# Canadian Privacy Law Review

VOLUME 16, NUMBER 1 Cited as (2018), 16 C.P.L.R. DECEMBER 2018

## • BREACH NOTIFICATION RULES UNDER GDPR, PIPEDA AND PIPA •

Stephen D. Burns, Partner and Trademark Agent, J. Sébastien A. Gittens, Partner and Trademark Agent, Martin P.J. Kratz QC, Partner and Trademark Agent, and Kees de Ridder, Associate



**Stephen D. Burns**

**J. Sébastien A. Gittens**

**Martin P.J. Kratz**

**Kees de Ridder**

### • In This Issue •



LexisNexis®

**The** breach notification obligations for Canadian organizations will change significantly in 2018: (i) the European Union's *General Data Protection Regulation* (GDPR) came into force on May 25, 2018; while (ii) new reporting obligations under Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) will come into force on November 1, 2018. To assist Canadian organizations with their potential compliance efforts with respect to same, the following is intended to provide a non-exhaustive, high-level comparison between: (i) the GDPR; (ii) PIPEDA; together with (iii) the *Personal Information Protection Act* of Alberta (PIPA). While there are important nuances to each of these regulatory frameworks, they broadly draw on fair information practices that result in substantial commonality among them. In fact, a number of elements in Canadian private sector privacy law, especially in the PIPA, have anticipated some provisions in the GDPR.

## CANADIAN PRIVACY LAW REVIEW

**Canadian Privacy Law Review** is published monthly by LexisNexis Canada Inc., 111 Gordon Baker Road, Suite 900, Toronto ON M2H 3R1 by subscription only.





**ISBN 0-433-44417-7 (print) ISSN 1708-5446**
**ISBN 0-433-44650-1 (PDF) ISSN 1708-5454**
**ISBN 0-433-44418-5 (print & PDF)**

Subscription rates: $325.00 per year (print or PDF)
$495.00 per year (print & PDF)

Please address all editorial inquiries to:

**General Editor**
Professor Michael A. Geist
Canada Research Chair in Internet and E-Commerce Law
University of Ottawa, Faculty of Law
E-mail: mgeist@uottawa.ca

**LexisNexis Canada Inc.**
Tel. (905) 479-2665
Fax (905) 479-2826
E-mail: cplr@lexisnexis.ca
Web site: www.lexisnexis.ca




This article focuses on breach notification requirements. For a more general comparison of these enactments, please see our companion piece here.

| | GDPR | PIPEDA | PIPA |
|---|---|---|---|
| What event triggers the obligation? | Any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data that has been transmitted, stored, or otherwise processed is subject to the breach reporting rules. | A breach of security safeguards involving personal information is subject to the breach reporting rules. | Any incident involving the loss of or unauthorized access to or disclosure of personal information is subject to the breach reporting rules. |
| Is there a threshold standard when reporting is mandatory? | Notification must be given unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. | An organization must report any breach of security safeguards involving personal information if it is reasonable to believe that the breach creates a real risk of significant harm to an individual. | Notification of a breach must be given where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss, or unauthorized access or disclosure. |
| Does the law define factors that influence the risk or harm? | No. | Definition: "significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property".<br>Factors indicating a real risk of significant harm are the sensitivity of the personal information involved in the breach; and the probability that personal information has been, is being or will be misused. | No. |
| Does the law define how quickly one must report? | The processor shall notify the controller without undue delay after becoming aware of a personal data breach. | The notification must be given as soon as feasible after the organization determines that the breach has occurred. | Notification must be given without unreasonable delay. |

| | GDPR | PIPEDA | PIPA |
|---|---|---|---|
| | The controller shall, within 72 hours of becoming aware of a breach, notify the supervisory authority. Where notification is not made within 72 hours, reasons must be given for the delay. When it would cause undue delay to provide the required information at the same time, the information may be provided in phases. | | |
| Reporting to the commissioner? | Controllers must notify the supervisory authority of the given EU member state. | Yes, to the federal Privacy Commissioner (in this column, the "Commissioner"). | Yes, to the provincial Information and Privacy Commissioner (in this column, the "Commissioner"). |
| Does the law prescribe what must be reported to the commissioner? | The notice must contain:<br>(a) a description of nature of personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;<br>(b) the name and contact details of the data protection officer or other contact person;<br>(c) a description of the likely consequences of the personal data breach; and<br>(d) a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate possible adverse effects. | The notice must contain:<br>(a) a description of the circumstances of the breach;<br>(b) the day on which, or the period during which, the breach occurred;<br>(c) a description of the personal information involved in the breach;<br>(d) an estimate of the number of individuals to whom there is a real risk of significant harm;<br>(e) a description of any steps the organization has taken to reduce the risk of harm;<br>(f) a description of any steps the organization has taken to notify individuals of the breach; and<br>(g) the name of and contact information for a person who can | The notice must contain:<br>(a) a description of the circumstances of the breach;<br>(b) the day on which, or the period during which, the breach occurred;<br>(c) a description of the personal information involved in the breach;<br>(d) an assessment of the risk of harm to individuals as a result of the breach;<br>(e) an estimate of the number of individuals to whom there is a real risk of significant harm;<br>(f) a description of any steps the organization has taken to reduce the risk of harm;<br>(g) a description of any steps the organization has taken to notify individuals of the breach; and<br>(h) the name of and contact information for a person who can answer, on behalf |

| | GDPR | PIPEDA | PIPA |
|---|---|---|---|
| | | answer, on behalf of the organization, the Commissioner's questions about the breach. | of the organization, the Commissioner's questions about the breach. |
| What sanction arises if one fails to report to the commissioner? | The supervisory authority of the given EU state may issue orders, warnings, or reprimands (including administrative fines) against a controller or processor. | It is an offence to fail to provide notice to the Commissioner, and may result in a fine of up to $100,000 for an organization.<br>The Court may order the organization to: correct its practices; and publish a notice of any action taken to correct its practices. | It is an offence to fail to provide notice to the Commissioner, and may result in a fine of up to $100,000 for an organization. |
| Reporting to the individual? | When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. | An organization shall notify an individual of any breach of security safeguards involving the individual's personal information under the organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual. | The Privacy Commissioner may require the organization to notify individuals' of the loss of their personal data. |
| Does the law address reporting to others? | No. | An organization that notifies an individual of a breach of security safeguards shall notify any other organization, including government institutions, of the breach if the notifying organization believes that the other organization concerned may be able to reduce the risk of harm. | No. |
| Does the law prescribe what must be reported to the individual? | The notice must include:<br>• a description, in clear and plain language, of the nature of the personal data breach; | The notice must include:<br>• a description of the circumstances of the breach; | The notice must include:<br>• a description of the circumstances of the breach; |

| | GDPR | PIPEDA | PIPA |
|---|---|---|---|
| | • the name and contact details of the data protection officer or other contact person;<br>• a description of the likely consequences of the personal data breach; and<br>• a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate possible adverse effects. | • the day on which, or period during which, the breach occurred;<br>• a description of the personal information that is the subject of the breach;<br>• a description of the steps that the organization has taken to reduce the risk of or mitigate any harm to the affected individual;<br>• a description of the steps that the affected individual could take to reduce the risk of or mitigate any harm resulting from the breach;<br>• a toll-free number or email address that the affected individual can use to obtain further information about the breach; and<br>• information about the organization's internal complaint process and about the affected individual's right, under PIPEDA, to file a complaint with the Commissioner. | • the date on which or time period during which the breach occurred;<br>• a description of the personal information involved in the breach;<br>• a description of any steps the organization has taken to reduce the risk of harm; and<br>• contact information for a person who can answer, on behalf of the organization, questions about the loss or unauthorized access or disclosure. |
| Does the law permit indirect notification of individuals? | Yes, provided that notifying the individual or individuals would involve "disproportionate effort". | Yes, provided that:<br>• direct notification would be likely to cause further harm to the affected individual;<br>• direct notification would be likely to cause undue hardship for the organization; or<br>• the organization does not have contact information. | Notification may be given to an individual indirectly if the Commissioner so allows. |

| | GDPR | PIPEDA | PIPA |
|---|---|---|---|
| What sanction arises if one fails to report to the individual? | The data subject has the right to:<br>• lodge a complaint with a supervisory authority;<br>• an effective judicial remedy against a controller or processor (where the supervisory authority does not handle the complaint within three months); and<br>• receive compensation for material or non-material damage suffered. | The Court may order the organization to:<br>• correct its practices, pay damages to the complainant, including damages for humiliation; and<br>• publish a notice of any action taken to correct its practices. | The Commissioner may make any order it considers appropriate.<br>The Court may order the organization to pay damages to the complainant for loss or injury. |
| Does the law mandate record keeping requirements? | The controller shall document any personal data breaches, including facts relating to the breach, its effects, and the remedial action taken. This documentation will allow the supervisory authority to verify compliance with the GDPR. | • Organizations must keep and maintain a record of every breach of security safeguards involving personal information under its control.<br>• Records must be kept for 24 months following the date the organization determines that the breach has occurred. | PIPA does not impose any specific requirements to keep records related to breaches. |
| Does the law contemplate exemptions to the notification responsibilities? | Notice to the individual is not required in any of the following circumstances:<br>• the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;<br>• the controller has taken subsequent measures which ensure that the | The organization is not required to notify the individual of a breach if doing so is prohibited by law.<br>The organization is not required to notify the Commissioner or the individual if it is not reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual. | The organization is not required to give notice to the Commissioner if there is no real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure of personal information.<br>The organization is not required to give notice to the individual unless so ordered by the Commissioner. |

| | GDPR | PIPEDA | PIPA |
|---|---|---|---|
| | risk to the rights of data subjects is no longer likely to materialize; or<br>• it would involve disproportionate effort, in which case there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner. | | |

**Bibliography**

*General Data Protection Regulation*, EU Reg. 2016/679.

*Personal Information Protection Act Regulation*, Alta. Reg. 366/2003.

*Personal Information Protection Act*, S.A. 2003, c P-6.5.

*Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [*PIPEDA*] (in force).

*PIPEDA* (pending amendments).

*PIPEDA* (pending regulations).

[***Stephen D. Burns*** *is a partner and trade-mark agent at Bennett Jones LLP.*

***J. Sébastian A. Gittens*** *is a partner and trade-mark agent at Bennett Jones LLP.*

***Martin P.J. Kratz QC, FCIPS*** *is a partner and trade-mark agent at Bennett Jones LLP.*

***Kees de Ridder*** *is an associate at Bennett Jones LLP.*]

## • UNDERSTANDING THE GDPR — COMPARING CONSENT PROVISIONS TO PIPEDA, PIPA AND CASL •

Stephen D. Burns, Partner and Trademark Agent, J. Sébastien A. Gittens, Partner and Trademark Agent, Martin P.J. Kratz QC, Partner and Trademark Agent, and Graeme S. Harrison, Associate



**Stephen D. Burns**

**J. Sébastien A. Gittens**

**Martin P.J. Kratz**

**The** European Union's General Data Protection Regulation (GDPR) came into force on May 25, 2018. To assist Canadian organizations with their potential compliance efforts with respect to this legislation, the following is intended to provide a non-exhaustive, high-level comparison between the consent provisions of:

1. the GDPR;
2. Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA);

3. the Personal Information Protection Acts of Alberta and British Columbia (collectively, the PIPAs); and
4. Canada's Anti-Spam Legislation (widely known as CASL).

While there are important nuances to each of these regulatory frameworks, they broadly draw on fair information practices that result in substantial commonality among them. In fact, a number of elements in Canadian private sector privacy law, especially in the PIPAs, have anticipated some provisions in the GDPR.

EXPRESS CONSENT

The Alberta and B.C. Privacy Commissioners have held that consent must be "meaningful" (*i.e.*, an individual must understand what an organization is doing with their information).

On or before collecting personal information about an individual, an organization must generally disclose to the individual verbally or in writing: (i) the purposes for the collection of the information; and (ii) the position name or title and the contact information of a person who is able to answer the individual's questions about the collection. Consent can also be implied or deemed in certain circumstances.

The PIPAs provide that an organization shall not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information about an individual beyond what is necessary to provide the product or service.

Canada's privacy regulators plan to adopt new guidelines applicable to meaningful consent as of January 1, 2019.

| GDPR | PIPEDA | PIPAs | CASL |
|---|---|---|---|
| Express consent is generally required to control or process personal data, except in certain circumstances. Consent means any freely given, specific, informed and unambiguous indication of an individual's wishes which, by a statement or by a clear affirmative action, signifies an agreement to the processing of their personal data. | Consent is generally required for the collection, use or disclosure of personal information. Consent can be express, implied or deemed. Express consent is only valid if it is reasonable to expect that an individual would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting. | The Alberta and B.C. Privacy Commissioners have held that consent must be "meaningful" (*i.e.*, an individual must understand what an organization is doing with their information). On or before collecting personal information about an individual, an organization must generally disclose to the individual verbally or in writing: (i) the purposes for the collection of the information; and (ii) the | CASL provides that a sender must hold the consent of a recipient in order to send the recipient a commercial electronic message (CEM), unless the CEM is exempt. Consent can be express or implied/deemed under CASL. Unlike the principle-based forms of express consent under privacy statutes, CASL sets out various formalities that must be met in order for an express consent to be valid, including certain informational disclosures that must be made at the time |

| GDPR | PIPEDA | PIPAs | CASL |
|---|---|---|---|
| The GDPR provides that, when assessing whether consent is freely given, "utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract". | PIPEDA provides that an organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes. Canada's privacy regulators plan to adopt new guidelines applicable to meaningful consent as of January 1, 2019. | position name or title and the contact information of a person who is able to answer the individual's questions about the collection. Consent can also be implied or deemed in certain circumstances. The PIPAs provide that an organization shall not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information about an individual beyond what is necessary to provide the product or service. Canada's privacy regulators plan to adopt new guidelines applicable to meaningful consent as of January 1, 2019. | consent is collected. The purpose for which an organization seeks consent must be clearly set out, with consent limited to that purpose. Express consent under CASL may be obtained orally or in writing. CASL puts the onus of proof upon an organization alleging that it holds express consent, obligating an organization to put forward evidence in its own favour or face regulatory consequences. CASL provides that a request for express consent is a CEM and therefore cannot be sent without consent. |

IMPLIED/DEEMED CONSENT

| GDPR | PIPEDA | PIPAs | CASL |
|---|---|---|---|
| The GDPR provides that the control or processing of personal data is lawful absent express consent in certain circumstances analogous to implied/ deemed consent under PIPEDA and the PIPAs. For example, where processing of personal data is necessary for the performance of a contract to which the data subject is party, such processing is lawful even absent express consent. | PIPEDA recognizes that consent may be implied or deemed in certain cases. PIPEDA recognizes the validity of opt-out consent by way of pre-checked boxes in certain situations. PIPEDA permits organizations to rely on implied or deemed consent depending on the circumstances, for example the reasonable expectations of individuals who | The PIPAs recognize that consent may be implied or deemed in certain cases. Under the PIPAs, an individual is deemed to consent to the use, collection or disclosure of personal information for a particular purpose where the individual voluntarily provides information to an organization for such purpose, and it is reasonable that such person would | Unlike the principle-based forms of express consent under privacy statutes, CASL recognizes implied/deemed consent only in certain limited prescribed cases. Under CASL, implied consent arises where a sender and recipient have an existing business relationship or an existing non-business relationship. CASL provides that specific factual circumstances must exist in order for either of these relationships to form. CASL recognizes a limited form of |

| GDPR | PIPEDA | PIPAs | CASL |
|---|---|---|---|
| | purchase goods or services. | voluntarily do so, among other situations. The PIPAs recognize implied consent in various situations, including certain situations where an organization gives an individual notice of an intent to collect, use or disclose personal information, and the individual does not object after being given a reasonable opportunity to do so. | implied consent where an individual discloses or publishes an electronic address without a disclaimer–note that this kind of implied consent is subject to certain restrictions on content. CASL recognizes a limited form of deemed consent in specific circumstances related to referrals. This consent can only be used once before it expires. CASL permits the holder of an express consent to share it with third parties in certain circumstances. |

EXCEPTIONS TO CONSENT

| GDPR | PIPEDA | PIPAs | CASL |
|---|---|---|---|
| The GDPR provides that there are exceptions from the requirement for consent in certain circumstances, including compliance with legal obligations and for the performance of official duties. | PIPEDA also provides that there are exceptions from the requirement for consent in certain circumstances, including compliance with legal obligations and for law enforcement purposes. | The PIPAs also provide that there are exceptions from the requirement for consent in certain circumstances, including compliance with legal obligations and for law enforcement purposes. | CASL and its regulations create a variety of exceptions to the consent requirement, including for CEMs sent by a registered charity for the primary purpose of fundraising. |

[***Stephen D. Burns*** *is a partner and trade-mark agent at Bennett Jones LLP.*

***J. Sébastian A. Gittens*** *is a partner and trade-mark agent at Bennett Jones LLP.*

***Martin P.J. Kratz QC, FCIPS*** *is a partner and trade-mark agent at Bennett Jones LLP.*

***Graeme S. Harrison*** *is an associate at Bennett Jones LLP.*]

# • PROTECTING YOUR SOCIAL MEDIA PROFILE: HOW ONE NEW ZEALAND TECHNOLOGY COMPANY ALLEGEDLY VIOLATED CANADIAN PRIVACY LAW •

Carole J. Piovesan, Associate, Akiva Stern, Articling Student, McCarthy Tetrault


**Carole J. Piovesan**

**Akiva Stern**

**On** June 12, 2018, the Office of the Privacy Commissioner of Canada (the "OPC") issued a report relating to allegations against Profile Technology Ltd. ("PTL"), a New Zealand-based company, concluding that PTL imported millions of Canadian Facebook users' profiles in violation of Canadian privacy law, to bolster its own social media platform called The Profile Engine.

## OVERVIEW

The OPC's report came about as a result of five complainants who sought help from the office to have their personal information removed from the website. The main issues are:

1. PTL was using personal information posted to Facebook, pursuant to a data sharing agreement between PTL and Facebook. Issues with data accuracy were key; and
2. the process of deleting data from PTL's site was opaque and overly cumbersome.

The OPC's report finds the complaints well-founded as violations of Canada's *Personal Information Protection and Electronic Documents Act* (the "*Act*" or "*PIPEDA*"),[1] as well as the *Regulations Specifying Publicly Available Information* (the "Regulations").[2]

## CONSENT AND COLLECTION

PTL asserted that its agreement with Facebook provided it unlimited access to user data; data that users had 'consented' to make public and accessible.

The OPC found this to be a violation of sections 7(1)(d) and 7(2)(c.1) of the *Act* that state that a company can use and collect personal information if "the information is publicly available and is specified by the regulations".[3] Sections 1(e) of the Regulations specify that "personal information that appears in a publication, including a magazine, book or newspaper, in printed or electronic form, that is available to the public, where the individual has provided the information"[4] is considered fair game for collection.

The OPC outright rejected the assertion that personal profiles are "publically available". They note that Facebook profiles are "ever-changing" and are subject to user's personal privacy settings.

## ACCURACY OF INFORMATION AND RETENTION

The complainants claimed that the information they found on PTL's website was either never accurate or "inaccurate by virtue of being out of date". While Facebook's profiles would constantly update and change over time through its active users, PTL's information would be dated from when the user data was pulled in order to populate their site with information, but without corresponding users to keep them up to date.

The OPC took issue not only with the cumbersome process users were required to go through to attempt to delete inaccurate profile information, but also that the PTL helpdesk maintained personal information indefinitely. The OPC found this to be a violation

of section 5(3) of the *Act*, which states that "an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances".[5] It is the opinion of the OPC that keeping information that is inaccurate or maintaining helpdesk data longer than needed to help the user is unreasonable.

OPC'S RECOMMENDATIONS

In its Preliminary Report of Investigation (PRI), the OPC recommended the following two measures:

1. "Remove from its website, and delete from its records, all individual profiles and groups associated with any Canadian (or Canadians), including those associated with the complainants. In order to respect any choices Canadians have made to use the respondent's social networking services, this recommendation would not apply to those profiles or groups that were: (i) created by an individual independently on the website; or (ii) claimed by an individual, where the individual has not also requested its deletion; and
2. Introduce a retention policy for its helpdesk system information, which includes a reasonable retention period for personal information, and delete helpdesk tickets that are past this reasonable retention period."

In response to the PRI, PTL has begun making changes to its website. It has removed, anonymized and archived millions of profiles. The archives are still accessible but the ability to use search engines for the data has ceased.

Despite these changes, the OPC still maintains its concerns so long as the data is not destroyed completely. According to the OPC, the threat of commercializing this user data is still a live issue.

GOING FORWARD

Data governance is an increasingly critical aspect of risk mitigation in a data-driven economy. It is important for companies to conduct an assessment of existing data to determine regulatory compliance as well as data monetization opportunities. Classifying information for ease of access, deleting duplicate or outdated records, and creating the policies and procedures to manage information responsibly is not only part of a good corporate governance system, but is also important to risk mitigation as well as revenue-generation opportunities.

1 S.C. 2000, c. 5 [*PIPEDA*].
2 SOR/2001-7 [*Regs*].
3 *PIPEDA*, note 1, s. 7(1)(d) and 7(2)(c.1).
4 *Regs,* note 2, s. 1(e).
5 *PIPEDA*, note 1, s. 5(3).

## • YOUR 10-STEP GUIDE TO NEW MANDATORY BREACH REPORTING REGULATIONS •

Ruth E. Promislow, Partner, and Katherine Rusk, Associate, Bennett Jones LLP,



**Ruth E. Promislow**


**Katherine Rusk**

10-STEP GUIDE TO NEW MANDATORY BREACH REPORTING REGULATIONS

**This** 10-step guide will walk you through the upcoming changes to the *Personal Information Protection and Electronic Documents Act* (PIPEDA), the factors to consider in being prepared under PIPEDA and other related considerations. This guide is no replacement for targeted legal advice. If you are an organization

affected by the changes to PIPEDA, please contact us to determine what you need to do to be prepared and how you can minimize your organization's potential legal exposure. There is no "one size fits all" when it comes to managing compliance with privacy regulation. The biggest changes, which will be **came into force on November 1, 2018**, are:

1. Mandatory breach reporting to the Office of the Privacy Commissioner (OPC).
2. Mandatory breach notification to impacted individuals.
3. Mandatory breach record-keeping.
4. Financial penalties of up to $100,000 for non-compliance with items 1 to 3.

## BACKGROUND

**PIPEDA applies to the collection, use or disclosure of *personal information* in the course of a *commercial activity.*** 1 **Personal information** includes any factual or subjective information about an identifiable individual. Information will be about an "identifiable individual" when there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information. Examples include: email addresses, credit card numbers, name, the contents of a safe deposit box, financial records, biometric records, and information collected through GPS or RFID chips.

A **commercial activity** is conduct that is of a commercial character (including the selling, bartering or leasing of donor, membership or other fundraising lists). PIPEDA does not generally apply to: business contact information; information used by an individual for only personal purposes; information used only for journalistic, artistic or literary purpose; information about an employee if it is not used or disclosed in connection with the operation of a federal work, undertaking or business; information handled by municipal, provincial, territorial, or federal governments; municipalities, universities, schools, and hospitals (they are covered by provincial laws); or political parties, political associations, charities or not-for-profits unless they are engaging in commercial activities that are not central to their mandate.

## STEP 1: IDENTIFY WHAT INFORMATION YOU HAVE

### Primary Considerations

Identify categories of **personal information** for which your organization is responsible and which of those fall within the scope of PIPEDA. Not all information falls within the same degree of sensitivity. Consider what information is high-risk. For example, financial and medical records have been considered as very sensitive by the OPC. Was the personal information collected by fair and lawful means? Do you have documentation on why the personal information was collected? Do you have documentation of the individuals' consent? The purpose for which the personal information is being collected must be identified by the organization before or at the time of collection. The collection and use of information must be limited to the identified purpose. Consider whether you **need** the personal information you are gathering. If not required to fulfill the identified purpose, information should be destroyed, erased or made anonymous. Develop guidelines and implement procedures to govern destruction of personal information.

### Other Considerations

Does your organization have personal information affected by the legislation in other jurisdictions? For example, if your organization offers goods or services to, or monitors the behaviour of, EU data subjects, the General Data Protection Regulation (GDPR) may apply. Non-compliance with the GDPR can result in administrative fines of up to €20 million or 4% of annual worldwide turnover (whichever is higher). Does your organization have any contractual obligations with third parties should there be any incident affecting any category of confidential information? If a consumer or individual calls and requests access to their information, can you give it to

them in a timely manner? Is the personal information as accurate, complete, and up-to-date as possible?

## STEP 2: UNDERSTAND HOW INFORMATION IS STORED

### Primary Considerations

Understand where and how the personal information is stored and the means by which it could be accessed.

### Other Considerations

Limit internal access to those employees who require access in order to carry out the purpose for which the information was collected.

## STEP 3: IMPLEMENT SAFEGUARDS TO PROTECT YOUR INFORMATION

### Primary Considerations

Implement safeguards appropriate to the sensitivity of the information, including:

1. **Physical measures** (e.g., locked filing cabinets; restricted access to offices).
2. **Organizational measures** (e.g., security clearances and limiting access on a "need to know" basis).
3. **Technological measures** (e.g., use of passwords and encryption).

Make employees aware of importance of maintaining confidentiality of personal information —develop, document and deliver appropriate and mandatory privacy training for all employees. Use care in disposal or destruction of personal information. For example, are your printers wiped before they are thrown out?

### Other Considerations

Implement measures so that your organization can detect unauthorized access to or disclosure of personal information. A failure to implement any detection measures may expose an organization to an invader without even knowing about it. Are your security measures regularly reviewed and updated?

## STEP 4: ENSURE THIRD-PARTY CONTRACTS PROTECT YOU

### Primary Considerations

*Contracting third parties to process personal information on your behalf does not relieve you of responsibility under PIPEDA.*

Have a recorded basis for selecting the third-party vendor and for your satisfaction that they have appropriate safeguards in place. Contractual provisions with third parties should identify items such as:

1. Their obligation to safeguard the personal information.
2. Their obligation to notify you about security incidents.
3. Your ability to oversee and potentially audit their operations as it concerns the personal information they process on your behalf.
4. Who bears the burden of the costs associated with a data security incident.

### Other Considerations:

When the contract is completed, ensure the information is returned or disposed of. Limit all information sent to the third party to that required for the fulfilment of the contract. Consider requiring certification of cyber hygiene from a third party. Consider requiring insurance for data breaches as part of any contract.

If there is a data security incident, can your third party afford to deal with the resulting costs or will they fold and leave you hanging?

## STEP 5: INSTITUTE BREACH RESPONSE PLAN

### Primary Considerations

Who will be informed of a data security incident? A security breach response team typically includes someone from: counsel (external and internal); information technology; security; communications/ media relations; executive team; and privacy/ compliance. How will your team be informed of

the breach? Specific mechanisms of notification for each team member should be instituted. Identify responsibilities of each team member in managing incident and response to that incident. Are there "understudies" available if one of your team is unavailable? Your plan should include: procedures for analyzing a potential data security incident; procedures for containing a potential data security breach; procedures for remediation measures following a data security breach; insurance information; plan for notifications; and counsel contact information.

### Other Considerations

Are there backups of all of your business information? What if…

1. You're locked out of your email?
2. The data security incident happens during off hours or on a holiday?
3. You're locked out of your network?

## STEP 6: EVALUATE FOR A REAL RISK OF SIGNIFICANT HARM

### Primary Considerations

*Was there a breach of security safeguards?*

Breach of security safeguards means loss of, unauthorized access to, or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards or from failure to establish those safeguards (see Step 3).

*If so, is there a real risk of significant harm?*

"Significant harm" includes: humiliation, damage to reputation or relationships and identity theft. When analyzing whether there is a real risk of significant harm, look at what personal information has been breached and the circumstance through the following factors:

*1. The sensitivity of the personal information involved in the breach.*

Some information (SIN, health information, income records, etc.) are almost always considered to be sensitive information. Some information can be sensitive depending on the context. For example, a subscription to a news magazine would not be considered sensitive, but a subscription to certain special interest magazines might be. Look at the harms that can be accrued to the individual to determine sensitivity.

*2. The probability that the personal information has been, is being, or will be, misused.*

Ask yourself the following questions, for example:

What happened? How likely is it that someone would be harmed by the breach? Who actually accessed or could have accessed the personal information? How long has the personal information been exposed? Is there evidence of malicious intent? Were a number of pieces of personal information breached? Is the breached information in the hands of an individual/ entity that represents a reputational risk to the individual(s) in and of itself? Was the information exposed to limited/ known entities who have committed to destroy and not disclose the data? Was the information exposed to individuals/entities who have a low likelihood of sharing the information in a way that would cause harm? Was the information exposed to individuals/ entities who are unknown, or to a large number of individuals, where certain individuals might use or share the information in a way that would cause harm? Is the information known to be exposed to entities/ individuals who are likely to attempt to cause harm with it? Has harm materialized (demonstration of misuse)? Was the information lost, inappropriately accessed or stolen? Has the personal information been recovered? Is the personal information adequately encrypted, anonymized or otherwise not easily accessible?

**Consult external legal counsel to determine if security incident needs to be reported if it is in grey zone. Consult external legal counsel on content of**

**assessment as it may have legal implications for the organization.**

## STEP 7: MAINTAIN PRIVILEGE

### Primary Considerations

Your written assessment of whether the security incident gives rise to a real risk of significant harm can have legal implications for your organization, and may be producible in investigations or litigation concerning this event or future events. Maintain privilege through correspondence with external counsel with respect to the written assessment of whether there is breach of security safeguards that has given rise to a real risk of significant harm. Correspondence with in-house counsel is not always protected by solicitor-client privilege.

## STEP 8: RECORD ALL BREACHES

### Primary Considerations

You must maintain a record of every breach of security safeguard for at least 24 months after the date on which your organization learned of the breach. This record can be requested by the Office of the Privacy Commissioner. Record all breaches of personal information under your control — whether there is a real risk of significant harm or not.

The record should include:

1. date or estimated date of the breach;
2. general description of the circumstances of the breach;
3. nature of information involved in the breach;
4. whether or not the breach was report to the Privacy Commissioner of Canada/individuals were notified;
5. if the breach was not reported to the Privacy Commissioner/ individuals, a brief explanation of why the breach was determined not to pose a "real risk of significant harm"; and
6. the individual responsible for report.

### Other Considerations

Appoint one specific senior individual (e.g., CEO or privacy officer) to record the information and maintain the breach. Keep the board of directors apprised of management of security events. Consider issues of privilege when reporting to the board as the board minutes may be producible in litigation or investigations concerning this event or future events. If cybersecurity incidents or risks materially affect a company's products, services, relationships or competitive conditions, publically traded companies must provide appropriate disclosure. The breach record may have legal implications as it may be producible in investigations or litigation concerning this event or future events. Consider consulting external counsel.

## STEP 9: REPORTING AND NOTIFICATION OBLIGATIONS

Non-compliance with the notification obligations listed below can result in: The court ordering an organization to correct its practices, pay damages to the complainant, including damages for humiliation; and publish a notice of any action taken to correct its practices.2 Fines of up to $100,000.

### Office of the Privacy Commissioner

Report to the Office of the Privacy Commissioner as soon as feasible after you have determined a breach involving a real risk of significant harm has occurred.

The report must contain prescribed elements such as:

1. a description of the circumstances of the breach;
2. the date of the breach;
3. a description of the personal information involved;
4. an estimate of the number of individuals impacted;
5. a description of any steps the organization has taken to reduce the risk of harm;
6. a description of any steps the organization has taken to notify individuals of the breach; and
7. the name of and contact information for a person who can answer the Commissioner's questions about the breach.

**Consult external legal counsel on content of report as it may have legal implications for organization.**

### Affected Individuals

Notify affected individuals. The notification must include certain prescribed elements, including:

1. a description of the breach;
2. the date of the breach;
3. a description of the personal information that is the subject of the breach;
4. the steps that the organization has taken to reduce the risk of or mitigate any harm to the affected individual;
5. the steps that the affected individual could take to reduce the risk of or mitigate any harm; and
6. a toll-free number or email address that the affected individual can use to obtain further information. The notification can be provided in any "reasonable" manner, including in person, by email, or by telephone. Some exemptions for broader notifications (eg newspaper ads) instead of individually addressed notification are possible in certain circumstances.

**Consult external legal counsel on content of report as it may have legal implications for the organization.**

The organization is not required to notify the individual of a breach in some specific circumstances (e.g., if doing so is prohibited by law).

### Organizations That Can Help Mitigate Harm

Notify any institutions or organizations that you believe can reduce the risk of harm that could result from the breach or mitigate the harm.

For example:

1. notify law enforcement; and
2. notify everybody who processes your payments, including your payment processor or acquiring bank in the case of a breach affecting individual.

**Consult external legal counsel on content of notification as it may have legal implications for organization.**

## STEP 10: REVIEW AND LEARN

### Primary Consideration:

Once the crisis is past, take this opportunity to review your operations. Look for areas of weakness and areas that can be improved for the next breach.

Notes:

1. With respect to organizations that are not a federal work, undertaking or business, PIPEDA does not apply with respect to the collection, use or disclosure of personal information occurring within British Columbia, Alberta or Québec, as each of those provinces have privacy legislation that has been deemed substantially similar to PIPEDA. Several other provinces have health information privacy legislation that have been deemed substantially similar to PIPEDA. PIPEDA does not apply to employee information if it is not a federal undertaking, but other provincial legislation may apply.
2. In certain circumstances, the Federal Court may order an organization to correct its privacy practices and award damages to a complainant as a private right of action.

[***Ruth E. Promislow*** *is a partner at Bennett Jones LLP.*

***Katherine Rusk*** *is an associate at Bennett Jones LLP.*]