Protection of personal information remains at the forefront of public policy debate in Canada. Federal and provincial privacy legislation has a profound impact on the way virtually all organizations carry on business across the country. In addition, Canada has now enacted comprehensive anti-spam and anti-spyware legislation that will apply to commercial electronic messages and computer program distribution by legitimate businesses in Canada, not just those engaged in deploying spam and spyware.

**Tough New Spam and Spyware Law**

Canada has enacted what may be the most comprehensive spam law in the world. The legislation, which is known as Canada’s Anti-spam Law (or CASL), goes much further than regulating bulk, unsolicited email communications. Rather, it creates an “express” or “opt-in” consent-based regime that applies to almost all electronic messages, including e-mail, text and instant messages and other electronic messages sent for a commercial purpose. As well, it sets out prescriptive rules governing, among other things, unsubscribe mechanisms, sender identity and contact information.

CASL also includes an express consent and related disclosure requirements for the installation of computer programs. Although the principal policy objective of the new rules is to deter the distribution of “spyware,” they will apply to many computer programs and regardless of whether the program is installed for a malicious purpose.

Once the new anti-spam and spyware rules come into force (which is expected in late 2011), organizations that fail to comply will be exposed to stiff penalties, including administrative monetary penalties of up to $10,000,000 for corporations ($1,000,000 for individuals). As well, a private right of action would allow consumers and businesses to commence enforcement proceedings and recover damages, including statutory damages of up to $1 million a day.
Public Sector Privacy Laws

Public sector privacy laws apply in the federal and most provincial and municipal jurisdictions. Similar to the U.S. federal Privacy Act, the federal Privacy Act and provincial counterparts require government departments, agencies, most Crown corporations and municipal government bodies to define, and notify individuals of, the lawful, authorized purposes for their collection of an individual’s personal information and to provide access to personal information they hold that is requested by individuals. Some provincial public sector privacy laws restrict public sector bodies and/or their service providers from permitting access to or disclosure of personal information from or to a place outside Canada. (See International Personal Data Transfers below.)

Private Sector Privacy Laws

Canadian businesses are subject to federal or provincial privacy protection legislation governing both customer and (with some exceptions) employee information. The federal Personal Information Protection and Electronic Documents Act (PIPEDA)1 applies to all private sector organizations in Canada, except in provinces that have enacted “substantially similar” legislation. PIPEDA also applies when personal information is disclosed across a provincial border in the course of commercial activity and in most situations where an organization in Canada receives or transmits personal information from or to a destination outside Canada.

Québec, B.C. and Alberta2 each have their own private sector privacy law3 which has been recognized as “substantially similar” to PIPEDA. Ontario’s health information law has also been declared substantially similar to PIPEDA.

There is uneven privacy law coverage of employee personal information in Canada. PIPEDA only applies to information about employees if an organization is a federal work, undertaking or business.4 However, privacy legislation in Québec, B.C. and Alberta does apply to employee information. Businesses operating in the other provinces,

---

1 S.C. 2005, c. 5, as amended.
2 Québec Act Respecting the Protection of Personal Information in the Private Sector, RSQ, c. P-39.1 (Que. PPIPS); B.C. Personal Information Protection Act, SBC 2003, c. 63 (B.C. PIPA); Alberta Personal Information Protection Act, SA 2003, c. P-6.5 (Alta. PIPA).
3 Ontario Personal Health Information Protection Act, SO 2004, c. 3, Schedule A (Ont. PHIPA).
4 Federal works, undertakings or businesses are those in the inter-provincial transportation, shipping and communication sectors, banks and offshore operators, as well as in Canada’s three territories (Yukon, Northwest territories and Nunavut).
where PIPEDA applies, will not be subject to privacy laws in relation to their employees unless the business is federally regulated for purposes of employment and labour relations.

PIPEDA and provincial privacy statutes also do not apply to the journalistic, artistic or personal collection, use or disclosure of personal information.

**Requirements of Private Sector Privacy Legislation**

PIPEDA requires compliance with the 10 “fair information management principles” of the *Model Code for the Protection of Personal Information* (Model Code) developed by the Canadian Standards Association.

The Model Code requires organizations to notify individuals of the purposes of, and obtain their consent for, the collection, use or disclosure of their personal information (PIPEDA sets out limited exceptions to this notice and consent requirement) and to have reasonable and appropriate purposes for their collection, use or disclosure of personal information. Organizations also are required to limit the amount of personal information that the organization collects, uses, discloses or retains to that necessary for the purpose for which it was collected; are prohibited from tying the provision of goods or services to consent by individuals to a collateral collection, use or disclosure of personal information; and must meet standards for accuracy and the security of the personal information they hold.

In addition, organizations must implement a privacy policy and appoint a privacy officer who will be responsible for representing the organization in privacy matters, provide individuals with access to their personal information (with limited exceptions) and correct inaccurate information at the request of individuals.

Provincial privacy statutes in Québec, B.C. and Alberta contain similar requirements and exceptions, although differences between provincial statutes and PIPEDA necessitate close examination of each law in most situations involving personal data collection, use and disclosure.

Federal and provincial Privacy Commissioners have made numerous findings with significant impact on business practices, ranging from decisions on the standards for notice and consent for marketing communications, affiliate sharing, purchase histories, international data transfers and social media applications, to decisions on large international personal data breaches, the use of voice recognition and GPS technologies for data collection, restrictions on collection of drivers’ licences for fraud prevention purposes, use of publicly available and aggregate personal information, standards for video surveillance, inappropriate collection and use of personal information by psychological profiling services and data retention by online dating services.
Privacy law requirements relating to service providers and outsourcing, data breach notification and international personal data transfers are set out below.

**Health Sector Privacy Law Requirements**

Alberta, Saskatchewan, Manitoba, Ontario, New Brunswick, Newfoundland and Labrador and Nova Scotia\(^5\) have each passed health information protection laws to deal specifically with the collection, use and disclosure of personal health information by public and private sector health care providers, called custodians or trustees. Health information protection laws also apply, directly or indirectly, to agents who act for health care custodians, as well as to service providers that manage information, such as data storage and system management providers.

Health information statutes require custodians to notify and obtain express consent from patients for all collection, use or disclosure of personal health information, with limited exceptions for disclosures to other health information custodians within a patient’s circle of care. Subject to detailed, limited exceptions, each statute contains provisions entitling patients to access their personal health information, limits access to and use of health information within a custodian’s organization, and prohibits disclosure for purposes other than those to which a patient has consented.

**Enforcement of Privacy Laws**

**Domestic**

The Privacy Commissioner of Canada (PCC) oversees both the federal Privacy Act and PIPEDA. The PCC may audit the privacy practices of organizations suspected of a breach of PIPEDA, and may receive and investigate complaints of non-compliance. The PCC can make recommendations regarding PIPEDA compliance and report to Canada’s Parliament organizations that are found not to comply. Both the PCC and complainants may seek remedies for non-compliance in the Federal Court of Canada, which has wide remedial authority to award damages and issue mandatory compliance orders.

Provincial privacy laws are enforced by provincial Information and Privacy Commissioners (IPCs) or Ombudsmen, who can investigate complaints and issue binding orders requiring compliance. In addition, individuals have a private right of action for privacy breaches in Québec, B.C., Alberta and Ontario (under the Ontario PHIPA) where a Commissioner has made an order finding a breach.

---

\(^5\) Alberta Health Information Act, RSA 2000, c. H-5; Saskatchewan Health Information Protection Act, SS, 1999 c. H-0.021; Manitoba Personal Health Information Act, CCSM c. P33.5; Ontario PHIPA (footnote 3); New Brunswick Personal Health Information Privacy and Access Act, SNB 2009, c. P7.05; Newfoundland Personal Health Information Act, SNL 2008, c. P7.01; Nova Scotia Personal Health Information Act, SNS 2010, c. 41 (not in force as of June 14, 2011). The Ontario PHIPA has been declared substantially similar to PIPEDA.
International

PIPEDA applies to the personal information of non-residents, so that non-residents of Canada can complain to the PCC about PIPEDA breaches by an organization in Canada.

The PCC can co-operate and share investigation information with foreign authorities, such as the U.S. Federal Trade Commission, when investigating an international privacy breach involving Canada. Both the PCC and IPCs investigate and make findings regarding alleged breaches of PIPEDA or provincial privacy laws that may originate or be caused outside Canada but involve the personal information of Canadians.6

Data Breach Notification

2010 amendments to the Alberta PIPA now require notification to the Alberta IPC by businesses that have experienced a data breach and empower the IPC to order organizations to notify individuals of data breaches, in both cases where the data breach represents a “real risk of significant harm” to individuals. In the year since passage, the Alberta IPC has issued over 20 notification orders in cases of data breaches involving organizations in Alberta as well as organizations outside Alberta and/or Canada where individuals in Alberta may be affected.

Proposed 2010 amendments to PIPEDA7 would require businesses to notify the PCC and individuals (and other organizations capable of mitigating the harm) of a data breach where the breach presents a real risk of significant harm to individuals, as soon as feasible after the detection and assessment of the risk of harm caused by the breach. Direct, clear and conspicuous notification including sufficient information for a person to understand the significance of the breach and, if possible, mitigate any resulting harm would be required. The PCC has also issued guidance in advance of the PIPEDA amendments that the PCC expects to be notified of data breaches presenting a real risk of significant harm.

Outsourcing and Service Providers

Organizations that outsource or contract for services retain responsibility for privacy compliance in respect of the personal information transferred to the service provider. While this puts service providers – including those providing services from outside the country – in the position of ensuring information is handled or processed in compliance with PIPEDA, the contracting organization is generally responsible for obtaining consent from individuals and for ensuring,

---

6 Examples are PCC investigations and findings regarding the Abika search service, Facebook’s third-party applications and Google’s street video mapping WIFI data collection and Alberta IPC data breach notification orders involving data breaches occurring in the U.S.

7 Bill C-29 died with the 2011 federal election, but is expected to be re-introduced in the fall of 2011.
through contractual means, that service providers provide comparable protection for the personal information that they process or store for organizations subject to Canadian privacy laws.

International Personal Data Transfers

Private Sector Privacy Laws

The European Union’s (E.U.) “safe harbour” rule requires organizations to ensure that any jurisdiction to which they are sending personal data has enacted legislation providing “adequate” privacy protection. The E.U.’s designation of PIPEDA as providing “adequate protection” enables the exchange of personal data between E.U. member states and Canada (where PIPEDA applies) without the necessity of a safe harbour agreement.

PIPEDA and provincial privacy laws require organizations to notify individuals of out-of-country personal data processing or storage by the organization or its service providers.8 Alberta’s PIPA also requires organizations to disclose to individuals who request its policies and practices and to provide a contact person to answer questions regarding service providers handling personal information outside Canada. In addition, the Alberta and B.C. PIPAs and most health information protection laws require consent for disclosure of personal information to law enforcement and investigatory bodies outside Canada.

The Québec PPIPS (An Act Respecting the Protection of Personal Information in the Private Sector) makes organizations responsible for compliance when they use, transfer or disclose personal information outside Québec, and prohibits the transfer or disclosure if it cannot be assured that the personal information will not be used or disclosed for other purposes than those for which it was transferred or disclosed to third parties without consent.

Public Sector Privacy Laws

In response to public concerns about threats to privacy arising under the USA PATRIOT Act, B.C. and Nova Scotial,9 have enacted data-blocking measures that prohibit public sector bodies (which include utilities, hospitals and Crown corporations in those provinces) from permitting out-of-country access or disclosure.

The data-blocking restrictions place tough restrictions on the storing, accessing and disclosing of B.C. and Nova Scotia public sector data by service providers from or to locations outside Canada. A number of other provinces, such as Alberta, have amended their public sector privacy laws to require notice to and consent from individuals for disclosure of personal information to law enforcement bodies outside Canada.

---

8 The Québec PPIPS does not require such notice, but notice of out of country data transfers is recommended as a best practice.

In addition, the Canadian federal and most provincial governments have adopted a risk assessment approach to mitigate the risk of information breaches, address privacy and security risks in service contracts and determine the level of trans-border personal data processing or storage permissible by service providers to public bodies. These legislative restrictions and policies will significantly impact how service providers to public sector bodies in Canada store or access personal information.

Finally, as part of a broad discussion on border security and harmonization, the Canadian federal government is in ongoing discussions addressing trans-border data flows through the Security and Prosperity Partnership with the U.S. and Mexico. These discussions involve potential agreements to collect and share personal information about travelers, transporters, importers and exporters between Canada, the U.S. and Mexico.

Osler’s Privacy team has helped shape the privacy landscape in Canada and can help clients identify practical solutions to privacy issues. Patricia Wilson and Michael Fekete are partners in our Firm.

PATRICIA WILSON
pwilson@osler.com
613.787.1009

MICHAEL FEKETE
mfekete@osler.com
416.862.6792