A Look at Canadian Privacy and Anti-Spam Laws

By: Junior Sirivar and Shana Wolch

Junior Sirivar is a Partner in McCarthy Tétrault's Litigation Group and Co-Chair of the Firm's International Arbitration Practice Group. He advises domestic and international clients in complex commercial disputes across a variety of industries including mining, banking and telecommunications.

Shana Wolch is a partner in McCarthy Tétrault's National Labour and Employment Group in Calgary. She assists clients with their daily human resources matters (including privacy and occupational health and safety), across the full spectrum of industries, including oil & gas, utilities, banking, retail, forestry, transportation, hospitality, and education. She has also been a lead investigator in workplace and OHS investigation matters and frequently provides support and training for clients to conduct their own investigations.

CANADA'S comprehensive federal and provincial privacy laws regulate how organizations collect, use, and disclose personal information in the course of conducting or operating their businesses. These laws are intended to protect individual privacy rights and, in doing so, require that organizations take reasonable steps to ensure that such rights are sufficiently protected. Canadian privacy laws can have a significant impact on organizations' policies and practices while operating in Canada.

Organizations must establish reasonable security measures to protect personal information that crosses international borders. The obligations imposed by privacy laws supplement existing obligations

respecting transparency, consent and safeguarding. Moreover, organizations need to provide assurances that the foreign third-party service provider's privacy practices provide a comparable level of protection as to that which is required under Canadian law, recognizing that the laws of the foreign jurisdiction cannot be overridden.

Canadian privacy laws provide a mechanism that is intended to facilitate more streamlined transactions where such transactions involve the collection, use or disclosure of personal information. Corporations operating, or looking to operate, in Canada must be aware of the obligations imposed on them by these laws as a failure to do so can have significant repercussions.

This paper will aid those that are operating or seeking to do business in Canada by promoting compliance with Canada's privacy and anti-spam laws, which will in turn prompt strong and effective business activities. Specifically, we discuss the obligations imposed by Canada's anti-spam legislation, more commonly referred to as "CASL,"[1] as well as the other federal and provincial privacy laws that outline the framework and rules for the collection, use and disclosure of personal information by federally-regulated private-sector organizations operating across Canada.

These laws are not intended to restrict businesses from operating in Canada. Rather, they seek to support commerce, including electronic commerce, and promote the adaptability of the Canadian economy and market by clarifying expectations and rights for protecting an individual's privacy while in the process. Public confidence in the integrity of a business's operations is of key importance to operating successfully. By developing appropriate policies and corporate strategies, organizations can comply with the applicable privacy law requirements while mitigating risks associated with improperly collecting, using or disclosing personal information in potentially damaging manners.

I. CASL: Canada's Anti-Spam Law

A. General

CASL is a comprehensive legislative regime created to combat

[1] 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, S.C. 2010, c. 23.

spam. It is aimed at preventing organizations, including foreign ones, from sending unsolicited or misleading commercial electronic messages ("CEM") or programs to consumers without their consent. In particular, CASL introduces the requirement to obtain the consent of a recipient before an organization sends a CEM. This requirement extends to email messages, messages to social networking accounts and text messages to smart phones.

B. Principles

CASL came into force on July 1, 2014 and is widely considered to be among the most comprehensive, and to an extent onerous, commercial electronic messaging statutes in the world. It has significant implications for Canadian businesses, not-for-profit organizations, and individuals using electronic communications. CASL also applies to foreign organizations that operate or do business in Canada, or that send commercial electronic messages to Canada.

CASL's provisions regarding CEMs extend far beyond typical "spam" emails. A CEM is an electronic message that is intended to encourage participation in a commercial activity. When determining if an electronic message encourages a commercial activity, the content of the message, the hyperlinks in the message or the contact information contained in the message may all be considered. Further, the types of commercial activities that would be considered to constitute a CEM include but are not limited to:

(i) offers to purchase, sell, barter or lease a product, goods, a service, land or an interest or right in land;
(ii) offers to provide a business, investment or gaming opportunity;
(iii) advertisements or promotions of anything referred to in (i) or (ii); or
(iv) promoting a person, including the public image of a person, as being a person who does anything referred to in any of (i), (ii) or (iii), or who intends to do so.[2]

Organizations must therefore carefully scrutinize their use of email and other electronic messaging systems, including SMS, social networks and online portals.

On January 15, 2015, provisions of CASL relating to unsolicited installation of computer programs or software came into force. These provisions prevent the installation of computer programs without an

[2] CASL, s. 1(2).

individual's consent.[3] CASL's computer programs provisions affect a wide range of platforms, from applications on personal computers, tablets and mobile devices, to programs embedded in consumer products, such as automobiles, TV sets, and home audio systems. CASL's computer program provisions apply only to programs that automatically install software on someone's computer; they do not apply to individuals installing software on their own devices.

C. Consent

Consent, as interpreted by CASL, can either refer to express consent, or under certain circumstances, implied consent. Express consent means that a person has clearly agreed to receive a CEM, prior to a CEM being sent to him or her. By requiring consent first, CASL has enabled an "opt-in" regime in relation to spam, unlike some other countries that have enabled "opt-out" regimes, like the United States. CASL's "opt-in" regime applies to both Canadian organizations and non-Canadian organizations so long as these organizations are sending commercial electronic messages to recipients *within* Canada.[4]

Under certain circumstances, such as an existing business relationship between an organization and a recipient of a CEM, an organization may be able to rely on implied consent in sending CEMs. Other circumstances where implied consent may be relied upon are described in section 10(9) of CASL.

The onus of proving consent is always on the sender. As a result, it is prudent for the sender of a CEM to employ good record-keeping practices, which may help the sender establish a due diligence defense in the case of an alleged violation of CASL.[5] Good record-keeping may include retaining hard copies or preferably electronic records of:

1. all evidence of express and implied consent (e.g. audio recordings, copies of signed consent forms, completed electronic forms) from

[3] Government of Canada, *Canada's Anti-Spam Legislation*, 2013, available at http://fightspam.gc.ca/eic/site/030.nsf/eng/h_00039.html.

[4] CASL, s. 12(1).

[5] Government of Canada, *Enforcement Advisory – Notice for businesses and individuals on how to keep records of consent* July 27, 2016, available at https://www.canada.ca/en/radio-television-telecommunications/news/2016/07/enforcement-advisory-notice-for-businesses-and-individuals-on-how-to-keep-records-of-consent.html.

consumers who agree to receive CEMs;
2. documented methods through which consent was collected;
3. policies and procedures regarding CASL compliance; and
4. all unsubscribe requests and resulting actions.[6]

Diligent record keeping is of critical importance. Anything not in writing will be difficult to prove later in the event of a complaint. Moreover, lack of documentation makes it complicated – even impossible – to allow for internal management purposes such as tracking implied and express consents that have been previously obtained or even withdrawn.

D. Enforcement

Three federal agencies are responsible for the enforcement of CASL: (i) The Canadian Radio-television and Telecommunications Commission ("CRTC"), (ii) the Competition Bureau, and (iii) the Office of the Privacy Commissioner of Canada (the "Privacy Commissioner").

The CTRC has the primary enforcement responsibility for CASL and is able to investigate, take action against, and set administrative monetary penalties for violations of CASL. For the most part, CASL is enforced by undertakings of the sender to remedy his/her actions,[7] and notices of violation.[8]

CASL provides for significant administrative monetary penalties of up to CAD$1,000,000 per violation for individuals, and CAD$10,000,000 for organizations. In 2016, 22 notices of violation were issued by the CTRC for violations of CASL with associated penalties ranging from $5,000 to $650,000,[9] and in 2015 the CTRC issued a notice of violation for CAD$1,100,000 for sending CEMs to individuals without their consent, along with other violations of CASL.[10]

The Competition Bureau is also

---

[6] Government of Canada: Canadian Radio-television and Telecommunications Commission, from *Canada's Anti-Spam Legislation (CASL) Guidance on Implied Consent*, September 4, 2015, available at http://www.crtc.gc.ca/eng/com500/guide.htm.

[7] CASL, s. 21.

[8] CASL, s. 22.

[9] Government of Canada, *Canadian Radio-Television and Telecommunications Commission: Notices of Violation 2016*, August 30, 2017, available at http://www.crtc.gc.ca/eng/DNCL/dnclc_2016.htm.

[10] Government of Canada, *Canadian Radio-Television and Telecommunications Commission: Notices of Violation 2015*, October 28, 2015, available at http://www.crtc.gc.ca/eng/DNCL/dnclc_2015.htm.

enabled to enforce the law under CASL through more effectively addressing false and misleading representations and deceptive marketing practices. CASL enables the Privacy Commissioner to enforce the law regarding the collection of personal information through access to computer systems, as well as electronic address harvesting.[11]

E. CASL's Private Right of Action

It is anticipated that CASL will allow individuals and organizations to bring a private right of action ("PRA") in court against persons they allege to have violated the law.[12] The PRA will allow individuals and organizations to seek compensatory damages in an amount equal to the loss or damages suffered, or expenses incurred, as a result of the contravention.[13] There may be statutory damages imposed by the court in addition to the compensatory damages under this PRA.[14] An individual could claim for breaches of CASL including the improper transmission or rerouting of CEMs to other destinations than those intended by the sender, unauthorized installation of computer programs, or participating or promoting any of these activities. They can also bring claims for being the target of false or misleading CEMS under the Competition Act, that their electronic address has been obtained without their consent or that their personal information has been obtained through accessing a computer system without authorization in breach of the federal Personal Information Protection and Electronic Documents Act.[15]

In the case of unsolicited emails, these statutory damages may reach a maximum of $200 per contravention of CASL, not exceeding CAD$1,000,000 for each day on which a contravention occurred.[16] Considering that a single email sent to a recipient, without his or her consent would be considered a violation of CASL, if even a small company sent out 1,000 unsolicited emails, they could face up to $20,000 in fines, in addition to any compensatory damages to the recipients of those emails.

---

[11] Government of Canada, *Canada's Anti-Spam Legislation: Enforcement*, June 13, 2017, available at http://fightspam.gc.ca/eic/site/030.nsf/eng/h_00026.html.

[12] CASL, s. 47; Government of Canada, *Canada's Anti-Span Legislation*, June 13, 2017, available at http://fightspam.gc.ca/eic/site/030.nsf/eng/h_00039.html. This section was intended to take effect July 1, 2017 however was suspended and is under review.

[13] CASL, s. 51(1)(a).

[14] CASL, s. 51(1)(b).

[15] CASL, s. 47.

[16] CASL, s. 51(1)(b)(i).

II. Private Sector Privacy Laws in Canada

A. Basic Principles

In addition to CASL, which regulates specific electronic commercial activities, such as emailing individuals, other Canadian legislation is more generally aimed at regulating how private-sector organizations collect, use, and disclose personal information in the course of their business operations. Owing to Canada's federal framework, these laws may be federal or provincial. Federally, Canada has enacted the Personal Information Protection and Electronic Documents Act ("PIPEDA"). PIPEDA is comprehensive federal legislation that outlines the framework and rules for the collection, use and disclosure of personal information by federally-regulated private-sector organizations operating across Canada.[17] It also governs the collection, use and disclosure of personal information in the course of commercial activities by non-federally regulated private sector organizations operating across Canada.

PIPEDA does not, however, govern private-sector organizations operating in provinces that have comprehensive privacy legislation deemed substantially similar to PIPEDA. To this end, there are only three provinces that have been found to have privacy legislation which is substantially similar to PIPEDA: Québec, British Columbia, and Alberta.[18] The privacy legislation applicable to each of these provinces are:

- Québec's *Act* Respecting the Protection of Personal Information in the Private Sector,[19] (the "Québec Act");
- British Columbia's Personal Information Protection Act (the "BC PIPA");[20] and
- Alberta's Personal Information Protection Act (the "AB PIPA").[21]

B. Federal Law

PIPEDA applies to "every organization in respect of personal information that the organization collects, uses or discloses in the course of commercial activities".[22] Organizations must first determine what personal information is collected, used, or disclosed as part

---

[17] That is, federally-regulated works, undertakings, or businesses including banks, airlines, and telecommunications companies.

[18] Manitoba has also enacted similar legislation, which has not yet come into force, the Personal Information Protection and Identity Theft Prevention Act, SM 2013, c 17.

[19] RSQ, c P-39.1 [Québec Act].

[20] SBC 2003, c 52 [BC PIPA].

[21] SA 2003, c P-6.5 [AB PIPA].

[22] PIPEDA, s. 4(1)(a).

of their operations in Canada. They must then determine whether such personal information is collected, used, or disclosed in the "course of commercial activities" and in which jurisdictions. The Federal Privacy Commissioner[23] has expressed the opinion that information *created* (as opposed to collected) by an organization as part of commercial activity may also be subject to PIPEDA. For instance, the Federal Privacy Commissioner determined that an individual's credit score is information subject to PIPEDA because it was created by an organization in the course of its commercial activities.[24]

PIPEDA protects "information about an identifiable individual".[25] Canadian courts have deemed "identifiable individual" to be someone who it is reasonable to expect can be identified from the information at issue when combined with information from sources otherwise available, including sources publicly available.[26] Business contact information is excluded from this definition because it is collected by organizations for the purpose of communicating or facilitating communication with an individual in relation to his/her employment, business or profession.[27]

Schedule 1 of PIPEDA sets out the ten principles of fair information practices (the "Fair Information Principles") for organizations to observe. These Fair Information Principles form ground rules for the collection, use, and disclosure of personal information,[28] and underscore basic privacy obligations and practices for organizations to implement and maintain. Corporations would be well-served by ensuring that their internal policies adhere to these 10 principles:

1. accountability;
2. identifying the purposes;
3. consent;
4. limiting collection;
5. limiting use, disclosure, and retention;
6. accuracy;
7. safeguards;

---

[23] The Federal Privacy Commissioner is responsible for investigating alleged violations of PIPEDA.

[24] The Privacy Commissioner of Canada, *PIPEDA Case Summary #2002-39*, 2002, available at https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2002/*PIPEDA*-2002-039/.

[25] PIPEDA, s. 2(1).

[26] *Canada (Information Commissioner) v. Canada (Canadian Transportation Accident Investigation and Safety Board)*, 2006 FCA 157, at para. 43; *Gordon v. Canada (Minister of Health)*, 2008 FC 258, at paras. 31-34.

[27] PIPEDA, s. 4.01.

[28] Office of the Privacy Commissioner of Canada, *Privacy Toolkit for Businesses*, 2015, available at https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-*PIPEDA*/*PIPEDA*-compliance-help/guide_org/.

8. openness;
9. individual access; and
10. challenging compliance.

Additionally, in June 2015, the federal government amended PIPEDA through the enactment of the Digital Privacy Act[29] in six respects of significance to organizations. The amendments:

1. addressed the issue of consent and what constitutes valid consent;
2. introduced additional exceptions to obtaining consent including in the exchange of personal information for business transactions;
3. addressed employment relationships and the exchange of personal information produced in the course of employment;
4. introduced mandatory breach notification to be provided to both the privacy commissioner and affected individuals where there has been a breach of security safeguards that poses a real risk of significant harm to the affected individuals;
5. introduced penalties including compliance agreements; and
6. introduced broader public interest disclosure powers.

1. Key Obligations under PIPEDA

a) Limitation on the Collection of Personal Information

PIPEDA recognizes "the right of privacy of individuals with respect to their personal information" while accepting "the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."[30] An organization's ability to collect, use or disclose personal information is accordingly framed in the following terms under Section 5(3) of PIPEDA: "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."

Collection, use or disclosure of personal information is considered "appropriate in the circumstances" if:

[29] SC 2015, c. 32. All amendments under the *Digital Privacy Act* are now in force, except for the data breach requirements, which have not yet come into force, pending the formulation and passage of regulations. No timeline has been publicly set for completion the formulation of the regulations.

[30] PIPEDA, s. 3.

(i) the collection, use or disclosure of personal information is necessary to meet a specific need;
(ii) the collection, use or disclosure of personal information is likely to be effective in meeting that need;
(iii) the loss of privacy is proportional to the benefit gained; and
(iv) there is no less invasive way of achieving the same end.[31]

Schedule 1 to PIPEDA also contains "The Model Code" which limits an organization's collection of personal information to that which is necessary for the purposes identified by the organization. [32] Organizations shall not collect personal information indiscriminately. All aspects of the collection of information must correlate to the identified purpose. Where collection of information is found to be unnecessary, the result will be non-compliance with PIPEDA,[33] and may be taken to Federal Court to enforce compliance.[34]

For example, the Federal Privacy Commissioner has found that it was unreasonable for an automobile business to scan customers' vehicle registration documents in relation to simple automobile maintenance services. The automobile business could collect sufficient technical information about a vehicle (i.e. make, model, year) to service the vehicle from scanning the vehicle identification number. Scanning the vehicle registration document, which disclosed more personal information (i.e. the owner's address, drivers' license number), was not necessary for the purpose of changing motor oil in vehicles.

b) Limitation on the Use, Disclosure, and Retention of Personal Information

Organizations are required to limit the use, disclosure, and retention of personal data to the purpose(s) for which the data was collected. Any other use or disclosure of personal information requires the consent of the individual or must either fall under a PIPEDA exception or be required by law. Moreover, such information is to be retained only as long as is necessary for the fulfillment of those purposes.[35]

---

[31] *Mountain Province Diamonds, Inc. v. De Beers Canada, Inc*., 2014 ONSC 2026, at para. 47.

[32] PIPEDA, Schedule 1, s. 4.4.

[33] The Federal Privacy Commissioner, *PIPEDA Case Summary #2010-006*, 2010, available at https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/ investigations-into-businesses/2010/*PIPEDA*-2010-006/.

[34] PIPEDA, s. 14.1.

[35] PIPEDA, Schedule 1, s. 4.5.

Organizations are encouraged to develop policies and procedures with respect to the retention of personal information, including minimum and maximum retention periods. Personal information that has been used to make a decision about an individual is to be retained long enough to allow the individual access to the information after the decision has been made.[36]

c) Ensuring the Accuracy of Personal Information

Organizations are required to ensure that the personal data they collect and store is as accurate, complete, and up-to-date as is necessary for the purposes for which the data are to be used. The extent to which an organization must meet these requirements will depend upon the use of the information, taking into account the interests of the individual.[37]

2. Rights of the Individual

a) Identification of Purpose

In order for individuals to give informed consent to the collection, use, or disclosure of personal information, organizations must identify the purpose for the collection of personal information.[38] The purposes must be legitimate and explicitly specified.[39]

b) Informed Consent

Consent is required prior to the collection, use, or disclosure of personal information under PIPEDA. Consent may be implicit or explicit and, depending on the circumstances, in oral form or in writing. An organization should generally seek express consent when the information is likely to be considered sensitive, while implied consent is more appropriate when the information is less sensitive. In all cases, the consent must be "informed".[40] The Digital Privacy Act sets out parameters for determining whether consent is valid, which is only where it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting. This amendment to PIPEDA arguably creates an obligation on organizations to ascertain the degree of sophistication of the individual when obtaining consent.

An individual may withdraw consent at any time, subject to legal or contractual restrictions and

[36] PIPEDA, Schedule 1, s. 4.5.2.
[37] PIPEDA, Schedule 1, s. 4.6.
[38] PIPEDA, Schedule 1, s. 4.2.
[39] PIPEDA, Schedule 1, s. 4.3.3.
[40] PIPEDA, Schedule 1, s. 4.3.

reasonable notice. The organization is required to inform the individual of the implications of such withdrawal.[41]

The general approach privacy commissioners in Canada have taken on the issue of informed consent has been outlined in guidance issued by the Federal, Alberta and British Columbia privacy commissioners on the specific issue of best practices for privacy in mobile apps. [42] This guidance noted that at the point of downloading, the user should be clearly informed (a) what personal information the app will be collecting and why; (b) where information will be stored (on the device or elsewhere); (c) who it will be shared with and why; and (d) how long it will be kept. The guidance also noted that advance notice should be given before implementing changes to the privacy policy.

Consent to collection of personal information is not necessary in certain situations specified under the Act, including when the collection is clearly in the interest of the individual and consent cannot be obtained in a timely way, when it is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province, and when the information is publicly available. PIPEDA provides a list of exceptions to the consent requirements, subject to specific conditions, including in the context of prospective or completed business transactions.[43]

1. Right to Information

Organizations must make information about policies and practices relating to the management of personal information readily available. Under PIPEDA there are express requirements for provisions in privacy policies that follow the Fair Information Principles. [44] A well drafted and accessible privacy policy is both legally required and mutually beneficial for both organizations and the individuals from whom they collect or might collect personal information. [45] In

[41] PIPEDA, Schedule 1, s. 4.3.8.

[42] The Federal, Alberta and British Columbia privacy commissioners, *Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps*, 2012, available at https://www.oipc.bc.ca/guidance-documents/1426.

[43] PIPEDA, s. 7.

[44] The privacy policy must identify the safeguards in place, procedures for making and responding to complaints/ inquiries/access requests, procedures for training and communicating the privacy policies and practices to staff, provide explanatory information of these policies and practices, privacy officer's information, describing the type of personal information to be held and a general account of its use, identifying the personal information that is available to affiliates, and making this policy available.

[45] For example, the Federal Privacy Commissioner conducted a review of privacy policies on websites. The report

addition, organizations ought to go beyond that which is expressly required in the legislation to include, for example, additional uses and disclosures such as personal information that is being transferred and stored internationally.

2. Right of Access and Correction

Individuals are entitled to be informed of the existence, use, and disclosure of their personal information and must be given access to that information. Exceptions to the access requirement should be limited and specific, and any reasons for denying access should be provided to the individual upon request.[46]

3. Right to Challenge Compliance

Organizations must also facilitate complaints or inquiries regarding personal information within their control, including procedures to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information.[47] In order to comply with this requirement, an organization must design an effective and accessible process to address inquiries from time of receipt, through internal review and, ultimately, to resolution and/or communication with the individual. In most instances, the organization's privacy officer should control this process.

4. Security and Protection of the Data

Appropriate security protocols to protect personal information against loss or theft, unauthorized access, disclosure, copying, use, or modification must also be established.[48] The extent to which an organization must establish security protocols will depend on the sensitivity of the information at issue. The more sensitive the information, the higher the level of protection required. [49] It is important to ensure that employees

published following the review identifies observed best practices, as well as unsatisfactory manners in which privacy policies were handled. The Federal Privacy Commissioner, *Privacy enforcement authorities launch first-ever international Internet Privacy Sweep*, May 6, 2013, available at https://www.priv.gc.ca/en/opc-news/news-and-announcements/2013/nr-c_130506/.

[46] PIPEDA, Schedule 1, s. 4.9.

[47] PIPEDA, Schedule 1, s. 4.10.

[48] PIPEDA, Schedule 1, s. 4.7.

[49] Businesses should consider the regulatory framework set out by the Office of the Superintendent of Financial Institutions (OSFI), which imposes specific obligations on federally regulated financial institutions in respect of information technology outsourcing arrangements. Cloud-based outsourcing contracts must comply with the requirements of OSFI Guideline B-10, *Outsourcing of Business Activities, Functions*

are aware of the need to maintain the confidentiality of personal information and destroy or render anonymous the personal information upon completion of the retention period. In this electronic era, safeguarding will often entail the use of encryption software.[50]

5. Transfer of Information to a Third Party

The organization must also use contractual or other means to provide a comparable level of protection for information to be processed by the third party.

Organizations that transfer personal information across Canadian borders should consider the guidelines issued by the Federal Privacy Commissioner in this regard.[51] The guidelines require organizations to consider the legal requirements of the jurisdiction to which data will be transferred, and to take into account "potential foreign political, economic and social conditions, and events that may conspire to reduce the foreign service provider's ability to provide the service, as well as any additional risk factors that may require adjustment to the risk management program." The sensitivity of the information is a factor in the assessment of risk to the security of the information as a result of the transfer.

6. Transparency, Notification, and Registration with Local Authorities

Registration with, or notification to, data protection supervisory authorities is not required under PIPEDA. However, in Québec, there is a requirement for "personal information agents" to register with the provincial

and Processes, revised in March 2009, available at http://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/b10.aspx.

[50] The Federal Privacy Commission recently emphasizes the need to use encryption of date in its recent investigation into the personal information handling priorities of WhatsApp Inc. *See* The Federal Privacy Commissioner, *PIPEDA Report of Findings #2013-001 - Investigation into the personal information handling practices of WhatsApp Inc.*, 2013, available at https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2013/*PIPEDA*-2013-001/.

[51] The Federal Privacy Commissioner, *Guidelines for Processing Personal Data Across Borders*, 2009, available at https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/. *See also* joint publication of the Federal, B.C. and Alberta Privacy Commissioners, *Cloud Computing for Small and Medium-sized Enterprises*, June 2012, available at https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/online-privacy/cloud-computing/gd_cc_201206/. AB PIPA has express provisions relating to the transfer of personal information outside of Canada.

Commission d'accès à l'information.[52]

C. Provincial Law

Québec, British Columbia, and Alberta have in force provincial privacy protection laws that are substantially similar to PIPEDA. These laws apply to private-sector businesses that collect, use and disclose personal information while carrying on business in those provinces.

The Québec Act enables the protection of rights that are prescribed under the Québec Civil Code[53] (the "Civil Code"). The rights prescribed under the Civil Code are intended to recognize and protect individual reputation and privacy, including through restrictions on retention of certain private data. In addition, the Québec Charter of Human Rights and Freedoms grants every person the right to safeguard his/her dignity, honor, and reputation, the right to respect for his/her private life, and the right that their confidential information not be disclosed.[54]

The BC PIPA and AB PIPA both govern the collection, use and disclosure of personal information by private sector entities in their respective jurisdictions.

Regulatory and enforcement oversight under the applicable privacy legislation falls to "Privacy Commissioners" appointed in the various jurisdictions. While each Privacy Commissioner is independent, there is cooperation among the offices on various initiatives including joint investigations.[55]

The BC PIPA and AB PIPA protect information that can identify an individual and information about an individual, defined as "personal information." Both of these Acts also exclude business contact information from the definition of personal information.

The Québec Act defines personal information as any information that "relates to a natural person and allows that person to be identified;"[56] business contact information is not excluded from the definition of personal information in Québec. Non-Québec businesses may be subject to the application of the Québec Act if there is a sufficient connection to Québec, such as business operations, storage of data,

---

[52] Québec Act, s. 70. A personal information agent is "any person who, on a commercial basis, personally or through a representative, establishes files on other persons and prepares and communicates to third parties credit reports bearing on the character, reputation or solvency of the persons to whom the information contained in such files."

[53] CQLR c C-1991, ss. 35-41.

[54] CQLR c C-12, s 5.

[55] *See, for example*, joint publication of the Federal, B.C. and Alberta Privacy Commissioners, *Guidelines for Online Consent*, 2014, available at https://www.priv.gc.ca/media/2105/gl_oc_201405_e.pdf.

[56] Québec Act, s. 2.

or by virtue of the data subject being resident of Québec.

D. Enforcement

1. Federal Enforcement

The Federal Privacy Commissioner's principal responsibility is to act as an ombudsman in disputes between organizations and individuals,[57] but it has investigative powers in relation to complaints regarding the use or misuse of personal information. Importantly, the Federal Privacy Commissioner has asserted jurisdiction against foreign service providers with operations in Canada.[58] While the Federal Privacy Commissioner is not empowered to impose fines, the Commissioner's report or findings may be used as basis for private legal proceedings in which provincial courts are empowered to issue orders and award monetary damages.[59]

2. Provincial Enforcement

The Privacy Commissioners in the various provinces also have similar powers. However, unlike their federal counterpart, British Columbia and Alberta's Privacy Commissioners are empowered to impose significant fines for breaches of their respective statutes: up to CAD$10,000 for individuals and up to CAD$100,000 for businesses.[60] The Québec Privacy Commissioner can impose fines from CAD$1,000 to $50,000 for a first offence, and from CAD$10,000 to $100,000 for a subsequent offence.[61] Further, a contravention under the *AB PIPA* or *BC PIPA* may give an individual a cause of action in court for damages the individual has suffered as a result of a breach of an obligation by an organization under either Act.[62] Individuals may initiate claims for breach of privacy in Manitoba, Newfoundland and Labrador, Nova Scotia, Saskatchewan and Ontario.[63] As well, Québec civil law provides

---

[57] PIPEDA, s. 12.1.

[58] The Federal Privacy Commissioner, *PIPEDA Case Summary #2009-008 - Report of Findings into the Complaint Filed by the Canadian Internet Policy against Facebook Inc.*, July 16, 2009, available at https://www.priv.gc.ca/media/1033/2009_008_0716_e.pdf; The Federal Privacy Commissioner, *PIPEDA Report of Findings #2014-001 - Use of sensitive health information for targeting of Google ads*, January 14, 2014, available at https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2014/*PIPEDA*-2014-001/.

[59] PIPEDA, s. 14. *See also Randall v Nubodys Fitness Centres*, 2010 FC 681; *Nammo v. TransUnion of Canada Inc.,* 2010 FC 1284; *Biron v. RBC Royal Bank,* 2012 FC 1095; *Stevens v SNF Maritime Metal Inc.*, 2010 FC 1137.

[60] AB PIPA, s. 59; BC PIPA, s. 56.

[61] Québec Act, ss. 91-93.

[62] AB PIPA, s. 60; BC PIPA, s. 57.

[63] *See, for example, Jones v. Tsige*, 2012 ONCA 32.

remedies for invasions of privacy.[64] The common law tort of invasion of privacy may impose additional liability, although the availability and elements of the tort can differ from province to province.

III. Privacy Considerations in Business Transactions

A. Disclosure of Personal Information in Business Transactions

PIPEDA, the AB PIPA, and the BC PIPA provide certain exceptions to the requirement to obtain consent before the collection, use or disclosure of personal information. For organizations looking to do business in Canada, the most important exception allows the transfer of personal information to another organization, without the consent of the individual, in the context of a business transaction.[65]

This exception allows a business transaction to proceed confidentially and without needing to disrupt the workplace prematurely and potentially unnecessarily, also recognizing that obtaining consent from every employee in a timely fashion might be impractical (if not impossible).

The provisions relating to business transactions in PIPEDA, the AB PIPA, and the BC PIPA are substantially similar. Under all three Acts the exception to consent applies to proposed and completed business transactions, and the primary purpose of the business transaction must not be for the purchase, sale, or transfer of the personal information itself.[66]

For a proposed transaction, the parties must enter into an agreement that protects the personal information that they intend to transfer.[67] The agreement must require that the personal information will only be used for the purpose of the proposed business transaction and determining whether to proceed.

In the case of PIPEDA and the AB PIPA, there is a further requirement that the information also be necessary in order to complete the

---

[64] Civil Code of Québec, S.Q. 1991, c. 64, s. 3 and ss. 35-41.

[65] PIPEDA, s. 7.2; AB PIPA, s. 22; BC PIPA, s. 20. Note that both PIPEDA and the AB PIPA allow for the disclosure of an "identifiable individual" without their consent in the context of a business transaction, while *the BC PIPA* allows for the disclosure of personal information about an organization's employees, customers, directors, officers or shareholders.

[66] PIPEDA, s. 7.2(4); AB PIPA, s. 22(6); BC PIPA, s. 20(7).

[67] PIPEDA, ss. 7.2(1)(a), 7.2(2)(a); AB PIPA, s 22(3)(a)(i); BC PIPA, s. 20(2)(b). Under section 7.2(a)(ii) PIPEDA states that this agreement requires the organization that receives the personal information to protect that information by "security safeguards appropriate to the sensitivity of the information." The AB PIPA and BC PIPA do not have this requirement.

transaction.[68] The BC PIPA only requires that the information be necessary for determining whether to proceed with a proposed transaction.

For a completed transaction, the parties must enter into an agreement that requires that the personal information will only be used for the purpose for which it was previously collected (i.e., by the vendor organization and unrelated to the transaction).

These agreements are important not only for complying with the law and protecting information but can also be effective for establishing liability in the event that the agreement is breached.

Where a business transaction has been completed, both the BC PIPA and PIPEDA require that an individual be notified that the transaction took place and that his/her personal information was disclosed;[69] however, there is no such requirement under the AB PIPA.

Where a business transaction is not completed, all three Acts require that the prospective organization destroy any personal information that was collected under this exception, or return the personal information to the organization from which it originated.[70]

B. Cross-border transactions

The transfer of personal information outside of Canada is often undertaken by sending physical files or digital copies, or storing information on remote servers. Storing information on remote servers has become increasingly frequent, and the acquirers of this information can gain access to that server during the transaction. Both the provider and acquirer need to be cautious of the implications of transferring personal information outside of Canada.

Under PIPEDA, an organization is responsible for personal information in its possession, including information that has been transferred to a third party for processing, such as a remote server.[71] While information is being processed by a remote server, the organization is required to use contractual or other means to provide a comparable level of protection as the information would receive in Canada.[72] However, the Federal Privacy Commissioner has observed that where personal information is transferred to a foreign third party that information is subject to the laws of the foreign country and those laws cannot be

[68] PIPEDA, s. 7.2(1)(b); AB PIPA, s. 22(3)(a)(ii); BC PIPA, s. 20(2)(a).
[69] BC PIPA, s. 20(3)(c); PIPEDA, s. 7.2(2)(c).
[70] PIPEDA, s. 7.2(1)(a)(iii); AB PIPA, s. 22(4); BC PIPA, s. 20(6).
[71] PIPEDA, Schedule 1, s. 4.1.3.
[72] *Id.*

overridden by contractual provisions.[73]

As a result, the Privacy Commissioner has stated that, while consent is not required in order to transfer information across borders, an organization in Canada that transfers personal information to a foreign third party should at least notify affected individuals that their information may be stored or accessed outside Canada. This notification will depend on the sensitivity of the personal information and should address the potential impact that the storage of their information outside of Canada may have on their privacy rights.[74]

There are no specific provisions in PIPEDA regarding notification to individuals in the case of cross-border transfers. However, the AB PIPA includes a mandatory requirement for organizations to notify individuals before transferring personal information to a foreign service provider. [75] Further, while Québec's privacy legislation does not require notification to an individual in cross-border transfers, it does require organizations to take all reasonable steps to ensure that cross-border transfers of personal information will not be used for collateral purposes, nor communicated to third parties without the consent of the individuals concerned.

While the BC PIPA does not address cross-border transfers or the storage of information on remote servers, the BC Privacy Commissioner may still assess whether reasonable security measures were implemented in such transfers and consider whether individuals should be notified that their personal information was moved across borders.[76]

C. Representations and warranties

The due diligence phase also affords the acquirer the opportunity to evaluate the target's privacy

[73] The Federal Privacy Commissioner, *Guidelines for Processing Personal Data Across Borders*, January 2009, available at https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/. *See also* joint publication of the Federal, B.C. and Alberta Privacy Commissioners, *Cloud Computing for Small and Medium-sized Enterprises*, June 2012, available at: https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/online-privacy/cloud-computing/gd_cc_201206/.

[74] The Federal Privacy Commissioner, *Guidelines for Processing Personal Data Across Borders*, *supra* note 73. *See also* joint publication of the Federal, B.C. and Alberta Privacy Commissioners, *Cloud Computing for Small and Medium-sized Enterprises*, June 2012, available at https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/online-privacy/cloud-computing/gd_cc_201206/.

[75] AB PIPA, s. 13.1.

[76] BC PIPA, s. 34.

compliance and controls. Generally, the target provides representations and warranties stating that they are in compliance with all applicable privacy legislation as well as their own privacy policy. However, the acquirer should still thoroughly investigate whether or not the target has a privacy policy in place and whether it satisfies obligations under applicable privacy legislation.

The failure to satisfy privacy obligations is a potential liability, and an acquirer should evaluate the remedial measures that would be required to bring operations into compliance. The acquirer should also consider the types of data the target collects and stores, and look at the manner in which information is collected and stored and the process through which consents to use that information are obtained. If a third-party service provider is employed to manage the data, the service agreement and practices of the service provider should also be reviewed.

Acquirers often view the personal information collected by a target as an asset. However, it will need to be determined whether or not the acquirer will be able to use the information in the manner it intends to or whether they may be limited in the ways they can use and disclose this information.

D. Reducing transactional related privacy risks

By allowing an exception in the context of business transactions to the general rule that consent is required prior to the disclosure of personal information, parties to a business transaction avoid having to obtain the consent of every individual the organization may have personal information on. Yet this exception should not be taken to be an overarching or broad loophole. One alternative is to ensure that all necessary consent is obtained in advance through the organization's privacy policy by having the policy contemplate the collection, use, and disclosure of personal information during such transactions.

Suggested measures that could be taken by organizations in order to reduce privacy related risks include:

- implementing a privacy policy that contemplates the collection, use, or disclosure of "personal information" during business transactions and cross-border transactions;
- making information anonymous by removing any identifying information such as a person's name or address. Anonymous information is not "personal information;"
- only exchanging personal

information that is necessary for carrying out the business transaction (e.g., there will likely never be a reason to provide a social insurance number);
- if relying on implied consent under PIPEDA, ensuring that personal information is not sensitive;
- increasing protection through the use of confidentiality or non-disclosure agreements. Include provisions outlining procedures for destruction/return of personal information in the event the transaction is no longer pursued and address liability, notification and cooperation in the event of a data breach;
- ensuring adequate contractual provisions are in place to protect personal information;
- ensuring the necessary representations and warranties are provided. Indemnification clauses should be included in respect of representations or warranties relating to the protection of personal information; and
- outlining the process for transfer of personal information in the purchase and sale agreement.

IV. Data Breach

A. Principles

1. Federal Law

PIPEDA and other Federal laws do not explicitly provide notification requirements in the event of data breach. However, the Digital Privacy Act includes an amendment to PIPEDA that, upon coming into effect, will bring about mandatory data breach notification requirements.[77] Once these regulations are promulgated, the notification requirements will come into effect.

Organizations will be required to report any breach of security safeguards involving personal information under their control to the Federal Privacy Commissioner and the affected individuals. This notification will be required where it is reasonable to believe the breach creates a real risk of significant harm to an individual. Such a report must be made "as soon as feasible after the organization determines

[77] The Government of Canada, *For Discussion — Data Breach Notification and Reporting Regulations*, March 4, 2016, available at http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11177.html.

that the breach has occurred."[78] Organizations will also be required to notify a potentially affected individual of such breach, using a similar threshold.

An organization experiencing a breach will have additional reporting obligations to other organizations and government institutions if the breached organization believes the other organizations may be able to reduce their risk of harm as a result.

The Digital Privacy Act introduces liability for knowingly violating the notification requirements. An organization may be liable for fines up to CAD$100,000 per violation. It is unclear at this time whether a "violation" will include a single incident (e.g. a single failure to notify all individuals) or each incident (e.g. each failure to notify each individual).

Until statutory requirements come into force, organizations should follow the Federal Privacy Commissioner's guidelines.[79] These guidelines encourage organizations to report material privacy breaches to the appropriate privacy commissioner(s), and to notify affected individuals, as part of the efforts to mitigate the impact of the breach. The guidelines identify four key steps in responding to a breach of security:

(a) breach containment and preliminary assessment;
(b) evaluation of the risks associated with the breach;
(c) notification; and
(d) prevention of future breaches.

2. Provincial Law

In Alberta, organizations must notify the Commissioner in the case of a loss, unauthorized access, or disclosure.[80] Such notification to the Commissioner should occur without unreasonable delay. The Commissioner may require the organization to notify the affected individuals within a specified period of time.[81] Failure to notify the Commissioner may result in a fine of up to CAD$10,000, and in the case of an organization, a fine of up to CAD$100,000.[82] Neither BC PIPA nor the Québec Act make breach reporting mandatory.

---

[78] PIPEDA, s. 10.1(2).

[79] The Federal Privacy Commissioner, *Key Steps for Organizations in Responding to Privacy Breaches*, 2007, available at https://www.priv.gc.ca/media/2086/gl_070801_02_e.pdf. *See also* Office of the Information and Privacy Commissioner, Alberta, *How to Report a Privacy Breach*, available at https://www.oipc.ab.ca/action-items/how-to-report-a-privacy-breach.aspx.

[80] The AB PIPA, s. 34.1(1).

[81] The AB PIPA, s. 37.1.

[82] The AB PIPA, s. 59.

B. An organization's obligations to non-Canadians

The Federal Privacy Commissioner observes that organizations subject to PIPEDA may collect personal information that pertains to individuals who reside outside of Canada (for instance, residents of the United States). The Federal Privacy Commissioner is of the view that notification and reporting obligations require a consideration of the extent to which organizations may have to notify individuals outside of Canada who may be affected by a data breach undergone by an organization subject to PIPEDA. At a minimum, the Federal Privacy Commissioner suggests that regulations should require organizations to consider the breach notification laws of those jurisdictions, as well as any local notification requirements.

V. Conclusion

The combination of federal and provincial privacy laws and CASL regulate the manner in which organizations collect, use, and disclose personal information in the course of their business operations and are intended to protect personal information in the course of commercial activities. These laws can have a significant impact on organizations operating in Canada. The legislation includes robust enforcement mechanisms and authorizes governmental agencies to impose significant financial penalties, which can bring scrutiny and negative publicity to organizations found to be in breach of their obligations. Organizations would be well served by implementing policies and strategies that ensure compliance with these laws.