Privacy Alert™
Legal and political developments affecting privacy

A publication of Nixon Peabody LLP

MAY 17, 2012

Canadian privacy law and its application to U.S. companies doing business with Canadians

By Benjamin R. Dwyer and Jacob J. Herstek[1]

Companies are increasingly concerned about compliance with U.S. federal and state privacy laws. If they do business across the Canadian border or receive personal information of Canadian citizens in the U.S, they should be concerned about Canadian privacy laws as well. Canada's laws are more far-reaching than their U.S. counterparts, and may apply to non-Canadian entities. This Alert discusses issues of concern to such companies.

Background on the Personal Information Protection and Electronic Documents Act

Canada's privacy statutes broadly govern how personal information can be collected, maintained, used and disclosed. Relative to such laws in the U.S., Canada's privacy laws apply more comprehensively and encompass virtually all commercial entities. The Personal Information Protection and Electronic Documents Act (PIPEDA) is Canada's federal privacy statute, with general application throughout Canada.[2] In contrast, state and federal laws in the United States form a patchwork of regulations that are often industry and jurisdiction specific. Enforcement of these laws is also equally uneven between state and federal agencies all with varying interests in privacy.

PIPEDA applies to organizations that collect, use, or disclose *personal information* in the course of *commercial activities*. Commercial activity is defined broadly: a transaction, act, or regular course of conduct that is commercial in character.

Personal information is "information about an identifiable individual" other than the name, title, business address, or telephone number of an organization's employee. It has been interpreted broadly and includes information as diverse as business e-mail addresses, computer internet protocol addresses, salespersons' sales statistics, and photographs of the interior of one's apartment. The essence of the definition is that the information presents a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information.

PIPEDA empowers Canada's Office of the Privacy Commissioner (OPC) to investigate complaints. The Canadian Federal Court can order compliance with the law and award damages to complainants.

How might U.S.-based companies fall within the scope of PIPEDA?

A U.S.-based company with operations in Canada that handles the personal information of Canadians—whether customers or employees—clearly falls within PIPEDA's scope. Even if its operations are solely on the U.S. side of the border, such a company handling Canadians' personal information may also fall within the scope of PIPEDA. Canadian courts have held that PIPEDA may apply to—and the OPC's investigative authority extends to—non-Canadian companies that obtain Canadians' personal information, even if they operate outside Canada's borders. California-based internet services companies, a Wyoming-based online data broker, a Dutch airline, and a Belgium-based processor of international banking transactions have each been deemed to come within the scope of PIPEDA.

What are the implications of the application of PIPEDA TO U.S.-BASED COMPANIES?

While the ability of the OPC to sanction non-Canadian entities for PIPEDA noncompliance is limited, the Canadian courts have held that the OPC does have the authority to investigate such entities to the extent they directly obtain and handle Canadian citizens' personal information. As some U.S.-based companies have learned, such investigations may result in well-publicized adverse findings. Non-Canadian companies interested in protecting their reputation and their business relationships vis-à-vis Canadian counterparts should consider ensuring that their privacy policies meet PIPEDA standards. In addition, depending upon circumstances, a violator may be subject to the jurisdiction of the Canadian courts for a claim for damages by a PIPEDA complainant.

U.S. companies that do not obtain Canadians' information directly but receive it pursuant to a service contract with a Canadian company—e.g., for e-mail or financial services data storage—ought to be aware of their counterparts' obligations under PIPEDA or other privacy laws. The OPC has held that in such situations the Canadian outsourcer is obligated to ensure the foreign entity's practices are PIPEDA-compliant.

Finally, U.S.-based companies considering an asset purchase of a Canadian entity should conduct due diligence review to ensure that the vendor's personal information collection and maintenance practices are compliant with PIPEDA and other Canadian provincial privacy laws.

What are the obligations imposed by PIPEDA?

Briefly, companies subject to PIPEDA must designate a privacy officer accountable for the organization's compliance. They must implement policies and practices to give effect to the requirements, including protection of the personal information, responding to complaints and inquiries, training staff, and publicizing their policies and procedures. Such companies must identify the purposes for which they collect personal information and must, subject to some exceptions, obtain consent from individuals for the collection, use, or disclosure of personal information. Collection of information must be limited to the purposes described in disclosures and the information can be retained only as long as necessary for the fulfillment of the purposes for which it was collected. Such companies must protect personal information by security safeguards appropriate to the sensitivity of the information. Upon request, companies must respond with information about their policies and practices relating to the management of personal information, give individuals access to their own personal information, and be able to inform them of the existence, use, and disclosure of their information. In essence, these privacy and security measures are best practices and are consistent with U.S. federal and state laws.

For assistance with these cross-border privacy and other issues, please contact your Nixon Peabody Privacy & Data Protection team attorney or:

- Benjamin R. Dwyer at bdwyer@nixonpeabody.com or (716) 853-8122
- Jacob J. Herstek at jherstek@nixonpeabody.com or (716) 848-8207

---

[1] Mr. Dwyer is licensed to practice law in the Province of Ontario. Mr. Herstek is a recognized Certified Information Privacy Professional accredited by the International Association of Privacy Professionals.

[2] Although some provinces have privacy laws of their own, from the point of view of non-Canadian companies, PIPEDA is the main focus.