

# Responding to a Privacy Breach under Federal, Alberta and British Columbia Legislation *An Overview*

BY: KAREN JACKSON ([kjackson@stikeman.com](mailto:kjackson@stikeman.com))

P R I V A C Y



# Responding to a Privacy Breach under Federal, Alberta and British Columbia Legislation

## An Overview

BY: KAREN JACKSON (kjackson@stikeman.com)

This paper was prepared with the invaluable assistance of Andrew Cunningham and Edu Iduke.

---

As recent publicized privacy breaches have shown, information security is a critical public relations and business issue for Canadian companies.<sup>1</sup> This paper examines responses to a privacy breach under Canada's federal, Alberta and British Columbia privacy regimes. It provides a brief overview of the relevant legislation, outlines key steps an organization should consider when a privacy breach is discovered, discusses notification requirements and investigation procedures, considers the Commissioners' powers to order disclosure of documents, their confidentiality obligations, the use of the Commissioners' reports in other litigation and an organization's rights to respond to Commissioners' report.

### PRIVACY LEGISLATION

Privacy protection in Canada in the private sector is both federally and provincially regulated. In 1993, Quebec became the first Canadian jurisdiction to enact private sector privacy legislation.<sup>2</sup> This was followed in 2001 by federal legislation – the *Personal Information Protection and Electronic Documents Act* (“PIPEDA”) – which came into full effect in 2004.<sup>3</sup> Subsequently, Alberta and British Columbia also enacted private sector privacy legislation, known in both provinces as the *Personal Information Protection Act* (hereafter, “AB PIPA” and “BC PIPA” respectively).<sup>4</sup> While privacy legislation has also been enacted in Manitoba<sup>5</sup>, Saskatchewan<sup>6</sup>, and Ontario<sup>7</sup>, these statutes deal exclusively with health information and do not otherwise affect private businesses. A special provision in PIPEDA causes that statute to apply to the private sector not only with respect to any “federal work, undertaking or business” and to interprovincial privacy issues (which would normally be the limit of federal legislative power) but also with respect to privacy issues arising entirely within a province

---

<sup>1</sup> In early 2007, TJX Companies, Inc., the parent company of Winners and HomeSense, disclosed that it suffered a computer intrusion affecting the personal information of an estimated 45 million payment cards in Canada, the United States, Puerto Rico, the United Kingdom and Ireland. CIBC also reported that account information for about 470,000 customers was lost when a computer file was lost in transit between company offices. Other recent privacy breaches include the Staples/Business Depot's failure to delete a customer's files from computers that had been returned to the store and subsequently resold (*The Business Depot Ltd.*, P2006-IR-001 (Alta. Information and Privacy Commissioner)) and the August 2007 hacking of Monster.com, an employment website including approximately 73 million CVs. See [www.vnunet.com/2197408](http://www.vnunet.com/2197408) (accessed November 2, 2007).

<sup>2</sup> *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q. c. P-39.1.

<sup>3</sup> *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5. PIPEDA is currently under legislative review. On May 2, 2007, the Standing Committee on Access to Information, Privacy and Ethics of the House of Commons made recommendations in its Fourth Report to the Parliament. On October 17, 2007, the Government tabled its response to the Fourth Report in the House of Commons and on October 27, 2007 a notice was published in the Canada Gazette advising the public of the consultations on the implementation of the Government's response to the Fourth Report.

<sup>4</sup> *Personal Information Protection Act*, S.A. 2003, c. P-6.5; *Personal Information Protection Act*, S.B.C. 2003, c. 63.

<sup>5</sup> *Personal Health Information Act*, C.C.S.M., c. P-33.5.

<sup>6</sup> *Health Information Protection Act*, S.S. 1999, c. H-0.021.

<sup>7</sup> *Personal Health Information Protection Act*, S.O. 2004, c.3.

whose legislature has not enacted a law that is “substantially similar” to PIPEDA.<sup>8</sup> In essence, this means that privacy legislation applies to all Canadian businesses, whether it is provincial legislation (with respect to intra-provincial activity in Alberta, British Columbia or Quebec) or federal legislation (in all other cases). The co-existence of federal and provincial legislation may mean that some personal information practices will be subject to both PIPEDA and applicable provincial legislation (i.e. to the extent that the practices are followed partly within a province and partly inter-provincially).

PIPEDA applies to “every organization in respect of personal information that the organization collects, uses or discloses in the course of commercial activities.” It also applies to employee information collected, used or disclosed “in connection with the operation of a federal work, undertaking or business.”<sup>9</sup> A federal work, undertaking or business is defined as that of an organization that falls under the legislative authority of the federal government, including banks, airlines and railways. The underlying purpose of PIPEDA (and that of AB PIPA and BC PIPA) is to provide rules that govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.<sup>10</sup>

According to the principles set out in PIPEDA<sup>11</sup>, an organization is required to:

- > Designate an individual or individuals who are accountable for the organization’s compliance with the principles guiding the collection, use and disclosure of information.
- > Identify the purpose for the collection of personal information.
- > Obtain the consent of individuals to the collection, use or disclosure of personal information.
- > Ensure that the collection of personal information is limited to that which is necessary for the purposes identified by the organization.
- > Limit the use, disclosure and retention of personal information.
- > Ensure the accuracy and completeness of personal information with regard to the purpose of its use.
- > Demonstrate openness with regard to the organization’s policies and practices with respect to the management of personal information.
- > Ensure that personal information is protected by security safeguards appropriate to the sensitivity of the information.
- > Upon request, inform individuals of the existence, use and disclosure of their personal information and provide access to the information.
- > Provide procedures to receive and respond to complaints or inquiries about practices regarding the handling of personal information.

Most of these principles can also be found in, or are implied by, the British Columbia and Alberta legislation.

---

<sup>8</sup> PIPEDA, s. 26(2)(b).

<sup>9</sup> PIPEDA, s. 4. It does not apply to government institutions subject to the *Privacy Act*.

<sup>10</sup> PIPEDA, s. 3.

<sup>11</sup> See PIPEDA, Schedule 1.

## WHAT IS A “PRIVACY BREACH”?

A privacy breach occurs when there is unauthorized access to or collection, use or disclosure of personal information. The access, collection, use or disclosure is “unauthorized” if it occurs in contravention of applicable privacy legislation. Privacy breaches can be the result of anything from criminal activity to a software defect or the inadvertent act of an employee.<sup>12</sup> For businesses, the most problematic type of breach occurs when personal information of consumers – such as credit card or debit card information – is stolen, lost or inadvertently disclosed to a third party.

## DISCOVERY OF A PRIVACY BREACH

Privacy legislation in Canada does not prescribe a mandatory response to privacy breaches. Nevertheless, as it can be of critical importance to make an appropriate response, it is advisable to develop an incident response plan and designate an incident response team. The members of an organization’s incident response team will depend on the roles and responsibilities of the organization’s management team, the scope of personal information collected and other factors. In many organizations it would be appropriate to include the organization’s privacy officer, in-house IT personnel, security personnel and legal counsel as members of the incident response team.<sup>13</sup> In developing an incident response plan or when responding to a privacy breach in the absence of an incident response plan, it is useful to consider the following steps.<sup>14</sup>

### 1) Gather information

It is important to establish what happened, when the breach started, how long it lasted, how it was perpetrated and who was involved, especially in cases of access by electronic hackers. In determining the cause of the privacy breach, an organization should conduct a site visit, interview witnesses, engage IT security specialists and hire private investigators as circumstances demand.<sup>15</sup>

### 2) Containment

An organization should immediately implement measures to stop or limit the breach and to mitigate any possible harm caused by the breach. Containment measures may include shutting down the system that was breached, revoking unauthorized access, stopping an unauthorized practice or correcting weaknesses in physical security.

### 3) Evaluation

An organization should evaluate the risks associated with the privacy breach by:

- > Identifying the personal information that was accessed, stolen or lost.
- > Determining the number of individuals that may be affected.
- > Determining the extent of exposure to specific categories of risk (e.g. potential fraud, identify theft, reputational damage or humiliation, loss of business).
- > Considering any risk to public safety.

<sup>12</sup> See Elizabeth Denham, “Implementing Reasonable Safeguards: An Update from the Commissioner’s Office”, a presentation delivered at the PIPA Conference 2007, Vancouver, British Columbia, available online: <http://www.verney.ca/pipa2007/presentations.php> (accessed October 9, 2007).

<sup>13</sup> The legislation requires the appointment of a compliance officer. See PIPEDA, Schedule 1, para. 4.1; AB PIPA, s. 5(3); BC PIPA, s. 4(3).

<sup>14</sup> The Office of the Information and Privacy Commissioner for British Columbia, *Key Steps in Responding to Privacy Breaches* (December 2006), available online: [http://www.oipcbc.org/pdfs/Policy/Key\\_Steps\\_Privacy\\_Breaches\\_\(December\\_2006\).pdf](http://www.oipcbc.org/pdfs/Policy/Key_Steps_Privacy_Breaches_(December_2006).pdf) (accessed October 25, 2007). The Office of the Information and Privacy Commissioner for Alberta, *Key Steps in Responding to Privacy Breaches*, (based on the key steps published by the BC OIPC) available online: <http://www.oipc.ab.ca/Search/DetailsPage.cfm?ID=3000> (accessed October 2, 2007). The Office of the Privacy Commissioner of Canada, *Key Steps for Organizations in Responding to Privacy Breaches*, available online: [http://www.privcom.gc.ca/information/guide/2007/gl\\_070801\\_02\\_e.asp](http://www.privcom.gc.ca/information/guide/2007/gl_070801_02_e.asp) (accessed November 1, 2007).

<sup>15</sup> See Catherine Tully, “How to Diagnose, Stem and Repair a Privacy Bleed”, presented at the PIPA Conference 2007, Vancouver, B.C. Available at <http://www.verney.ca/pipa2007/presentations.php> (accessed October 9, 2007).

#### 4) Internal notification

Consider the key personnel at the organization who should be briefed on the privacy breach including senior management, public relations personnel and customer relations staff.

#### 5) Monitor containment efforts

Containment and mitigation efforts should be monitored to ensure they are effective and should be revised if necessary as more information about the cause and the scope of the breach becomes available.

#### 6) External notification

It is necessary to consider the organization's notification obligations under applicable legislation, its existing contracts and other requirements. If the privacy breach was, or may have been caused by, criminal activity the appropriate law enforcement agencies should be notified.

The legislative requirements in the jurisdictions where the organization operates and in jurisdictions where the individuals whose privacy was breached reside must both be considered. Privacy legislation in Canada does not create an explicit duty to notify the privacy Commissioners or the affected individuals of the occurrence of a privacy breach.<sup>16</sup> However, the Office of the Information and Privacy Commissioner for British Columbia ("BC OIPC") and the Office of the Information and Privacy Commissioner for Alberta ("AB OIPC") have each published a privacy breach reporting form, to be completed if an organization decides to notify them of a breach.<sup>17</sup> Both forms require a description of the incident, the personal information involved, the safeguards in place at the time of the breach, the possible harm resulting from the breach and other information.

The Office of the Privacy Commissioner of Canada ("OPC"), the AB OIPC and the BC OIPC have each published factors to consider when deciding whether or not to notify individuals of a privacy breach.<sup>18</sup> The key consideration is whether notification is necessary in order to avoid or mitigate harm to the individuals affected by the breach. Other considerations include:

- > Risk of identity theft.
- > Risk of fraudulent activities.
- > Risk of physical harm.
- > Risk of humiliation or damage to reputation.
- > Risk of affecting business or employment opportunities.

If individuals whose privacy has been breached reside outside of Canada, it is also important to consider if the organization has any notification obligations in the jurisdictions where the individuals reside. For example, more than 30 states in the United States have privacy breach notification laws that may, in certain circumstances, be applicable.

Notification of individuals can be by phone, letter or in person to affected individuals (where the identities of the individuals are known). Alternatively, it can take place indirectly through website postings, notices posted in the organization's premises, or media publicity. Indirect notification may be appropriate where direct notification could cause humiliation or further harm, where it would be too costly or where contact information is lacking.

---

<sup>16</sup> However, PIPEDA may be amended in the relatively near future to provide for notification to individuals when the privacy breach results in a high risk of significant harm to individuals. See the Government's response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics of the House of Commons, note 3 above.

<sup>17</sup> BC OIPC, Privacy Breach Reporting Form, available online: <http://www.oipc.bc.ca/HelpfulForms.htm> (accessed November 1, 2007). AB OIPC, Reporting a Privacy Breach to the OIPC, available online: <http://www.oipc.ab.ca/publications/detailspage.cfm?id=3001> (accessed November 1, 2007).

<sup>18</sup> See note 14 above.

Notices should generally include the following information:

- > The date and nature of breach.
- > The steps the organization is taking to mitigate the harm.
- > The steps that affected individuals may take to further mitigate the harm.
- > Contact information of persons within the organization who can answer questions.
- > Information about additional resources that may be available to individuals.

The organization should also determine if it has any contractual requirements to notify others of the privacy breach. It is common for outsourcing agreements and agreements with debit and credit card issuing companies to contain notification obligations relating to privacy breaches.

Finally, the organization should consider the notification requirements of applicable professional and regulatory authorities and the notification requirements under its insurance policies. If the breach was caused by an equipment or software failure or malfunction, then the organization would also want to notify the equipment manufacturer or software supplier. In order to mitigate harm, in certain circumstances it may be appropriate for the organization to notify credit reporting agencies.

## 7) Media and communication strategy

The organization should consider when to issue press releases, the content of the press releases, how to respond to questions from the media and requests for interviews, what, if any response, should be given to negative or inaccurate stories in the media, how to respond to calls from individuals affected by the privacy breach or from individuals who are concerned about the safety of their personal information. It should also consider developing talking points or scripts to ensure responses are consistent.

## 8) Prevention

Having taken the steps discussed above, an organization should develop an appropriate plan to prevent further privacy breaches. Such a plan would generally be a product of its analysis of “what went wrong” in the case of the breach, together with a review of industry best practices and any recommendations or orders that were received or made in the event that the OPC, AB OIPC or BC OIPC investigated the breach.

## INVESTIGATION OF PRIVACY BREACHES

The OPC, the AB OIPC and the BC OIPC are empowered to investigate – and, in the case of the OPC, *must* investigate<sup>19</sup> – complaints lodged by individuals. The Privacy Commissioners can also initiate their own investigations in relation to protection of personal information, if there are reasonable grounds to investigate or to ensure compliance with the legislation.<sup>20</sup> The Federal Commissioner is required to notify the organization that an investigation has been initiated and the Alberta and British Columbia Commissioners may notify the organization that an investigation has been initiated.<sup>21</sup> As a matter of practice, the Alberta and British Columbia Commissioners generally notify an organization when they have initiated an investigation.

---

<sup>19</sup> PIPEDA, ss. 11(1) and 12(1). Compare AB PIPA, s. 46(3), allowing the Commissioner to insist that an individual exhaust other means of resolving an issue before the Commissioner will proceed with the requested review or investigation. BC PIPA, s. 38(4) is similar. Section 13(2) of PIPEDA allows the Commissioner to decline to issue a report if it believes that the complaint would be better resolved by means of some other process.

<sup>20</sup> PIPEDA, s. 11(2); AB PIPA, s. 38; BC PIPA, s. 38.

<sup>21</sup> PIPEDA, s. 11(4); AB PIPA, s. 48(2); BC PIPA, s. 48(2).

The investigatory powers of the privacy commissions are generally quite broad. The Federal Commissioner has the power to:

- i) summon persons to appear before her, give oral or written evidence on oath and produce any records,
- ii) administer oaths,
- iii) receive any evidence or other information, whether or not it would be admissible in a court of law,
- iv) at any reasonable time enter any non-residential premises occupied by the organization on satisfying any security requirements of the organization relating to the premises,
- v) converse in private with any person in any of the premises, and
- vi) examine or obtain copies of or extracts from records found in the premises that contain matter relevant to the investigation.<sup>22</sup>

The powers of the Alberta and British Columbia Commissioners during an investigation are similar to the powers of the Federal Commissioner.<sup>23</sup>

Anyone who obstructs an investigation by a Federal or Provincial Commissioner (e.g. by disposing of documents necessary to an investigation) is liable to a fine that under PIPEDA can be as high as \$100,000 and which under AB PIPA and BC PIPA is a maximum of \$10,000 in the case of an individual, or up to \$100,000 in any other case.<sup>24</sup>

Within one year of initiating an investigation, the Federal Privacy Commissioner must generally prepare a report indicating findings, recommendations and any settlement reached by parties.<sup>25</sup> The Commissioner is not required to prepare a report in certain circumstances, including if she is satisfied that the complainant ought to exhaust other available grievance or review procedures first or that the complaint is trivial, frivolous or vexatious or was made in bad faith.<sup>26</sup>

The AB PIPA and the BC PIPA do not explicitly establish time periods within which the reports of the Commissioners' investigations must be prepared. However, a recent decision with respect to AB PIPA seems to imply that, unless the Alberta Commissioner notifies the person initiating the complaint, the organization and other relevant parties that he is extending the time to complete the investigation and/or any subsequent inquiry, the investigation and any subsequent inquiry must be completed within 90 days from the date the Commissioner received the request initiating the complaint.<sup>27</sup>

The Federal and British Columbia Privacy Commissioners publish their investigation reports on their websites but generally only after information identifying the organization has been removed. The Alberta Privacy Commissioner is specifically authorized to publish "findings or decisions" in whole or in part and has adopted the practice of publishing the entire investigation report on its website, including information identifying the organization whose privacy practices were investigated.<sup>28</sup>

Within 45 days following the release of a report by the Federal Commissioner, the complainant (an individual or the Commissioner) or, if the Commissioner is not the complainant, the

---

<sup>22</sup> PIPEDA, s. 12(1)(a).

<sup>23</sup> AB PIPA, ss. 38(1)-(3); BC PIPA, s. 38(1).

<sup>24</sup> PIPEDA, s. 28; AB PIPA, s. 59(2); BC PIPA, s. 56(2).

<sup>25</sup> PIPEDA, s. 13(1).

<sup>26</sup> PIPEDA, s. 13(2).

<sup>27</sup> *Kellogg Brown and Root Canada v. (Alberta) Information and Privacy Commissioner*, 2007 ABQB 499.

<sup>28</sup> AB PIPA, s. 38(6).

Commissioner with the consent of the complainant, may apply to the Federal Court – Trial Division for a hearing in respect of any matter (i) in respect of which the complaint was made, (ii) that is referred to in the report, or (iii) that is referred to in certain provisions of PIPEDA.<sup>29</sup> In addition to any other remedies it may give, the Court may order an organization to correct its personal information management practices to comply with PIPEDA and it may award damages to the complainant for any humiliation the complainant has suffered.<sup>30</sup>

Under the Alberta and British Columbia legislation, if the investigation does not result in the matter being resolved the Commissioner may conduct an inquiry,<sup>31</sup> pursuant to which he or she will issue an order deciding the outcome of the issues.<sup>32</sup> In both provinces the Commissioner has considerable latitude in establishing the ground rules of the inquiry. For example, he or she decides whether the inquiry will be held privately, whether representations will be made verbally or in writing and whether a person is entitled to be present during, to have access to, or to comment on, the representations made to the Commissioner by another person.<sup>33</sup> The Commissioner's orders are published on the AB OIPC and the BC OIPC websites in their entirety. A copy of an order made by the Alberta Commissioner may be filed with the Court of Queen's Bench and thereafter the order is enforceable as a judgement or order.<sup>34</sup>

Upon the issuance of the order, an organization has 30 days (BC PIPA) or 50 days (AB PIPA) to comply.<sup>35</sup> An order may be subject to judicial review provided that an application is made within 30 days (BC PIPA) or 45 days (AB PIPA) of the date on which an organization receives the order.<sup>36</sup> An application for judicial review will act as a stay of the Commissioner's order.<sup>37</sup> Under both AB PIPA and BC PIPA, once all rights of appeal have been exhausted, an individual affected by the conduct with respect to which an order was made has a cause of action against the organization for damages for actual harm arising from the breach of the obligations under the legislation.<sup>38</sup>

## POWER TO ORDER DISCLOSURE OF DOCUMENTS

The Federal, Alberta and British Columbia Privacy Commissioners have broad powers to order the disclosure of documents. The Federal Commissioner has the same powers as a "superior court of record" and although that term is not defined in PIPEDA, it has been held that it refers to the Federal Court of Canada.<sup>39</sup> Under Rule 225 of the *Federal Courts Rules*, the Federal Court may order a party that is a corporation to disclose all relevant documents in the possession, power or control of the corporation or its affiliates.<sup>40</sup> Rule 230 is a relieving clause to Rule 225 which allows a party to refuse disclosure if, on a motion, the party is able to successfully argue that it "would be unduly onerous" to require the party to produce the document.

In addition, in *Blood Tribe Department of Health v. Canada (Privacy Commissioner)* the Federal Court of Appeal ruled that the OPC does not have the power to compel the production of documents subject to solicitor-client privilege.<sup>41</sup> However, in March 2007, the

---

<sup>29</sup> PIPEDA, ss. 14 and 15.

<sup>30</sup> PIPEDA, s. 16.

<sup>31</sup> AB PIPA, s. 50(1); BC PIPA, s. 50(1).

<sup>32</sup> AB PIPA s. 52; BC PIPA, s. 52.

<sup>33</sup> AB PIPA, s. 50(4); BC PIPA, s. 50(4).

<sup>34</sup> AB PIPA, s. 52(6).

<sup>35</sup> BC PIPA, s. 53(1); AB PIPA, s. 54(1).

<sup>36</sup> BC PIPA, s. 53(2); AB PIPA, s. 54(3).

<sup>37</sup> AB PIPA, s. 54(4); BC PIPA, s. 53(1).

<sup>38</sup> AB PIPA, s. 60(1); BC PIPA, s. 57(1).

<sup>39</sup> PIPEDA, s. 12(i)(a); *Re Kerko* (1988), 21 F.T.R. 180 at para. 26.

<sup>40</sup> *Federal Courts Rules*, S.O.R./98-106.

<sup>41</sup> *Blood Tribe Department of Health v. Canada (Privacy Commissioner)*, [2007] 2 F.C.R. 561.

Federal Privacy Commissioner was granted leave to appeal the *Blood Tribe* decision before the Supreme Court of Canada.<sup>42</sup>

AB PIPA and the BC PIPA provide that the Commissioner may require any record or document to be produced and, unlike PIPEDA, they do not appear to limit the persons from whom a record or document may be requested.<sup>43</sup> In addition, both AB PIPA and BC PIPA provide that documents subject to solicitor-client privilege must be produced.<sup>44</sup>

## CONFIDENTIALITY

PIPEDA, AB PIPA and BC PIPA require the Commissioners to keep the information they receive in the course of an investigation confidential.<sup>45</sup> However, there are several fairly broad exceptions to these provisions. The exceptions are substantially similar in PIPEDA, AB PIPA and BC PIPA and include disclosure of:

- > Information the Commissioner considers necessary to conduct an investigation or to establish grounds for findings or recommendations.
- > Information in the course of a prosecution for an offence under the privacy legislation, or for perjury.
- > Information in the course of certain court hearings.<sup>46</sup>

In addition, PIPEDA expressly allows the Commissioner to disclose information relating to the personal information management practices of an organization if the Commissioner considers it is in the public interest to disclose the information.<sup>47</sup>

## USE OF INFORMATION IN OTHER LITIGATION

Subject to certain exceptions, the Commissioners under PIPEDA, AB PIPA or BC PIPA are not competent witnesses in respect of any matter that comes to their knowledge as a result of the performance of their duties. The exceptions include prosecutions of perjury or of an offence created by the privacy legislation, a hearing conducted to review the report of the Federal Commissioner, and a judicial review of the order of a Provincial Commissioner.<sup>48</sup> The consequence of this is that information provided to a Commissioner during an investigation cannot be entered into evidence in Canada in other proceedings without adherence to the normal rules of evidence.

## RESPONDING TO A COMMISSIONER'S REPORT

As already noted,<sup>49</sup> under PIPEDA the complainant or, if the Commissioner is not the complainant, the Commissioner with the consent of the complainant, may apply to the Federal Court for a hearing within 45 days of the release of the Commissioner's report.<sup>50</sup> Such a hearing can consider any matter raised in the complaint or referred to in the report. However, no such right is accorded the organization under investigation. This can pose a problem if neither the Commissioner nor the complainant wish to proceed to a hearing but the Commissioner's report contains findings of fact or legal conclusions that the organization

<sup>42</sup> *Privacy Commissioner of Canada v. Blood Tribe Department of Health*, 2007 CanLII 10547 (S.C.C.).

<sup>43</sup> AB PIPA, s. 38(2); BC PIPA s. 38(2).

<sup>44</sup> AB PIPA, s. 38(3). AB PIPA, s. 5 states that the operation of the Act does not affect any legal privilege. Section 38(3) of BC PIPA contains a clearer statement that solicitor-client privileged documents that are disclosed to, or obtained by, the Privacy Commissioner do not thereby lose their privilege. See also BC PIPA, s. 3(3).

<sup>45</sup> PIPEDA, s. 20; AB PIPA, s. 41; BC PIPA; s. 41.

<sup>46</sup> PIPEDA, s. 21; AB PIPA, s. 38(1); BC PIPA, s. 39(1).

<sup>47</sup> PIPEDA, s. 20(2).

<sup>48</sup> PIPEDA, s. 21; AB PIPA, s. 39; BC PIPA, s. 39.

<sup>49</sup> See page 6 above.

<sup>50</sup> PIPEDA, s. 14(2).

under investigation does not accept. In such a situation, the only recourse for the organization is to bring an application for judicial review of the Commissioner's decision pursuant to section 18.1 of the *Federal Courts Act* ("FCA").<sup>51</sup> However, an application for judicial review would focus on the investigation process not on the factual findings or legal conclusions in the report. The Federal Court would consider, among other things, if the Commissioner

- i) refused to exercise her jurisdiction,
- ii) acted without jurisdiction,
- iii) acted beyond the boundaries of her jurisdiction, or
- iv) breached her obligations of procedural fairness.<sup>52</sup>

To date, the courts have held, in relation to the limited grounds for judicial review in section 18.1(4) of the FCA, that the standard of review to be applied to decisions of the Commissioner is "correctness".<sup>53</sup> This means that the court could overrule the Commissioner with respect to decisions made in relation to the grounds for judicial review in section 18.1(4) of the FCA if the court would have decided differently, even if it agrees that the Commissioner's decision was not unreasonable.<sup>54</sup>

Under the Alberta and British Columbia legislation, the Commissioner "may" commence an inquiry if a matter under investigation is not resolved.<sup>55</sup> While an organization is free to request an inquiry in such a situation, the word "may" suggests that the Commissioner is not required to begin an inquiry simply because such a request has been made. On completing an inquiry, the Commissioners are required to make an order. Under AB PIPA or BC PIPA an order can be subject to judicial review at the instigation of either the complainant or the organization under investigation.<sup>56</sup> In the case of these provincial statutes, the applicable standard of review has sometimes been held to be reasonableness. Under the "pragmatic and functional approach" applied in Canada to determine appropriate standards of judicial review of administrative decisions, the factors considered are

- i) presence or absence of a privative clause, or statutory right of appeal;
- ii) the expertise of the tribunal relative to that of the reviewing court on the issue in question;
- iii) the purpose of the legislation and any particular provision in issue; and
- iv) whether the questions considered by the tribunal are primarily legal, factual or mixed fact and law.<sup>57</sup>

The fact that AB PIPA and BC PIPA do not significantly differ from PIPEDA in these respects could be taken to suggest that the "correctness" standard that has been applied to decisions of the Federal Commissioner under PIPEDA could also be applied to decisions of the Provincial Commissioners. However, the "reasonableness" standard has been applied to the British Columbia Privacy Commissioner's actions under that province's public sector privacy

---

<sup>51</sup> R.S.C. 1985, c. F-7.

<sup>52</sup> FCA, s. 18.1(4).

<sup>53</sup> See *Blood Tribe*, note 41 above and *Lawson v. Accusearch Inc.*, 2007 FC 125 (CanLII).

<sup>54</sup> As Chief Justice McLachlin wrote in *Chamberlain v. Surrey School District No. 36*, [2002] 4 S.C.R. 710: "The standard of 'correctness' involves minimal deference: where it applies, there is only one right answer and the administrative body's decision must reflect it." (para. 6).

<sup>55</sup> AB PIPA, s. 50(1); BC PIPA, s. 50(1).

<sup>56</sup> AB PIPA, s. 52(1); BC PIPA, s. 52(1).

<sup>57</sup> *Chamberlain*, note 54 above, para. 7.

legislation (the *Freedom of Information and Protection of Privacy Act*).<sup>58</sup> Nevertheless, with respect to jurisdictional questions, which by their nature are purely matters of law, the “correctness” standard has been held to be appropriate.<sup>59</sup> Similarly, in a judicial review concerning the Alberta Privacy Commissioner’s authority under Alberta’s *Health Information Act*,<sup>60</sup> the Alberta Court of Queen’s Bench maintained that the appropriate standard in the circumstances (which involved what was clearly a question of law) was correctness, but only after having observed that “[t]he same standard of review will not necessarily apply to every decision made by the Privacy Commissioner”.<sup>61</sup>

---

## APPENDIX: WEBSITES

### Legislation

PIPEDA: [www.canlii.org/ca/sta/p-8.6/whole.html](http://www.canlii.org/ca/sta/p-8.6/whole.html)

BC PIPA: [www.qp.gov.bc.ca/statreg/stat/P/03063\\_01.htm](http://www.qp.gov.bc.ca/statreg/stat/P/03063_01.htm) (not updated)

AB PIPA: [www.canlii.org/ab/laws/sta/p-6.5/20070910/whole.html](http://www.canlii.org/ab/laws/sta/p-6.5/20070910/whole.html)

### Privacy Commissions

Canada: [www.privcom.gc.ca/index\\_e.asp](http://www.privcom.gc.ca/index_e.asp)

B.C.: [www.oipcbc.org/sector\\_private/public\\_info/index.htm](http://www.oipcbc.org/sector_private/public_info/index.htm)

Alberta: [www.oipc.ab.ca/home](http://www.oipc.ab.ca/home)

Ontario: [www.ipc.on.ca/](http://www.ipc.on.ca/)

Quebec: [www.cai.gouv.qc.ca/index-en.html](http://www.cai.gouv.qc.ca/index-en.html)

### Other

Government Response to the Fourth Report of the Standing Committee on Access to Information Privacy and Ethics (Government of Canada):

[www.ic.gc.ca/epic/site/ic1.nsf/vwapj/ETHI-e.pdf/\\$file/ETHI-e.pdf](http://www.ic.gc.ca/epic/site/ic1.nsf/vwapj/ETHI-e.pdf/$file/ETHI-e.pdf)

---

<sup>58</sup> *Freedom of Information and Protection of Privacy Act*, R.S.B.C., 1996, c. 165. See, e.g. *B.C. Teachers' Federation, Nanaimo District Teachers' Association et al. v. Information and Privacy Commissioner (B.C.) et al.*, 2006 BCSC 131 (CanLII), para. 77 and *Guide Outfitters Assoc. v. British Columbia (Information and Privacy Commissioner)* (2004), 26 B.C.L.R. (4th) 1 (C.A.), para. 34.

<sup>59</sup> *British Columbia (Attorney General) v. British Columbia (Information and Privacy Commissioner) et al.* (2004), 34 B.C.L.R. (4th) 298 (S.C.), para. 40.

<sup>60</sup> *Health Information Act*, R.S.A. 2000, c. H-5.

<sup>61</sup> *Stubicar v. Alberta (Office of the Information and Privacy Commissioner)*, 2007 ABQB 480 (CanLII), para. 16.