PIPEDA and its Impact on Records Management in Canada

Nicole Bergen

University of Alberta

2018

PIPEDA and its Impact on Records Management in Canada

Overview of PIPEDA

According to the Office of the Privacy Commissioner of Canada (OPC), the Personal Information Protection and Electronic Documents Act (PIPEDA, S.C. 2000, c. 5) "is the federal privacy law for private-sector organizations" (OPC, 2018a). It describes what requirement business must adhere to in order to protect personal information that they might need to collect, use, or disclose in their business operations (OPC, 2018b). The act can be found on the Justice Department's website: Personal Information Protection and Electronic Documents Act (Justice Laws Website, 2018a). The Privacy Commissioner of Canada reports to Parliament and is responsible for ensuring that organizations comply with PIPEDA (OPC, 2016).

PIPEDA's code of conduct for business is listed and described in Schedule 1 of the Act (OPC, 2018b; Justice Laws Website, 2018b). In brief, it is as follows:

1. Accountability: Every organization must have someone who is responsible for ensuring that their company complies with this law and associated regulations.
2. Identifying Purposes: When, or before, information is collected, an organization must be able to communicate why that information is required.
3. Consent: With some exceptions, an individual must consent to an organization collecting, using, or redistributing their information.
4. Limiting Collection: An organization can't collect additional information that it has not justify collecting using its purpose identified in point 2.
5. Limiting Use, Disclosure, and Retention: An organization can't use or disclose information for anything other than what it originally said that it would unless it obtains additional consent. Information should only be kept for as long as necessary to fulfill its purpose.
6. Accuracy: Information must be "as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used" (OPC, 2018b).
7. Safeguards: Any information collected must be protected.

8. Openness: An organization needs to be able to describe its information collection and management policies and procedures and must disclose this information to individuals upon request.
9. Individual Access: An individual must be allowed to access their information and to correct it if it's inaccurate or incomplete.
10. Challenging Compliance: An individual must be able to discuss privacy and information management concerns with the person responsible for an organizations compliance chosen in point 1.

The OPC provides a Privacy Toolkit which explains each of the items in Schedule 1, though some of the links included in the document are broken (OPC, 2015a, which is the reference for the rest of this section). To fulfill item 1, accountability, they recommend creating a privacy management program which would analyse a company's information management practices, develop information management policies and procedures, and keep both staff and the public informed about these policies so that customers know what they can expect and staff know how to handle an inquiry or a complaint. To fulfill item 2, identifying purpose, they recommend defining the purpose for collecting information as clearly and as narrowly as possible since an overly broad purpose may lead a company to try to collect information that they can't justify requesting. They clarify that item 3, consent, is only consent if it's informed and if the person submitting information can be expected to understand what they're submitting, what will be done with it, and what it would mean to withdraw consent. They further specify that consent can't be obtained deceitfully and that employees should be trained to answer customer questions about what their information is being collected for. At this point it becomes clear that all these requirements are connected, since an organization needs to be clear about what information they're collecting and why, and train staff to answer the customer's questions when asking for consent; all this is closely connected to item 8, openness, when discussing the need for transparency in information management. There are a variety of ways to obtain consent and some instances in which consent is unnecessary to use or disclose personal information, though for some of these, e.g. literary or artistic, it might not in fact be in the company's best interests to do so if they also have to take public opinion into account.

Regarding item 4, limiting collection, they point out that complying with this point is more cost effective and less risky than collecting information more indiscriminately. Regarding item 5, limiting use, disclosure, and retention, they recommend a clear retention schedule that is regularly reviewed with disposal procedures that are consistently followed, accurately noting that this will prevent privacy breaches and will be less complicated than trying to destroy all the accumulated information ad hoc later. One still-relevant procedural recommendation is checking electronic equipment before disposal to ensure that information can't be retrieved from it.

To fulfill item 6, accuracy, they recommend recording the date that information was obtained and to ask of out-of-date or incomplete information would harm anyone when determining what to update. The OPC clarifies that PIPEDA doesn't specify what sort of safeguards, for item 7, are needed but that an organization needs to determine for itself what it needs. To this end they recommend developing a security policy, reviewing it regularly to ensure that it's up-to-date and still functional, and educating staff about security requirements and procedures. They further recommend making sensitive information "need-to-know" and blacking out any information that can be hidden when sharing it with anyone, and they provide steps that they recommend taking when a privacy breach does occur (OPC, 2007). For items 6 and 7, in particular, an RM team may wish to consult with an IT team given the number of technological advances since this law was written; the possibilities of automation in fulfilling items like accuracy have expanded and as have the potential hazards to security.

To fulfill, item 8, openness, they recommend making policies and procedures consistently available in various mediums, such in person & online, and they provide more details suggestions for maintaining privacy and transparency (OPC, 2013a). Regarding item 9, individual access, there are exceptions when an organization doesn't need to or is not allowed to provide access, but they do need to provide a written reason for not providing access, and that if they do provide information they need to make sure that the person they're giving it to has a right to have it. Lastly, regarding item 10, challenging compliance, they specify that an organization needs to provide complaint procedures, that they should investigate any complaint immediately, and keep records of complaints and decisions.

Exceptions & Similar Provincial Legislation

Some provinces may prefer to enact their own privacy legislation which can exempt business operating in those provinces from PIPEDA, although it won't exempt them from the law when it comes to interprovincial and international business (OPC, 2018b and OPC, 2018c). Some other institutions, particularly the MUSH sector (municipalities, universities, schools, and hospitals) are covered by both PIPEDA and provincial privacy legislation: private hospitals and schools may fall under the jurisdiction of PIPEDA more easily, unless provincial legislation covers their activities, and there may be instances where MUSH institutions or not-for-profit organizations are engaged in commercial activity and that aspect of their operations may be covered by PIPEDA while other activities are covered by provincial legislation (OPC, 2015b). The federal government's use of personal information is covered by the Privacy Act (OPC, 2015b).

Regulations

There are 14 regulations that are made under this act, one of which is not yet in force, and a further regulation that was repealed (Justice Laws Website, 2018a). These cover exceptions for the provinces with their own privacy laws, publicly available information, electronic signatures, security safeguards (not in force) and electronic alternatives (Justice Laws Website, 2018a).

Enforcement & Complaints

The Office of the Privacy Commissioner, which oversees PIPEDA, provides instructions and tips as well as training tools for businesses so that they can comply with PIPEDA and avoid complaints (OPC, 2018d). Any citizen can make a complaint to the commissioner though the commissioner doesn't need a citizen's complaint to begin an investigation if the situation warrants it: they can begin an inquiry or audit on their own, for instance if a potential instance of noncompliance has been discussed in the media (OPC, 2018f). Once a complaint begins, it can take one of two routes: first it can be handled by an early resolution officer who can mediate between the complainant and the accused party and then issue a

Case Summary (OPC, 2018b & OPC, 2018e). If that is unsuccessful, the Office the Privacy Commissioner can hold an investigation, issue findings, and make recommendations (OPC, 2018b).

The OPC is under no obligation to disclose the identity of the complainant and the complainant can ask that their identity be protected (OPC, 2018f). When an individual makes a complaint and the OPC doesn't begin an investigation, it can be because they thought another procedure or office would serve the complaint better, they found that the complainant waited too long to make the complaint, it was resolved in-house before an investigation could begin, or the organization in question is not covered by PIPEDA (OPC, 2018g). Any findings are published in the Report on Findings and if the response to their recommendations is unsatisfactory, they can apply to the Federal Court which has the authority to order business to change whatever practices were objectionable and to pay damages (OPC, 2018b). An organization is not allowed to destroy information that has been requested or to obstruct an investigation, nor can they retaliate against a complainant (OPC, 2018b). If the OPC decides not to go through the Federal Court, they can publicly disclose the name of the organization, audit its information management practices, arrange a compliance agreement to bring an organization into compliance with PIPEDA, or report offences to the Attorney General or to the relevant provincial government (OPC, 2018g).

Some of the most common types of complaints that have been logged with the OPC include access, accuracy, consent, identifying purposes, retention & disposal, safeguards, and use and disclosure; the most common sectors in which complaints have been made are financial institutions, by a long way, followed by telecommunications. Fewer are made in transportation, sales & services, accommodations, and professional industries (OPC, 2018e).

Impact on Records Management in Canada

This law provides a thorough basis for developing a records management policy that protects the privacy of anyone involved with the organization, whether employee or customer. It's written clearly and explained quite thoroughly on the government's website. That said, and despite the "electronic" in the title, it does not deal with the online and technical developments of the last 18 years, since it was written in 2000. What it does do is give a foundation on which to build policies and procedures that could take

such developments into account if the records manager set out to do so. This would require political will on the part of management, however, and that might not always be forthcoming. PIPEDA describes key concerns that any records management unit should take into consideration while creating a retention schedule and accompanying policy documents and it describes the responsibilities of the record manager regarding information privacy and security as well as management's responsibilities toward the public and their own staff. The education of employees is a key, if perhaps often overlooked, feature of the government's elaboration on the act.

There may also be instances, especially during the planning stage of a retention schedule and privacy policy, when a records manager may want to consult a company's lawyer to ensure that they're working under the correct legislation, following tha legislation and accompanying regulations correctly, and ensuring they have developed suitable procedures for dealing with breaches or complaints. There doesn't seem to be anything in this legislation that is surprising, but that doesn't mean that it can be ignored or taken-for-granted; as the accompanying how-to guides and supporting information indicates, leadership from management, clear policies and procedures developed by a person or unit who are responsible for ensuring compliance, and training of staff so that everyone is aware of the policies, are essential to ensure success and prevent the need for complaints to or audits by the OPC.

References

OPC: Office of the Privacy Commissioner of Canada. (2007). Key Steps for Organizations in Responding to Privacy Breaches. Retrieved from: https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gl_070801_02/

OPC: Office of the Privacy Commissioner of Canada. (2013a). Key Steps for Organizations in Responding to Privacy Breaches. Retrieved from: https://www.priv.gc.ca/en/privacy-topics/privacy-policies/02_05_d_56_tips2/

OPC: Office of the Privacy Commissioner of Canada. (2013b). Ten tips for avoiding complaints to the OPC. Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-

personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/02_05_d_55_tips/

OPC: Office of the Privacy Commissioner of Canada. (2015a). Privacy Toolkit: A Guide for Businesses and Organizations. ISBN 978-0-660-06541-0. Retrieved from: https://www.priv.gc.ca/media/2038/guide_org_e.pdf

OPC: Office of the Privacy Commissioner of Canada. (2015b). The Application of PIPEDA to Municipalities, Universities, Schools, and Hospitals. Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_25/

OPC: Office of the Privacy Commissioner of Canada. (2016). About the OPC. Retrieved from: https://www.priv.gc.ca/en/about-the-opc/

OPC: Office of the Privacy Commissioner of Canada. (2018a). The *Personal Information Protection and Electronic Documents Act* (PIPEDA). Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

OPC: Office of the Privacy Commissioner of Canada. (2018b). PIPEDA in brief. Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

OPC: Office of the Privacy Commissioner of Canada. (2018c). PIPEDA legislation and related regulations. Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/

OPC: Office of the Privacy Commissioner of Canada. (2018d). PIPEDA compliance help. Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/

OPC: Office of the Privacy Commissioner of Canada. (2018e). Investigations into businesses. Retrieved from: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/

OPC: Office of the Privacy Commissioner of Canada. (2018f). Compliance Framework. Retrieved from: https://www.priv.gc.ca/biens-assets/compliance-framework/en/index#&ui-state=dialog

OPC: Office of the Privacy Commissioner of Canada. (2018g). How the OPC enforces PIPEDA. Retrieved from: https://www.priv.gc.ca/biens-assets/compliance-framework/en/index#

Justice Laws Website. (2018a). Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5). Retrieved from: http://laws-lois.justice.gc.ca/eng/acts/P-8.6/

Justice Laws Website. (2018b). Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5): Schedule 1. Retrieved from: http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-11.html#h-26