car dealer may use the public list of attorneys to find a lawyer, but may not use that list to try to sell them cars). | Alberta and British Columbia have exceptions for certain public information (see PIPEDA). Quebec has no public information exception. Quebec defines protected personal information more narrowly than PIPEDA, protecting only information that relates to a natural person and allows that person to be identified. |
| Notice requirements (GLB requires annual notices). | No notice requirements. Consent has to be obtained (can be implied, negative/opt-out, or affirmative). | In Alberta and British Columbia, employers do not have to get consent from employees, but must notify them regarding purposes of disclosure or use of their personal information. In Quebec, an organization collecting information directly from individuals does not have to get consent, but when establishing a file must inform the individual regarding the (1) object of the file; (2) use that will be made of information; (3) categories of persons who will have access to the information; (4) location where it will be kept; and (5) individual’s rights of access and rectification. |
| GLB distinguishes between Affiliates and Nonaffiliates. | Limited use for the organization; parent and subsidiaries are treated as separate entities. | Alberta and British Columbia use PIPEDA’s narrow application. All allow outsourcing of data without consent. |

Table 5: U.S., Canadian (Federal and Provincial) Approaches to Data Privacy

---

75. See Shaw, supra note 2; PIPEDA, 2000 S.C., ch. 5 §§ 4.5.2, 4.9, 4.9.3 (Can.).
76. Notification of the “object of the file”—e.g., each piece of personal information in possession—under Quebec law is an important distinction from PIPEDA, which requires, more generally, that all purposes for all collected information be identified. See Racicot & Morgan, supra note 21, at 12.
Canadian privacy laws and follow the ten principles of PIPEDA. As mentioned above, Alberta, British Columbia, and Quebec have laws “substantially similar” to PIPEDA, which therefore apply to any organization doing business in those provinces. While the laws are, in fact, substantially similar to PIPEDA, Table 5 lists a few key differences between the approaches to data privacy protection under the federal and provincial law in Canada, focusing on certain requirements applicable to financial institutions under U.S. law.

PIPEDA does not have specific provisions regarding outsourcing. However, some critics have extrapolated an “agency concept” from its reference to “data processing” so that, for compliance purposes, outsourcing vendors are considered extensions of the businesses they serve.\(^78\) Quebec, Alberta and British Columbia, with varying specificity, have no provisions mandating obtainment of consent from data subjects for outsourcing.\(^79\) However, businesses remain accountable for whatever information it transfers to a service provider and even for the actions of the service provider itself. As one way of addressing this issue, Brian Keith—a legal practitioner in Canada who writes frequently on Canadian data privacy issues—advises businesses to put clauses in their outsourcing agreements protecting themselves from vicariously violating the applicable data privacy laws.\(^80\)

Additionally, Canadian privacy law provides for a few crucial exceptions to the general requirement of obtaining consent prior to collection, use, or disclosure of a data subject’s protected personal information. Businesses may collect, use and disclose an individual’s personal information if (1) such collection is in the individual’s best interest, and consent cannot be secured in a timely fashion, including in case of emergency threatening the individual’s life, health or security;\(^81\) (2) seeking consent would compromise the availability or accuracy of information sought for violations of agreements or laws (for example, in an insurance company’s investigation of a claimant’s allegations that involve collecting her personal information without her consent);\(^82\) (3) the collection is for journalistic, artistic, scholarly or literary purposes; or (4) the personal information sought is publicly available.

---

78. Keith, *supra* note 2, at 49.
79. *Id.* See also Racicot & Morgan, *supra* note 21, at 21; Cappone D’Angelo & Paul Varga, *Canada (Alberta)*, in 1 DATA PROTECTION LAWS, *supra* note 18, at 10; Cappone D’Angelo & Troy Lehman, *Canada (British Columbia)*, in 1 DATA PROTECTION LAWS, *supra* note 18, at 11.
81. PIPEDA, 2000 S.C., ch. 5 § 4.9 (Can.).
82. Racicot & Morgan, *supra* note 21, at 12.
Finally, businesses can use protected information without consent if the information will be used for law enforcement purposes. Businesses may disclose the information without obtaining consent of the data subject for disclosure to (1) counsel of the organization that collected the information, (2) to the government for security, defense, or law enforcement purposes; (3) to institutions that preserve historical records; (4) for purposes of debt collection; (5) pursuant to a court order or a law; or (6) in an emergency that demands disclosure (including breach of contract that is about to be, or has been, committed).

III. KEY CONSIDERATIONS FOR ORGANIZATIONS DOING BUSINESS IN CANADA

As mentioned earlier in this Essay, PIPEDA provides ten principles of data privacy. Examining and understanding these principles is crucial to an organization’s compliance. This section discusses the PIPEDA “Ten Commandments” and what actions organizations should take in order to stay current with—if not ahead of—the quickly-evolving Canadian and international data privacy regimes.

Accountability is PIPEDA’s first requirement, and serves as the cornerstone of compliance with privacy laws. Organizations holding or dealing with protected personal information are ultimately responsible for keeping it safe. This primarily means that organizations must adopt a privacy policy that complies with basic principles of data privacy protection as set forth in PIPEDA and train their employees in respect to these policies. Organizations should appoint an individual or team within such organization (e.g., a C-level security officer, such as a chief privacy officer or a similar senior executive83) who will be responsible for compliance and will have the ability to address complaints. Management of the organization must provide meaningful support to such privacy specialists. Subsidiaries and affiliates may be considered separate entities under PIPEDA, and may require additional staff and resources for compliance.

Second, organizations must inform data subjects of the purpose for the collection of their personal information, either before or after the information is gathered. Whether this should be accomplished orally or in writing depends upon the situation. Importantly, organizations can use personal information solely for the identified purpose for its collection. PIPEDA, therefore, effectively requires companies to obtain

83. “C-level” is a corporate term used to describe a ‘chief’ level executive, such as a chief operating officer or chief executive officer.
consent from data subjects to use that information for a new purpose, unless the new purpose is mandated by law or another exception applies.\textsuperscript{84} Accordingly, organizations should consider the kinds of information they hold regarding their employees and their customers, where such information is stored, how it is accessed, whether the organizations provide the necessary safeguards, and whether such information is transferred across national borders.

PIPEDA’s third requirement is \textit{consent}. Similar to the EU requirements, PIPEDA requires the “knowledge and consent” of the data subject for collection, use or disclosure of personal information in Canada. There are a few exceptions to this general rule on both sides of the Atlantic, including disclosure for law enforcement, artistic, and journalistic purposes. Another exception specifies permissible activity at the time of the sale of a business (though PIPEDA may apply differently to other forms of corporate transfers of ownership, such as a sale of assets of a corporation). Some of these exceptions are captured in Part II, above.\textsuperscript{85} In Canada, another exception is implied consent, where an individual should reasonably expect the use of personal information. Still, an organization is barred by PIPEDA from conditioning provision of a service or sale of products to consumers on consent to use of their personal information.\textsuperscript{86} Consumers may also withdraw their consent, subject to contractual constraints and reasonable notice.\textsuperscript{87} Consequently, organizations should be aware of what data they are collecting, using, or disclosing, and in what jurisdictions.

Fourth, organizations must \textbf{limit the collection} of protected personal information, and fifth, organizations must limit such information’s \textbf{use or disclosure}. Organizations may collect protected personal information only for a specific purpose, and thus may not gather personal information not necessary for that purpose. Information cannot be

\textsuperscript{84} See PIPEDA, 2000 S.C., ch. 5 § 4.2.4 (Can.); D’Angelo & Lehman, \textit{supra} note 79, at 11-12.
\textsuperscript{85} PIPEDA and the Quebec law are unclear regarding data privacy compliance at point of sale of assets of a business (where some disclosure and transfer of protected data can occur during due diligence). Federal and Quebequois authorities do not distinguish between sale of assets and sale of shares, but according to the Privacy Commissioner, this may change with PIPEDA’s next revision. Meanwhile, Alberta and British Columbia provide a protocol for “business transactions” which includes sale of assets. The seller and buyer are required to exchange confidentiality agreements, requiring, in part, the other party to use the information for the purposes it was collected. The British Columbia law also requires post-closing notification of the individuals. See Shaw, \textit{supra} note 2; D’Angelo & Lehman, \textit{supra} note 79, at 11-13 (British Columbia); D’Angelo & Varga, \textit{supra} note 79, at 10-13 (Alberta).
\textsuperscript{86} Spaeth et al., \textit{supra} note 15, at 35.
\textsuperscript{87} Id.
used, disclosed, or retained for any purpose other than the identified purpose or the exceptions applicable under PIPEDA, without obtaining consent of the data subject. Once an organization is finished using a data subject’s information, or if the data subject requests, the company must destroy, erase, or anonymize the information. For example, a bank cannot use the personal information of an employee who is also its customer in order to withhold or debit overpaid wages.89

Sixth, organizations must ensure that the personal information they have is accurate, complete, and up-to-date, based on the identified purpose for collecting and using the information. This requirement is controversial because organizations may have to gather more information to keep the information it has up-to-date and complete, but that collection of additional information may not be allowed under PIPEDA if not necessary for the identified purpose. Thus, PIPEDA presents organizations collecting information with a potential legal Catch-22, because such organizations may have to go back to collecting information from the data subject not for the identified purpose as at time of original collection, but solely to comply with this law.

Seventh, organizations must both effect policies to safeguard protected information (such as security clearances for accessing information) and have the technological savvy to protect such data from loss or

<table>
<thead>
<tr>
<th>No Consent</th>
<th>Implied Consent (Reasonably Expected)</th>
<th>Express Consent</th>
</tr>
</thead>
</table>

88. See PIPEDA, 2000 S.C., ch. 5 § 3 (Can.).
89. Racicot & Morgan, supra note 21, at 12.
Eighth, organizations must make their privacy policies and procedures transparent. They have to make readily available to individuals specific information about their policies and practices relating to the management of personal information. This relates directly to PIPEDA’s ninth requirement, which guarantees the data subject the right to access the information held by the organization. Organizations must inform the data subject (upon request) of the existence, use, and disclosure of his or her personal information and provide access to that information. Data subjects must be able to challenge the accuracy and completeness of the information, and organizations must amend the information accordingly.

Tenth and finally, individuals have the right to file a complaint directly with an organization challenging the organization’s compliance with the PIPEDA data privacy principles. Organizations must implement procedures to resolve and investigate all such complaints.

The Canadian Privacy Commissioner may require an organization to perform Privacy Impact Assessments (PIA) or Privacy Audits in order to assess an organization’s level of data protection compliance and identify gaps within its data protection practices. PIAs provide documentation to demonstrate that privacy issues have been appropriately identified and addressed. A cross-border PIA can be conducted as part of an initial privacy review and on an ongoing basis when new products, services, systems, operations, vendors, or business partners are under consideration. These audits can be time-consuming and expensive, and remain one of the more effective “sticks” available to the Privacy Commissioner in his or her quest to ensure compliance. While it may take a while to figure out whether a violation occurred or not and to determine which party should prevail in a privacy dispute, a Privacy Audit will require much attention from the very top of the organization and can divert valuable resources. The more an organization follows the principles above, the less likely it is to be the subject of complaint or privacy audit.

International data privacy laws are extremely complex and varied, and it is important for organizations to seek counsel from in-house or outside privacy experts on compliance issues. Canada’s privacy laws differ from province to province, which, in turn, differ from federal laws such as PIPEDA. The European Union’s privacy regime is even more daunting, considering that the European Union has twenty-seven members, each with its own set of privacy laws. Furthermore, data privacy protection in the United States is governed by an intricate patchwork of federal sectoral legislation, as well as dozens of state-
specific laws and regulations. Finally, in each of these global regions, data privacy laws apply differently to different kinds of organizations (e.g., public versus private, regulated versus non-regulated). This is a new and a fast-developing field, and consulting with a privacy expert is the best way to ensure that an organization will not violate any of the applicable laws, which can potentially save the organizations much time and money.

IV. THE FUTURE OF IDP IN CANADA AND OTHER WESTERN DEVELOPED NATIONS

In September 2005, Trevor Shaw, the Director General of Audit and Review in the Office of the Privacy Commissioner of Canada, addressed the U.S. Department of Homeland Security (DHS) on Canada’s international perspectives on the law of data privacy protection. Mr. Shaw concluded that, despite many similarities, Americans and Canadians view their privacy rights quite differently. Canadians are much more concerned with the use and disclosure of their personal information by public and private entities than are their American neighbors. The Privacy Commissioner conducted a survey of Canadians about emerging data privacy concerns. That survey found that “only 1 in 10 Canadians expressed low concern in the event that Canadians’ personal information was to be transferred across borders,” including to the United States, and that “virtually all Canadians want not only to be informed of transfers of personal information outside the country, but also first to be asked for their permission.” Mr. Shaw concluded that these results:

have profound implications for the outsourcing of data processing, and the sharing of personal information with foreign governments. Canadians are clearly concerned about these issues and want to retain control of their personal information. They do not want the reasonably strong protections afforded their personal information in Canada to disappear as soon as their personal information crosses the border.

The Privacy Commissioner urged “the federal government to review the implications of its outsourcing of personal information and to

90. Shaw, supra note 2, at 3.
91. Id. at 3, 5.
92. Id.
develop contractual clauses to protect personal information transferred to third parties for processing.”93 In response, the government implemented guidelines that set out rules for outsourcing activities in which the personal information of Canadians is handled or accessed by private sector agencies under contract with government institutions.

Surveys indicate that Canadians are also uneasy about infringement of their privacy rights for national security reasons. The Privacy Commissioner has repeatedly expressed concern about the USA PATRIOT Act, and has recently suggested that the Canadian government should consider tightening its requirements for export of its citizens’ personal information, particularly to the United States and, perhaps, making those restrictions similar to the EU Directive’s limitations on transferring personal information to countries without adequate data privacy protections.94

Also, in 2004, the Information and Privacy Commissioner of British Columbia conducted a survey of the extent to which Canadians’ personal information was available to the Federal Bureau of Investigation (FBI) under the USA PATRIOT Act.95 From this review emerged “an awareness of the extremely limited protection of personal information about Canadians in the hands of foreign governments.”96 In response to these results, the legislature of British Columbia passed a law preventing public bodies, and their contractors, from storing personal information outside of Canada and restricting the disclosure of personal information to organizations in other countries.97

Nevertheless, Canadians recognize the need to balance national security and privacy concerns. In late 2006, Canada adopted the Passenger Protect Program, which will require airlines to screen their

93. Annual Report, supra note 11, at 19.
95. See Office of Privacy Comm’r of Canada, Submission to the Office of the Info. and Privacy Comm’r for British Columbia, Transferring Information About Canadians Across Borders—Implications of the USA PATRIOT Act (Aug. 18, 2004); Shaw, supra note 2 (mentioning the research conducted by David Loukidelis, the Information and Privacy Commissioner of British Columbia, into the extent to which personal information about Canadians was available to the FBI under amendments to the Foreign Intelligence Surveillance Act introduced by the USA PATRIOT Act). See also USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).
96. Shaw, supra note 2, at 5.
97. Id.
passengers’ names with the government list of dangerous persons.\textsuperscript{98} The program was set to launch in early 2007 for domestic flights in Canada, and will extend to international flights by the end of this year.\textsuperscript{99} However, the Canadian government sought input from the Privacy Commissioner as well as civil liberties and ethno-cultural groups.\textsuperscript{100} As Trevor Shaw put it, Canadian officials are concerned with “secur\[ing\] democracy . . . without destroying democracy in the process.”\textsuperscript{101}

Following the terrorist attacks on September 11, 2001, the U.S. government has been trying to broaden the government’s access to individuals’ personal information. The United States continues to pursue a sectoral, self-regulatory approach to protection of personal information. At the same time, the European Union keeps expanding the reach of its data protection laws, along with strengthening the efforts to enforce any such laws and regulations. In contrast to both, Canadians favor an approach that is more comprehensive and respectful of protecting personal information than the current framework in the United States, while simultaneously endorsing a less aggressive solution than offered by the EU. Canada appears to be actively seeking to attain a balanced position on data privacy protection. Canada’s struggle to achieve this balance may be instructive for the U.S. and EU lawmakers and privacy watchdogs seeking to work out their differences. Canada’s solution may serve as a foundation for achieving greater consensus, or at least greater consistency, among the international data privacy laws.

\textsuperscript{99} Id.
\textsuperscript{100} Id.
\textsuperscript{101} Shaw, supra note 2, at 7.