Ensuring Adequate Protection of Employee and Client Data under Canadian Privacy Statutes in the Course of International Commercial Activity

Newsletter - TerraLex Connections

Ensuring Adequate Protection of Employee and Client Data under Canadian Privacy Statutes in the Course of International Commercial Activity

By Christopher Deehy and Sophie Roy-Lafleur*

Introduction

With the advent of information technology and the collection of data, Canadian statutes have been enacted and progressively adapted to protect personal information in the private sector. These statutes have been designed to account for progressive increases in sensitive employee data in the hands of employers and their human resources departments and the collection of consumer data. In some cases, foreign companies can themselves be held liable under this legislation for making use of Canadian consumer data. Foreign businesses interested in trading with Canadian companies are often contractually bound to comply with this legislation, by establishing practices and safeguards, as Canadian businesses can be held accountable for foreign use of Canadian employee and consumer data.

The personal information of Canadian employees collected, used, or disclosed in the course of commercial activities [1] is protected when the business is under the federal government's exclusive constitutional jurisdiction, referred to as *"Federal Works Undertakings or Businesses"* ("federally regulated business"); [2]

The provinces of Alberta, British Columbia and Quebec have enacted comprehensive "substantially similar" privacy legislation. [3] These provincial privacy statutes protect employee information collected, used, or disclosed in the course of commercial activities, by provincially regulated businesses.

In the seven provinces without substantially similar privacy legislation [4], the personal information of employees is not protected by PIPEDA or a provincial privacy statute. [5] However, companies may still be held liable at Common Law for breaching an individual's privacy rights in these provinces. [6] Therefore, even in such cases, best practices would be to implement the safeguards discussed herein below.

The personal information of Canadian consumers is protected by PIPEDA in the course of commercial activities if it is held by a federally regulated business. PIPEDA also protects the information of any Canadian consumer disclosed in the context of international or interprovincial commercial activities.

Consumer information will also be protected under PIPEDA if commercial activity undertaken by a provincially regulated business takes place within one of the seven provinces in which no "substantially similar" provincial privacy legislation is in force. The provincial privacy statutes protect the personal information of consumers held by provincially regulated businesses in the course of commercial activity undertaken within Alberta, British Columbia, and Quebec.

Application of PIPEDA to the personal information of Canadian consumers collected by foreign businesses

When a foreign business collects the personal information of Canadian consumers, who are themselves within Canada, that business may be subject to the provisions of PIPEDA if it has a "real and substantial connection" to Canada, even if it does not have a physical establishment or employees in Canada.

When a foreign corporation extensively markets to Canadian consumers, such as a foreign online retailer or social messaging service, despite having no physical presence in Canada, the Office of the Privacy Commissioner ("OPC") may have jurisdiction to investigate its activities when a complaint is filed against it.

For example, in a 2013 Case, the OPC initiated a complaint against WhatsApp, an American instant messaging service. The OPC found that it had jurisdiction to investigate the foreign cloud-based instant messaging application as it actively promoted and distributed its services to Canadian consumers, and was widely used by Canadians. [7]

Personal information protected by PIPEDA

When PIPEDA applies, only personal information in respect of an identifiable individual is protected. Information is "personal" when there is a serious possibility that it could be used, alone or combined with other information, to identify a specific individual, though it can include publicly available information and does not necessarily need to be accurate. Examples of protected personal information include: age, name, ID numbers (such as a social security number), income, ethnic origin, blood type, opinions, evaluations, comments, social status, disciplinary actions, employee files, credit records, loan records, and medical records.

PIPEDA does not restrict disclosure of an employee's business contact information, (such as a professional phone number, name, title, or work address), if

that information is used to communicate with that person in the course of their employment. [8] However, PIPEDA protects that information in contexts unrelated to facilitating communication between an employee and the business's employer or clients. [9]

Restricted purposes for making use of employee data

As a general rule, PIPEDA prohibits organizations and employers subject to it from disclosing, using, and collecting the protected personal information of employees for purposes that a reasonable person would not consider appropriate in the circumstances. [10]

To determine if an employer was justified in collecting, using, or disclosing the personal information of an employee, the OPC performs a "proportionality test." The OPC considers the employer's purpose for collecting the employee's personal information and the circumstances surrounding that purpose. [11] It then assesses whether or not the measure was demonstrably necessary to meet a specific need, if the measure was likely to effectively meet that need, if the loss of privacy was proportionate to the benefit gained, and if there was a less privacy invasive way to reach the same end. [12]

However an employer may be permitted to use, collect, or disclose any employee's personal information, without their knowledge or consent, if it was produced by the employee in the course of their employment, as long as its use is consistent with the purposes for which the information was produced. [13]

The collection, use, or disclosure of an employee's personal information may be undertaken without the employee's consent if it is necessary to establish, manage, or terminate his or her employment. However, in such a case the employee must be notified that the information may be collected, used, or disclosed for that purpose. [14]

Complaint process

If an organization collects, uses, or discloses information in a manner that breaches PIPEDA, an employee or client may submit a complaint against it to the OPC. [15] Within one year of the complaint, the OPC must either discontinue its investigation, or apply to the Federal Court for a hearing on the matter. If the complaint has been discontinued, the complainant may nevertheless apply to the Federal Court for a hearing on the complaint. [16]

Even if no complaint has been submitted against a corporation, the OPC may on its own initiate the complaint process when it has "reasonable grounds" to do so. [17]

The Federal Court may order the organization to rectify its conduct to comply with PIPEDA and award damages to the complainant. [18]

Data protection in the context of international business transactions and commercial activity

PIPEDA is an exceptional law as it has an extra-territorial reach. Consequently, it applies when a third party outside of Canada receives Canadian personal information protected under PIPEDA for processing. [19] An organization that has disclosed or transferred the personal information of Canadians to a foreign third party for processing can be held responsible by the Federal Court of Canada for data breaches caused by the third party. Under PIPEDA, the transfer of private information across borders is not expressly prohibited; however, an organization remains responsible for information wherever it is located. [20]

In June 2015, PIPEDA was amended to limit certain protections in the context of national and international business transactions, to encourage trade and facilitate the due diligence process. [21] A business transaction includes: the purchase or sale of shares or assets, mergers, amalgamations, loans, creating a charge or security, financing, leasing, and licensing. [22]

A federally regulated employer that wishes to disclose the personal information of employees without their consent in the context of business transactions must satisfy certain conditions to avoid being held liable. For such exceptions to apply, the transfer of personal information cannot be the primary purpose of the transaction. [23]

These exceptions apply at two stages in the process of a business transaction:

(1) Prior to the transaction occurring the parties may use and disclose the personal information of employees without their knowledge or consent.

Conditions: Provided that they execute a written agreement by which the party to whom such information is remitted undertakes: **i)** to use and disclose it only for the purposes of the transaction, **ii)** to protect it with appropriate security safeguards, and iii) to return or destroy the information if the transaction does not proceed. Moreover, the disclosure of the information must be limited to what is necessary to proceed with and complete the transaction. [24]

(2) After a transaction is completed, personal information of employees may be used, collected, and disclosed without their knowledge or consent.

Conditions: The information is used and disclosed for the same purposes as prior to the transaction, and is protected by appropriate security safeguards. [25]

If the party that receives such information wishes to disclose it after the transaction, disclosure of information must be limited to what is necessary to carry

on the business, and the employees in question must be notified within a reasonable time after disclosure. The same conditions apply with respect to the personal information of consumers.

Contractual measures to protect personal information

According to the OPC, to avoid being held responsible when data is transferred or disclosed in the course of international commercial activity or a business transaction, an agreement should be formed with the foreign party which guarantees the confidentiality and security of personal information, while allowing oversight, monitoring, and auditing of the foreign service provider.

Such agreements should provide that the third party must designate a person to manage privacy aspects of the agreement, and that use of personal information shall be limited to the purposes of the commercial activities or business transaction between the two organizations.

Such agreements should also: **i)** limit disclosure to what is authorized by law or the Canadian business, **ii)** refer persons seeking access to personal information to the Canadian business, **iii)** stipulate that transferred information be returned or disposed once the contract is concluded, and implement appropriate security safeguards, such as password encryption and storing of documents locked in filing cabinets.

In a case before the OPC, it was determined that a Canadian company subject to PIPEDA must take contractual measures to protect the information of its clients and employees when engaged in commercial activity with a foreign service provider. However, the OPC found that such contractual measures are not required when a Canadian company shares information with its American parent, as long as both companies adhere to the same level of data protection. [26] Such a company that operates in Canada and the United States will be subject to both the provisions of PIPEDA and of American statutes such as the Patriot Act. [27]

Ensuring compliance with PIPEDA through policy and safeguard measures

To ensure compliance with PIPEDA and substantially similar provincial statutes, employers must adopt adequate internal policies that create procedures to protect personal information, and respond to complaints. Employers must also train their employees to ensure that they understand the importance of consumer privacy and the consequences of unauthorized access to client information. Employers are also expected to develop information documents explaining the organization's privacy policy. [28]

The OPC states that organizations should also adopt technological safeguard measures to prevent privacy breaches. It is important to maintain access logs to determine what client information has been accessed by employees, and regularly audit such logs. [29]

The appropriateness of safeguard measures depends on the circumstances. Disclosure of personal information due to a clerical error, resulting in a data breach, does not necessarily mean that safeguard measures were inadequate. [30] Moreover, if an employee or client fails to take reasonable precautions to protect his or her personal information, such as setting up a secure password, the OPC may be more lenient with a business. [31]

Under the privacy statutes of Alberta and British Columbia, similar contractual measures must be undertaken to protect the personal information of employees in the course of international business transactions conducted by provincially regulated businesses. It should, however, be noted that the Quebec Privacy Act generally does not permit disclosure of employee information outside of Quebec without their consent. [32]

Conclusion

Ultimately, Canadian businesses should obtain written contractual undertakings from foreign companies to ensure that they will protect the privacy of their employees and clients, in order to avoid being held accountable for foreign data breaches. Such contracts must stipulate policy and safeguard measures to be respected by the foreign entity engaged in commercial transactions with the Canadian business. Moreover, a foreign business with no employees or establishment in Canada can be accountable to respect the provisions of PIPEDA, notwithstanding the absence of these contractual measures, if it is sufficiently connected to Canada.

Later this year, new PIPEDA provisions will enter into force which will require businesses subject to PIPEDA to keep registers of safeguard breaches concerning the personal information under their control and to report the breaches to the OPC upon its request. [33] Canadian businesses subject to PIPEDA will also be obligated to inform the OPC and an individual of a security breach likely to cause him or her serious harm. [34]

Under this amendment, an organization may be subject to substantial fines in the event that it fails to adequately maintain its registers or disclose security breaches.

[1] PIPEDA defines commercial activities as: any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.

[2] Such as: Banking, telecommunications, and interprovincial or international transportation. See: *Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5), s. 2, 4*

[3] See: https://www.priv.gc.ca/leg_c/legislation/ss_index_e.asp.

[4] Ontario, Newfoundland and Labrador, New Brunswick, Prince Edward Island, Nova Scotia, Manitoba, and Saskatchewan.

[5] See: https://www.priv.gc.ca/resource/fs-fi/02_05_d_26_e.asp

[6] See: *Doe v D.* 2016, ONSC 541, in which the Superior Court of Ontario reaffirmed the existence of a cause of action in tort for invasion of privacy.

[7] In other words these foreign corporations have a real and substantial connection to Canada and are subject to PIPEDA. See: PIPEDA Report of Findings #2013-001, *Investigation into the personal information handling practices of WhatsApp Inc.*, See also: PIPEDA Report of Findings #2015-002, *Complaints against globe24h.com*

[8] Supra note 2, at s. 4.01

[9] See for example: P*IPEDA Case Summary #2005-297, Unsolicited e-mail for marketing purposes*, in which a third party company collecting the email addresses of employees for the purpose of marketing to them breached PIPEDA.

[10] *Supra* note 2, at s. 5 (3)

[11] Alon-Shenker Pnina, Davidov Guy, *Applying the principle of proportionality in employment and labour law contexts* (2014), 59 McGill L. J. 375, p. 386

[12] *Ibid*, at p.386-387

[13] *Supra* note 2, at s. 7

[14] *Supra* note 2 at s. 7.3

[15] *Ibid*, at s. 11 (1)

[16] *Ibid*, at s. 14

[17] *Ibid*, at s. 11 (2)

[18] *Ibid*, at s. 16

[19] *Ibid*, at schedule 1, clause 4.1.3

[20] *Ibid: "An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party."*

[21] *Ibid*, at s. 7.2

[22] *Supra* note 2, at s. 2

[23] As would be the case, for example, when a data broker purchases another data broker.

[24] *Ibid*, at s. 7.2

[25] *Ibid*, at s. 7.2 (2)

[26] PIPEDA Case Summary #2006-333,*Canadian-based company shares customer personal information with U.S. parent*

[27] Office of the Privacy Commissioner, *Transferring Personal Information about Canadians Across Borders – Implications of the USA PATRIOT Act*

(2014), p. 9,10

[28] *Supra* note 2, at schedule 1, clause 4.1.4

[29] *Ibid*

[30] PIPEDA Case Summary #2003-251, *A Question of Responsibility*

[31] *Ibid*

[32] *An Act respecting the Protection of Personal Information in the Private Sector*, CQLR c P-39.1, s.1 4, 17, 22

[33] *Digital Privacy Act*, SC 2015, c 32, s. 10.1; Note that the province of Alberta already enforces such reporting obligations (*Personal Information Protection Act*, SA 2003, c P-6.5, s.34.1).

[34] *Ibid*

---

* Christopher Deehy is a partner in the Labour & Employment Practice Group of Lapointe Rosenstein Marchand Melancon, LLP. He can be contacted at christopher.deehy@lrmm.com. Sophie Roy-Lafleur is an associate in the Labour & Employment Practice Group of Lapointe Rosenstein Marchand Melancon, LLP. She can be contacted at sophie.roy-lafleur@lrmm.com. Special thanks to Jason Stober, articling student, for his contribution.

Christopher J Deehy
C. Deehy
Montreal, Quebec CANADA CAN
PROFILE | VCARD

Sophie Roy-Lafleur
S. Roy-Lafleur
PROFILE | VCARD

Posted: Tuesday, August 23, 2016

Topics: Employment / Labor Law, Labor & Employment