DOLDEN WALLACE FOLICK LLP

INFORMATION PROTECTION AND PRIVACY LEGISLATION IN CANADA

Jill M. Shore and Paul C. Dawson

November 2014

18th Floor - 609 Granville St.
Vancouver, BC
Canada, V7Y 1G5
Tel: 604.689.3222
Fax: 604.689.3777

308 - 3330 Richter Street
Kelowna, BC
Canada, V1W 4V5
Tel: 1.855.980.5580
Fax: 604.689.3777

850 - 355 4th Avenue SW
Calgary, AB
Canada, T2P 0J1
Tel: 1.587.480.4000
Fax: 1.587.475.2083

500 - 18 King Street East
Toronto, ON
Canada, M5C 1C4
Tel: 1.416.360.8331
Fax: 1.416.360.0146

CONTACT LAWYER

Jill Shore

604.891.0390
jshore@dolden.com

Paul Dawson

604.891.0378
pdawson@dolden.com

The laws applicable to information protection and privacy in Canada vary across the provinces and territories, and there is a combination of both provincial and federal laws that apply. There are 38 different personal information protection, health information protection and privacy statutes in force across Canada, which can be subdivided into four main types:

(1) personal information protection laws applicable to government and public bodies;

(2) personal information protection laws applicable to private sector organizations;

(3) provincial personal health information laws; and

(4) provincial privacy laws.

Not all provinces and territories have enacted one of each of the four types of statutes. Additionally, each jurisdiction has drafted slightly different wordings for each of these types of statutes. As a result, a thorough review of all of them is required to fully understand the legal landscape applicable to information protection and privacy in Canada.

This paper briefly summarizes the Canadian information protection and privacy laws as they apply across the country, and some of the high profile lawsuits that have resulted from data and privacy breaches in Canada.[1]

I. The Application of Federal Laws within the Provinces and Territories:

The federal government has legislative power over personal information in the possession or control of federal government entities, and over federally regulated entities (entities that are considered to be federal works, undertakings or businesses ("FWUB")), located anywhere in Canada. Provincial governments have legislative power over personal information in the possession or control of provincial government entities and over provincially regulated entities (all commercial activities within a province, excluding inter-provincial or international activities, or FWUBs).

[1] This paper does not include a discussion of Canada's Anti Spam Legislation, brought into force on July 1, 2014, which is related to information protection and privacy. A copy of CASL can be found here. Further information regarding CASL is available upon request.

The federal *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5, ("PIPEDA"), also applies to personal information held by private sector organizations in some but not all provinces. It applies in the provinces and territories as follows:

- to organizations in industries such as telecommunications, broadcasting, inter-provincial or international transportation (*i.e.*, trucking, railways, and aviation), banking, military, nuclear energy, maritime navigation and shipping, which are subject to federal legislative jurisdiction;

- to organizations in the Yukon, Northwest Territories and Nunavut, which are considered to be FWUBs;

- to employee information of FWUBs; and

- to personal information (excluding employee information) collected, used or disclosed in the course of commercial activities by provincially regulated private organizations, in those provinces which do not have their own provincial personal information protection legislation applicable to the private sector in a format that has been deemed to be substantially similar to the federal PIPEDA (*e.g.*, in Saskatchewan, Manitoba, Ontario, New Brunswick, Nova Scotia, PEI, Newfoundland, and the territories).

To clarify, the federal PIPEDA does not apply:

- to employee information of provincially regulated private organizations in any province, even if PIPEDA applies to commercial activities of such private organizations;

- to commercial activities of provincially regulated private sector organizations in the provinces of Alberta, British Columbia, and Quebec, which have their own provincial personal information protection legislation that has been deemed by regulation to substantially similar to the federal PIPEDA.

- to health information custodians operating in the private sector in Ontario, which are subject to Ontario's *Personal Health Information Act*, 2004 S.O. 2004, c. 3., because it has also been

deemed by regulation to be substantially similar to the federal PIPEDA.

II. Personal Information Protection Laws that Apply to Government and Public Bodies:

Federal	*Privacy Act*, RSC 1987, c. P-21.
Alberta	*Freedom of Information and Protection of Privacy Act*, RSA 2000, c. F-25
British Columbia	*Freedom of Information and Protection of Privacy Act*, RSBC 1996, c. 165
Manitoba	*Freedom of Information and Protection of Privacy Act*, CCSM, c. F175
New Brunswick	*Right to Information and Protection of Privacy Act*, SNB 2009, c. R-10.6
Newfoundland	*Access to Information and Protection of Privacy Act*, SNL 2002, c. A1-1.
Northwest Territories	*Access to Information and Protection of Privacy Act*, SNWT 1994, c. 20
Nova Scotia	*Freedom of Information and Protection of Privacy Act*, SNS 1993, c. 5
Nova Scotia	*Part XX of the Municipal Government Act*, SNS 1998, c. M-26
Nova Scotia	*Personal Information International Disclosure Protection Act*, SNS 2006, c. 3
Nunavut	*Access to Information and Protection of Privacy Act*, SNWT (Nu) 1994, c. 20
Ontario	*Freedom of Information and Protection of Privacy Act*, RSO 1990, c. F. 31
Ontario	*Municipal Freedom of Information and Protection of Privacy Act*, RSO 1990, c. M.56

Prince Edward Island	*Freedom of Information and Protection of Privacy Act*, RSPEI 1988, c. F-15.01
Quebec	*An Act respecting access to documents held by public bodies and the Protection of personal information*, CQLR, c. A-2.1
Saskatchewan	*The Freedom of Information and Protection of Privacy Act*, SS 1990-91, c. F-22.01
Saskatchewan	*The Local Authority Freedom of Information and Protection of Privacy Act*, SS 1990-91, c. L-27.1

These Acts protect the privacy of individuals with respect to personal information held by **public bodies**. The scope of coverage of these Acts varies across the jurisdictions, but they typically include (unless a separate local or municipal Act applies) the following:

- the applicable federal, provincial or territorial government institutions;
- crown corporations;
- provincial agencies, boards, and commissions;
- health care, social services, and educational bodies;
- professional and occupational governing bodies; and
- local public bodies, including municipal governments, agencies, boards and commissions;

all located within the jurisdiction of the enacting government. These Acts also provide individuals with a right of access to information held by these public bodies.

Personal information is typically defined as *"...information about an identifiable individual that is recorded in any form..."*. This definition is sometimes followed by a non-exhaustive list of the types of information specifically included as personal information.

These Acts prohibit the collection, use and disclosure of personal information without consent, other than as authorized by the Acts. Most of them impose on the public body a duty to protect personal information in its custody or control, by making reasonable security arrangements against risks such as the unauthorized access, collection, use, disclosure, or disposal of personal information.

None of these Acts specifically provide for a duty to notify affected individuals in the event of a breach of privacy, but such an order would likely fall within the general jurisdiction of the Commissioner under most Acts.

These Acts establish Privacy Commissioners in the respective jurisdictions, with powers to receive and investigate complaints from individuals relating to breaches of the Acts, and to initiate its own investigations and audits. The Acts typically do not create a statutory cause of action giving rise to damages for breach of privacy. Instead, they give the Commissioners various powers, which vary in degree among the jurisdictions. At the low end of the spectrum, the Commissioner has the power to make recommendations to offending organizations, and to request that the organizations report back to the Commissioner to confirm either that the recommendations have been implemented or to explain why they have not been implemented (federal *Privacy Act*). At the high end of the spectrum, the Commissioner has the power to make orders following an investigation to, among other things, require a duty imposed under the Act to be performed, require a public body to stop collecting, using or disclosing personal information in contravention of the Act, or require terms and conditions to be met (British Columbia).

Most of the Acts provide for a right of judicial review by or appeal to the local courts from the decision of the Commissioner, and make it an offence under the Act for an organization to fail to comply with the orders made by the Commissioner. The Quebec Act enables a person injured by a public body to bring an action in court to seek damages as compensation for injury, including punitive damages.

III. Personal Information Protection Laws that Apply to Private Sector Organizations:

Federal	*Personal Information Protection and Electronic Documents Act*, SC 2000, c.5, ("*PIPEDA*")
Federal	*An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, SC 2010, c. 23 *[usually referred to as the "Canadian Anti-Spam Law", or "CASL"]*
Alberta	*Personal Information Protection Act*, SA 2003, c. P-6.5
British Columbia	*Personal Information Protection Act*, SBC 2003, c. 63
Manitoba	*Personal Information Protection and Identity Theft Prevention Act*, SM 2013, c. 17, s. 34(2) [*not yet in force*]
Quebec	*An Act Respecting the Protection of Personal Information in the Private Sector*, RSQ, c. P-39.1

These Acts govern the collection, use, and disclosure of personal information by the **private sector.**

As noted above, the **federal** PIPEDA applies to:

- every "*organization*" in respect of "*personal information*" that the organization collects, uses or discloses in the course of "*commercial activities*", unless provinces or territories have enacted substantially similar legislation (*i.e.*, Alberta, British Columbia, Quebec, and health organizations in Ontario, in which case the provincial Acts apply and PIPEDA does not); and

- employees of organizations that operate a federal work, undertaking or business ("FWUB") (but not to employee information of non-FWUBs).

The terms "organization", "personal information" and "commercial activities" are defined very broadly, which gives PIPEDA a wide reaching scope of application. The federal PIPEDA does not apply to: any federal government institution to which the federal *Privacy Act* applies; information collected, used or disclosed for personal or domestic (family and home) purposes; or information collected by organizations for exclusively journalistic, artistic or literary purposes.

The **provincial** personal information protection Acts govern the collection, use and disclosure of personal information by **private organizations** (including businesses, charities, unincorporated associations, trusts, trade unions and labour organizations, and not-for-profit associations) within the enacting province. The provincial Acts typically do not apply to the collection, use or disclosure of personal information for personal or domestic (home or family) purposes.

Personal information is defined in these Acts in a manner that is substantially similar to the Acts that apply to protect personal information in the possession or control of public bodies. Personal information typically does not include business contact information, or work product information.

Organizations that are subject to private sector personal information protection Acts must comply with the minimum personal information protection measures contained in the Acts. All of them impose on the organizations a duty to protect personal information within their possession or control. Although the duty to protect sections are all worded differently, they typically require that personal information shall be protected by security safeguards appropriate to the sensitivity of the information, to protect against loss or theft, and unauthorized access, disclosure, or use.

The Alberta PIPA has some unique provisions that were added by amendment to that Act in May 2010, which set out minimum standards for notification requirements in the event of security breaches that pose a real risk of significant harm (organizations must notify the Commissioner, and upon receipt of such notice, the Commissioner may require the organization to give notice to affected individuals). The purpose of the notification requirements is to avoid or mitigate harm to individuals that might result from the breach.

The Federal Government has introduced legislation to amend *PIPEDA* and require mandatory data breach notification, to both the Privacy Commissioner and to affected

individuals, of any breach of security safeguards involving personal information, "*if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual*" (Bill S-4, the "*Digital Privacy Act*"). Two previous government Bills (Bill C-29, 2010; Bill C-12, 2011) failed to pass before the close of the respective Parliamentary sessions, and a substantially similar Bill introduced by an opposition Member of Parliament was defeated by the government in January, 2014 (Bill C-475). However, if the current Bill should pass, the amendments would dramatically increase the frequency of mandatory notice programs across Canada.

None of the other general personal information protection Acts currently contain an express duty to notify, but Manitoba's PIPITPA will, if it comes into force, require organizations to notify individuals "*as soon as practicable*" about the theft or loss of, or unauthorized access to, their personal information. As of November, 2014, this statute had not yet come into effect.

Like the personal information protection Acts that apply to the public sector, these Acts establish a Commissioner with similar powers to hear and investigate complaints, initiate their own complaints and audits, and write reports of their conclusions and make orders following an investigation. Many of these Acts give the complainant a right to apply to court for a hearing following an investigation.

The federal PIPEDA authorizes a complainant to bring action in court following a report of a Commissioner, and authorizes the court to order organizations to comply with the Act, and to award damages for breach of privacy. The provincial Acts provide the Commissioner with the power to make orders, and establish offences under the Act for failing to comply with the order of a Commissioner. None of these provincial Acts provide for a right to seek damages from the Commissioner for breach of privacy. However, the Quebec Act provides the Commissioner with broad powers to make remedial orders. Complainants may try to seek damages under this provision.

The BC and Alberta acts create a statutory cause of action for damages resulting from a breach of the Act found by the Commissioner, or resulting from an offence committed under the Act, if an individual has suffered loss or injury as a result of the breach or offence. These Acts do not provide for a right of appeal of a Commissioner's decision, but judicial review is available to the local courts.

Manitoba has not appointed a Privacy Commissioner, so its recent privacy legislation, not yet in effect, will allow affected individuals to commence action in the Courts directly, without any prior resort to an administrative process or remedy.

Actions filed by individual claimants arising from data and other privacy breaches are most commonly commenced by filing a pleading known as a "Notice of Civil Claim", "Statement of Claim", or something similar. Defendants (known in some jurisdictions as respondents) file a responsive pleading. After an exchange of documents, and usually examinations for discovery or an equivalent form of deposition under oath, the matter is set down for trial. The result is binding only on the individual parties involved.

PIPEDA specifies that parties who wish to rely on a breach of that statue must file their claims in the Federal Court of Canada, a Court that only addresses matters involving issues of federal jurisdiction, including the interpretation of Federal statutes. Claimants relying on equivalent personal information statutes, upon Provincial privacy statutes, or upon the common law right to privacy may commence proceedings in Provincial Supreme Courts (known in some jurisdictions as Superior Court). Under *PIPEDA*, s. 14, an action must be filed in Federal Court within 45 days of the report, decision, or notification issued by the Federal Privacy Commissioner; Alberta's personal information statute contains the same deadline, whereas the window is only 30 days in British Columbia.

IV. Provincial Personal Health Information Laws:

Alberta	*Health Information Act*, RSA 2000, c. H-5
British Columbia	*E-Health (Personal Health Information Access and Protection of Privacy) Act*, SBC 2008, c. 38
Manitoba	*Personal Health Information Act*, CCSM, c. P33.5
New Brunswick	*Personal Health Information Privacy and Access Act*, SNB 2009, c. P-7.05
Nova Scotia	*Personal Health Information Act*, SNS 2010, c. 41
Newfoundland & Labrador	*Personal Health Information Act*, SNL 2008, c. P-7.01

Ontario	*Personal Health Information Protection Act*, *2004*, SO 2004, c. 3
Québec	*An Act Respecting the Sharing of Certain Health Information*, CQLR C. P-9.0001
Saskatchewan	*Health Information Protection Act*, SS 1999, c. H-0.021
Yukon	*Health Information Privacy and Management Act*, SY 2013, c. 16 [*not yet in force*]

The provincial health information Acts apply to the collection, use and disclosure of personal **health information** held by "health information custodians" within the enacting provinces. Health information custodians are typically defined to include, among others, health care practitioners (doctors, dentists, physiotherapists, etc.), home care service providers, hospitals, independent health facilities, retirement and long term care homes, pharmacies, and ambulance services. Most of these Acts (all but British Columbia) impose on custodians a duty to protect against unauthorized use or disclosure of personal health information in its possession or control. Most empower the provincial Privacy Commissioner to hear complaints, make investigations, conduct inquiries and issue orders, like under the other provincial personal information protection Acts, and to appeal orders to the courts. These Acts also create offences for certain breaches of the Acts, which are punishable by monetary penalties.

Only the Ontario PHIPA contains a duty to notify the individual affected at the first reasonable opportunity, if personal health information is stolen, lost or accessed by unauthorized persons. The Ontario PHIPA also creates a statutory cause of action for damages resulting from a breach of the Act found by the Commissioner, or resulting from an offence committed under the Act.

The Saskatchewan Act empowers the court to make any order it considers appropriate if it has found that a breach of the act has occurred. Complainants could try to seek damages under this section.

V. Provincial Laws that Create a Statutory Cause of Action for Breach of Privacy:

British Columbia	*Privacy Act*, RSBC 1996, c. 373
Manitoba	*Privacy Act*, CCSM, c. P125
Newfoundland & Labrador	*Privacy Act*, RSNL 1990, c. P-22
Saskatchewan	*Privacy Act*, RSS 1978, c. P-24

The statutory cause of action under PIPEDA and equivalent Provincial statutes is premised specifically upon the loss, misuse, or unauthorized access to personal information held by an organization. However, the *Privacy Acts* in several Provinces (British Columbia, Saskatchewan, Manitoba, and Newfoundland and Labrador) have created a separate statutory cause of action premised upon a breach of a right to privacy. This cause of action may overlap with the *PIPEDA* and similar statutory causes of action; certain factual scenarios might give rise to claims under both the personal information and privacy statutory regimes, *e.g.*, where an employee accesses private customer information without authority, but it can arise in situations not covered under the personal information statutes (*e.g.*, where an employee is alleged to have spied on customers in a business' restroom).

Finally, in Provinces that have *not* adopted statutes equivalent to the *Privacy Acts* of British Columbia, *et al.*, the Courts have developed a broadly similar common law cause of action for breach of privacy, known as the tort of intrusion upon seclusion. First recognized by Ontario's Court of Appeal in *Jones v. Tsige*, 2012 ONCA 32, there is relatively little applicable case law on this new doctrine. The test for liability is whether the invasion of privacy was intentional, lacked legal justification, and would be considered offensive to the reasonable person. It will typically relate to particularly personal subjects, such as financial matters, sexual orientation, diaries and private correspondence, etc.

Whether the cause(s) of action relied upon are statutory or common law, it is important to note that, unlike in the United States, proof of economic loss or other particular harm is *not* a pre-requisite for liability.

VI. Significant Lawsuits Arising from Breach of Personal Information Protection and Privacy Laws:

Damages in individual data breach and privacy cases tend not to be large. The Court in *Jones*, *supra*, awarded only $10,000 to the successful plaintiff; in a recent Federal Court decision, *Chitraker v. Bell TV*, 2013 FC 1103, an award of $21,000 (including $10,000 in punitive damages) was widely considered to be large.

Because data breaches tend to involve large numbers of records relating to large numbers of affected individuals, and because individual harm to those individuals may be difficult to prove, court proceedings in Canada are often brought as class actions.

Several data breach and privacy-related class actions have been commenced in Canada in recent years, with diverse results:

- In *Evans v. Bank of Nova Scotia*, 2014 ONSC 2135, the Ontario Superior Court of Justice certified a class action based on the new tort of intrusion upon seclusion. Customers of the Bank sued the bank and its employee, as a result of the employee's disclosure of their personal information to his girlfriend, who then disseminated it for fraudulent and improper purposes. Several customers were the victims of identity theft or fraud. The plaintiffs seek to hold the bank vicariously liable for the tortious and deliberate actions of its employee.

- In *Douez v. Facebook, Inc.*, 2014 BCSC 953, the Court approved certification of a class action on behalf of all Facebook users resident in British Columbia whose name, portrait, or both had been used by Facebook in a "sponsored story" without the user's consent. The pleadings established a cause of action under British Columbia's *Privacy Act*, s. 3(2), which makes it a tort, actionable without proof of damage, to use a person's name or portrait for advertising or promotional services without that person's consent.

- In *Condon v. Canada*, 2014 FC 250, Canada's Federal Court certified a class proceeding on behalf of 583,000 students whose financial and student loan data, stored on an unencrypted hard drive, was lost by a

civil servant. The Court certified claims for breach of contract and for "intrusion upon seclusion" (*i.e.*, the privacy tort recognized in *Jones v. Tsige*, discussed above), but refused to certify claims in negligence because there was no evidence that any class member had suffered an actual loss.

- In *Maksimovic v. Sony of Canada Ltd.*, 2013 CanLII 41305 (ONSC), the Court approved a certification and settlement of a class action arising from the 2011 hacking of Sony's "Play Station Network" and related gaming services. Details of up to 4.5 million accounts held by Canadian gamers were compromised. Under the terms of the settlement, class members were entitled to be paid out in cash the balance of any affected PSN accounts; gamers were granted certain "online game and service benefits"; and Sony agreed to reimburse members who can demonstrate they actually suffered any identity theft, including expenses of up to $2,500 per claim. Class counsel fees were approved at $265,000, and Sony agreed to pay for a notice program that reached as many as 3.5 million accountholders' email addresses.

- Certification for the purpose of settlement was granted in *Speevak v. Canadian Imperial Bank of Commerce*, 2010 ONSC 1128. The defendant bank had inadvertently but repeatedly faxed customer information to a private fax machine in the United States. The Privacy Commissioner concluded that the bank had failed to properly safeguard the information. No cases of identity theft appear to have resulted from the breach, but the bank agreed to compensate anyone who did suffer a loss; it also paid $100,000 to a public interest advocacy group and $42,500 to class counsel for its fees, plus unspecified costs.

- The Court in *Rowlands v. Durham Region Health*, 2012 ONSC 3948, approved a settlement arising from a nurse's loss in 2009 of an unencrypted USB stick containing data on 83,524 flu shot recipients. By 2012, there was still no evidence any identity theft had occurred. The defendants agreed to reimburse any claims presented before August 2, 2016, and paid $500,000 to class counsel to cover costs.

- The Court in *Albilia c. Apple inc.*, 2013 QCCS 2805, certified what appears to be a highly speculative action on behalf of consumers in Québec who had downloaded applications from Apple that allegedly shared private information with third parties.

- Certification was refused in *St-Arnaud c. Facebook Inc.*, 2011 QCCS 1506, in which the class alleged they had been exposed to the disclosure of personal information as a result of changes Facebook made to its terms of use and policies. The Court concluded that class members had clicked to accept the changes, and could have no cause of action.

- Certification was also refused in *Mazzona c. DaimlerChrysler Fniancial Services of Canada*, 2012 QCCS 958, a case arising from the defendant's loss during shipment of an unencrypted tape containing data on approximately 240,000 customers. The proposed plaintiff admitted she had not suffered any identity theft, and the Court concluded that mere anxiety about the *possibility* of theft did not amount to compensable damages.

Several high-profile data breaches in the past several years involving Human Resources and Skills Development Canada, the British Columbia Ministry of Health, Health Canada (Medical Marihuana Program), and Home Depot Canada, have spawned numerous class action or putative class action privacy suits.

VII. Conclusion:

Information protection and privacy laws in Canada vary from province to province. There are 38 different statutes that apply in various jurisdictions, as of the date of this paper. Both federal laws and provincial and territorial laws apply, although in some provinces, some of the federal laws have been replaced with similar provincial laws. This is a rapidly developing area of the law, with legislative amendments pending and new cases being tried. This paper summarizes the key provisions of these various statues, the jurisdictions in which they apply, and how the courts in Canada are responding to breaches of these various laws.