

## CANADIAN PRIVACY LAW GOES ABROAD – THAT’S DATA PROTECTION!

**By: Julio Arboleda Ramirez and Curtis Ellery Marble<sup>1</sup>  
Borden Ladner Gervais, LLP  
Calgary, Canada**

*Case studies in privacy laws and their application highlight the scope and reach of Canadian privacy laws and their consequences both inside and outside Canada.*

Canadian privacy law now has a global reach. A stunning recent example of this is the report of the Privacy Commissioner of Canada on the recent investigation into Facebook.<sup>2</sup>

As a result of this investigation Facebook agreed to change its privacy practices worldwide, for all users.<sup>3</sup> While Facebook has over 12 million users in Canada, it has 200 million users world wide.<sup>4</sup> The question arises: how is it that a Canadian regulator came to believe that she had broad geographic jurisdiction, so that businesses possessing such information, regardless of their location in the world, need to ensure their compliance with Canadian privacy law?

Known in some countries as “data protection law”,<sup>5</sup> Canadian privacy law applies to personal information about Canadians. “Personal information” is information about an identifiable individual, that is a natural, or biological person. Canadian privacy law, along with the authorities’ investigatory capacity, now follows this information as it flows throughout the world.

This article is about the underpinnings of this remarkable reach of Canadian privacy law. The basis of this reach is not evident in Canadian privacy law statutes, but

---

<sup>1</sup> *Julio Arboleda Ramirez is a partner in the Calgary office of Borden Ladner Gervais, LLP and heads up that office’s Privacy and Access to Information Group and is the International contact for the Calgary office. He has an LL.M. from Osgoode Hall in e-business and his major paper dealt with privacy legislation and corporate mergers and acquisitions. He also has a significant private international business law practice dealing particularly with Spanish civil law jurisdictions.*

*Curtis Ellery Marble is an associate in the Commercial Litigation Group in the Calgary office of Borden Ladner Gervais LLP. Curtis holds an M.A. in International Affairs from the Norman Paterson School of International Affairs at Carleton University, and clerked at the Alberta Court of Queen’s Bench in Calgary.*

<sup>2</sup> PIPEDA Case Summary #2009-008, Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc., Decision of the Privacy Commissioner of Canada, (July 22, 2009), online: Office of the Privacy Commissioner of Canada <[http://www.priv.gc.ca/cf-dc/2009/2009\\_008\\_0716\\_e.cfm](http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm)>.

<sup>3</sup> News Release, Facebook agrees to address Privacy Commissioner’s concerns, Privacy Commissioner of Canada satisfied that proposed changes to the social networking site’s privacy practices and policies would bring Facebook into compliance with Canadian law, (August 27, 2009), online: Office of the Privacy Commissioner of Canada <[http://www.priv.gc.ca/media/nr-c/2009/nr-c\\_090827\\_e.cfm](http://www.priv.gc.ca/media/nr-c/2009/nr-c_090827_e.cfm)>.

<sup>4</sup> *Supra* note 2 at para. 8.

<sup>5</sup> For example, the European Union and Argentina.

rather, is found in the Federal Court of Canada decision in *Lawson v. Accusearch Inc.*,<sup>6</sup> (“*Abika*”), and the Privacy Commissioner’s final decision in this matter, as well as her decision in the *Report of Findings: Law School Admission Council Investigation* (“*LSAC*”).<sup>7</sup> These decisions interpret the jurisdiction and investigatory role of Canada’s Privacy Commissioner.

### ***Canadian Privacy or Data Protection Law – (“PIPEDA”)***

Canada’s federal private sector privacy legislation is the *Personal Information Protection and Electronic Documents Act*.<sup>8</sup> It is broad industry wide privacy legislation that applies to Canadians’ personal information collected, used or disclosed by an organization in the course of commercial activities, when that personal information crosses Canada’s provincial or international borders. Although less relevant to this article, it also applies inside certain Canadian provinces. Notably, Canada’s regime has been determined by the European Commission to provide an adequate level of protection for personal data transferred from the European Community to recipients in Canada subject to *PIPEDA*.<sup>9</sup>

An “Organization” is defined to include an association, partnership, person or trade union, and also includes a corporation. *PIPEDA* imposes a number of requirements with respect to the management of personal information collected, used or disclosed by organizations in the course of commercial activities.

Where it applies, *PIPEDA* requires reasonable personal information management practices to be implemented. This includes obtaining consent for, or giving notification of, the collection, use or disclosure of such personal information by the various organizations involved. *PIPEDA* also requires reasonable safeguards for the storage of such personal information, and limits the time it may be retained. In addition, Canadian organizations have detailed obligations when sending Canadians’ information abroad, although an analysis of the corresponding decisions of the Privacy Commissioner is beyond the scope of this analysis.<sup>10</sup>

However, foreign based employers will note that *PIPEDA* does not apply to employee information<sup>11</sup> unless connected to a federally regulated sector of the economy,

---

<sup>6</sup> 2007 FC 125 [*Abika*].

<sup>7</sup> Decision of the Privacy Commissioner of Canada, (May 28, 2008), online: Office of the Privacy Commissioner of Canada <[http://www.priv.gc.ca/cf-dc/2008/389\\_rep\\_080529\\_e.cfm](http://www.priv.gc.ca/cf-dc/2008/389_rep_080529_e.cfm)>.

<sup>8</sup> S.C. 2000 c. 5 [*PIPEDA*].

<sup>9</sup> Article 1, Commission Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, 2002/2/EC, online: < <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:002:0013:0016:EN:PDF>>.

<sup>10</sup> See, for example, *PIPEDA* case summary #313 (October 19, 2005), online: Office of the Privacy Commissioner of Canada <[http://www.privcom.gc.ca/cf-dc/2005/313\\_20051019\\_e.asp](http://www.privcom.gc.ca/cf-dc/2005/313_20051019_e.asp)> (“*CIBC*”).

<sup>11</sup> Although beyond the scope of this article, provincial privacy legislation in the Province of Quebec, which applies to most private sector provincially regulated organizations in Quebec, requires certain protection to be in place before personal information, including information about employees, can be

known as a federal work, undertaking or business. Examples of such sectors include, among others, airlines, banking, broadcasting, inter-provincial transportation and telecommunication. Of course, if an organization that is a federal work, undertaking or business transfers employees' personal information across Canada's borders, *PIPEDA* will apply.

The Privacy Commissioner is an officer of the Parliament of Canada and is empowered to investigate complaints and audit the personal information handling practices of organizations in accordance with *PIPEDA*. It is notable that there is no mention in *PIPEDA* as to where the Privacy Commissioner has jurisdiction. *Abika* and *LSAC* now make it clear that under *PIPEDA* the Privacy Commissioner has jurisdiction to investigate complaints related to the cross-border flow of Canadians' personal information,<sup>12</sup> as long as there is a real and substantial connection to Canada.<sup>13</sup> This is the case even if the business being investigated is not physically located in Canada. Therefore international businesses dealing with Canadians' personal information need to know that *PIPEDA* may apply to them.

#### ***Lawson v. Accusearch Inc. ("Abika")***

In this case a public interest lawyer, Phillipa Lawson, filed a complaint with the Privacy Commissioner. The substance of this complaint was that Accusearch Inc., a US corporation located in the United States, in the State of Wyoming, was collecting information about individual Canadians and selling it without the knowledge or consent of the individual, contrary to *PIPEDA*.

The Assistant Privacy Commissioner refused to investigate.<sup>14</sup> She determined that *PIPEDA* did not give her the jurisdiction to compel foreign companies to provide materials to aid in her investigation of the complaint. In her original response to the complainant, she stated that:

The general convention is that Canada only legislates for Canada and only regulates activities within its borders. While Parliament may legislate with extraterritorial effect, this is rarely done. In the infrequent case that it is, it is for national security purposes or for a limited class of other purposes.  
(...)

There is nothing explicit in *PIPEDA* to suggest that it was meant to apply outside of Canada or that the powers of the [Privacy] Commissioner

---

communicated to a person outside that province. Similarly, amendments to provincial privacy legislation in the Province of Alberta, which applies to most private sector provincially regulated organizations in Alberta, will require notice when personal information, including personal employee information, is sent abroad for processing or collected abroad.

<sup>12</sup> *Abika*, *supra* note 6 at paras. 42 and 51 and *LSAC*, *supra* note 7 at paras. 41- 45.

<sup>13</sup> *LSAC*, *supra* note 7 at paras. 41- 45.

<sup>14</sup> Letter from Heather Black, Assistant Privacy Commissioner of Canada to the Canadian Internet Policy and Public Interest Clinic regarding On-Line Data Brokers, (November 18, 2005) online: Office of the Privacy Commissioner of Canada <[http://www.privcom.gc.ca/legislation/let/let\\_051118\\_e.asp](http://www.privcom.gc.ca/legislation/let/let_051118_e.asp)>.

would extend beyond Canada's borders ... In the absence of any express or implied legislative intent, I must conclude that *PIPEDA* has no direct application outside of Canada.<sup>15</sup>

Upon application by Ms. Lawson the Federal Court of Canada reviewed the decision of the Assistant Privacy Commissioner. In its review the Federal Court noted that "...the [Privacy] Commissioner did not distinguish her power to investigate from the effectiveness of her investigation."<sup>16</sup> The Court further determined that while *PIPEDA* itself does not give an indication that Parliament intended to legislate extraterritorially, the Privacy Commissioner did not lose her power to investigate merely because the power to enter premises in the State of Wyoming, or to subpoena a foreign entity was not given.<sup>17</sup>

Specifically, the Federal Court held that as an investigative tribunal "[t]he [Privacy] Commissioner's jurisdiction must be considered *ratione materiae* (over the subject matter), *ratione personae* (over the person) and *ratione loci* (over the territory)".<sup>18</sup> The Federal Court further stated that "... the Privacy Commissioner erred in law by taking the position that Ms. Lawson's complaint could only be investigated if Parliament had intended and had given extraterritorial effect to *PIPEDA*."<sup>19</sup> By ordering the Privacy Commissioner to investigate, the Court implied that the Privacy Commissioner's powers under *PIPEDA* were, or at least included, powers *ratione materiae*.

Of particular interest to international businesses with cross-border flow of Canadians' personal information, the Court made it clear that the Privacy Commissioner does not lose her jurisdiction merely because a foreign entity refuses to cooperate:

It would be most regrettable indeed if Parliament gave the [Privacy] Commissioner jurisdiction to investigate foreigners who have Canadian sources of information only if those organizations voluntarily name names. Furthermore, even if an order against a non-resident might be ineffective, the [Privacy] Commissioner could target the Canadian sources of information.<sup>20</sup>

### ***The Law School Admission Council Investigation ("LSAC")***

As a result of the Federal Court's *Abika* decision, the Privacy Commissioner fine-tuned the test for jurisdiction in her *LSAC* decision. The Law School Admissions Council (the "Council") administers the L.S.A.T. examination used for admissions purposes by most Canadian and American law schools. In its efforts to ensure the integrity of test results, the Council required test takers to have their thumbprints taken.

---

<sup>15</sup> *Ibid.*

<sup>16</sup> *Abika*, *supra* note 6 at para. 27.

<sup>17</sup> *Ibid.* at para. 28.

<sup>18</sup> *Ibid.* at para. 29.

<sup>19</sup> *Ibid.* at para. 38.

<sup>20</sup> *Ibid.* at para. 42.

The thumbprints were stored in the United States. The Council itself is headquartered in the United States. A student complained that the requirement for thumbprints was an infringement of the student's right to privacy. The Privacy Commissioner commenced an investigation, and the Council agreed to replace the collection of thumbprints with the collection of photographs of the test takers. However, the Council stated that it was doing so without acquiescing to the jurisdiction of the Privacy Commissioner and without prejudice to its ability to reinstate the taking of thumbprints.<sup>21</sup>

In response, the Privacy Commissioner found that she had jurisdiction, held that the complaint was well founded and required the Council to permanently cease the collection of thumbprints, and to limit the retention of photographs of test takers to a maximum of five years.

Even though the Council was located in the United States and did not have a physical presence in Canada, the Privacy Commissioner resolved her jurisdiction as follows:

The question of the reach of Canadian legislation to an organization such as *LSAC*, which is physically located in the US, must also be considered. A statute may apply to persons, property or transactions physically located outside the enacting body's jurisdiction, where there is a sufficient link between the matter at issue and the jurisdiction of the enacting body. In such cases, the convergence of linking factors effectively brings the matter within the jurisdiction. The sufficiency of links is assessed by looking at real and substantial connections.

A variety of factors must be explored to determine whether such a connection exists, including: location in which the activity takes place; location to which profits flow; location of preparatory activities; residency of parties involved; location of contract; location of any potential related proceedings; jurisdiction where promotional efforts [are] primarily targeted; location of content provider; location of host server; location of intermediaries (sic); location of the end user.<sup>22</sup>

In short, where there is a real and substantial connection to Canada, the Privacy Commissioner is able to assert jurisdiction.

***The Privacy Commissioner's new Guidelines:***

Following the *LSAC* decision, the Privacy Commissioner then published guidelines for third party cross border data processing. Called *Processing Personal Data Across Borders – Guidelines* (the "Guidelines"),<sup>23</sup> the Guidelines provide a reference for businesses and consumers on the rules surrounding the outsourcing of the processing of

---

<sup>21</sup> *LSAC*, *supra* note 7 at para. 61.

<sup>22</sup> *Ibid.* at paras. 41 and 42.

<sup>23</sup> *Processing Personal Data Across Borders: Guidelines*, (January, 2009) online: Office of the Privacy Commissioner of Canada <[http://www.privcom.gc.ca/information/guide/2009/gl\\_dab\\_090127\\_e.pdf](http://www.privcom.gc.ca/information/guide/2009/gl_dab_090127_e.pdf)>.

personal data across borders. Specifically, the Guidelines provide that individual consumers can expect "...that their personal information is protected, regardless of where it is processed", and that "[o]rganizations transferring personal information to third parties are ultimately responsible for safeguarding that information."<sup>24</sup> Businesses operating in Canada should be aware of the Guidelines and specifically of the key principle that a business will continue to be responsible for the personal information even after it is provided to a foreign data processor.

The Guidelines stipulate that an organization is responsible to ensure, through contractual means or otherwise, a level of protection for personal information comparable to that available prior to its transfer. Accordingly, an organization dealing with Canadians' personal information:

...must take all reasonable steps to protect it from unauthorized uses and disclosures while it is in the hands of the third party processor. The organization must be satisfied that the third party has policies and processes in place, including training for its staff and effective security measures, to ensure that the information in its care is properly safeguarded at all times. It should also have the right to audit and inspect how the third party handles and stores personal information, and exercise the right to audit and inspect when warranted.<sup>25</sup>

In addition, an organization needs to consider all of the elements of a cross-border transaction, including the nature of the legal regime where the information is being sent. Finally, individuals are entitled to notice that their personal information will be transferred to a foreign country, and be subject to the laws of that country.

The Guidelines themselves are, however, silent on both transfers of personal information among intercompany affiliates, and the particulars of the Privacy Commissioner's authority to investigate beyond Canada's borders.

### ***Why do these developments to privacy law matter?***

Given *Abika* and *LSAC* and the Guidelines it is clear that if Canadians' personal information is transmitted to a United States or other foreign head office or to an affiliate or third party service provider outside of Canada, that personal information will *still* be subject to *PIPEDA*. In addition, that head office, affiliate or third party's management of that personal information will also be at issue. In the event that reasonable personal information management practices are not in place, and particularly in the event of a complaint to the Privacy Commissioner, that foreign or United States based head office, affiliate or third party service provider may find themselves subject to an investigation by Canada's Privacy Commissioner.

---

<sup>24</sup> *Ibid* at 8.

<sup>25</sup> *Ibid.* at 6.

Therefore, international businesses with cross border flow of personal information containing Canadians' personal information now know that based on a real and substantial connection to Canada, their handling of Canadians' personal information otherwise subject to *PIPEDA* will remain subject to *PIPEDA* as it journeys abroad. In addition, counsel for Canadian businesses sending Canadians' personal information outside of Canada must be aware of the requirements of *PIPEDA* as it applies to the management of that personal information.