itworldcanada.com

Understanding Canadian cybersecurity laws: Privacy protection in the modern marketplace — PIPEDA (Article 3)

Melissa Lukings and Arash Habibi Lashkari

13-16 minutes

Introduction

With the global spread of COVID-19, on-line scams are circulating and malicious actors have been spreading malware intended to steal individual information through both personal and corporate networks. We previously outlined the provisions regulating governmental access to, use of, and disclosure of personal information established in the *Privacy Act* and the *Access to Information Act* in our last instalment of this article series.

Related:

> Understanding Canadian cybersecurity laws: The foundations (Article 1)
>
> Understanding Canadian cybersecurity laws: Privacy and access to information, the Acts (Article 2)

In this article, we will focus on the laws regulating private sector access to, use of, and disclosure of personal information as established in the PIPEDA.

***Personal Information Protection and Electronic Documents Act* (SC 2000, c 5)**

The *Personal Information Protection and Electronic Documents Act,* otherwise known as PIPEDA, officially became law in April 2000 as a means to help grow consumer trust in both electronic commerce and the digital economy. The PIPEDA was implemented as Canada's response to the widespread call to establish "fair information practices" in the private sector after international consensus was reached regarding the need to promote fairness in the handling of personal information more generally, rather than just in certain sectors (such as those sectors which were already covered in the *Privacy Act*). Regulations such as the *Breach of Security Safeguards Regulations*, and the *Secure Electronic Signature Regulations* were all made under *PIPEDA*.

Application

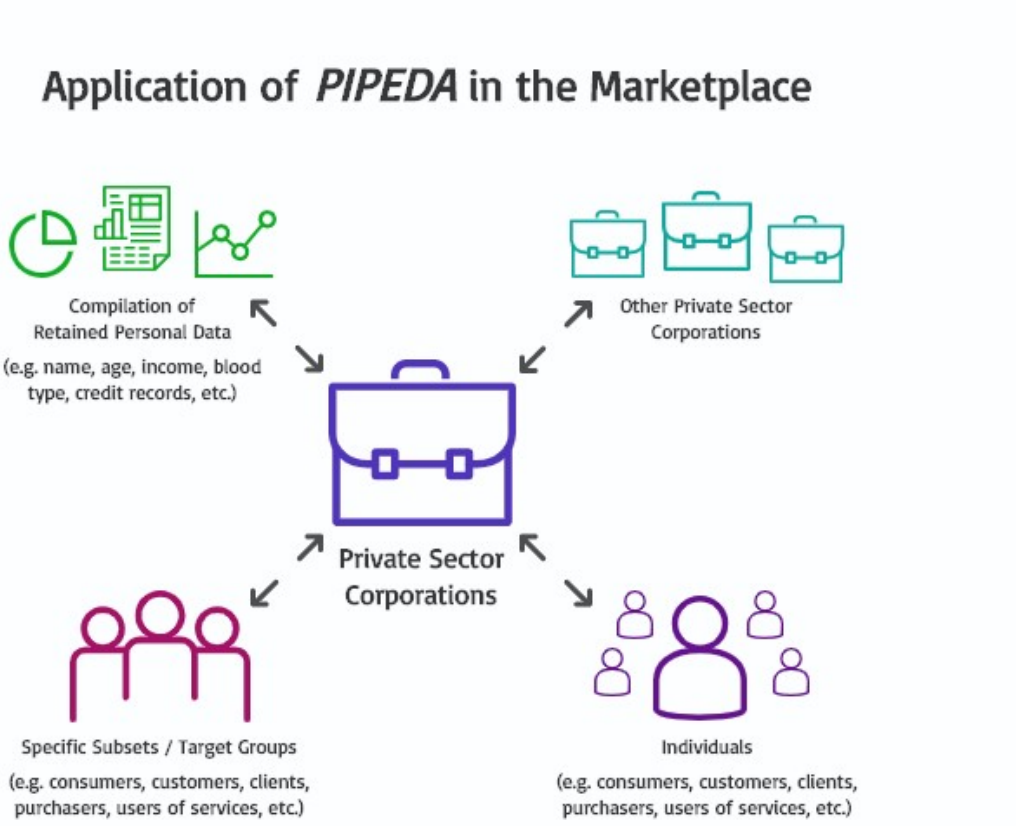
The PIPEDA applies specifically to: private-sector organizations; which are operating either fully or partially in Canada; and, that collect, use, or disclose personal information in the course of commercial activities. Specifically, "commercial activity" is defined in the PIPEDA as:

"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."

— *Personal Information Protection and Electronic Documents Act* (SC 2000, c 5)

Private sector organizations that fit into this category are bound by the provisions of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) to apply the privacy principles given in the PIPEDA to protect the consumer information exchanged during the commercial activity. These provisions aim to protect the privacy of those individuals, specific subsets / targeted groups of individuals, or organizations from whom the personal information has been gathered.

As discussed, the PIPEDA provisions do not apply to organizations wishing to access information held by federal government institutions. As with individuals, an organization can request access to their own personal information, as held by those federal government institutions, through the process outlined in the *Access to Information Act.*



PIPEDA provisions on personal information

Under the PIPEDA, “personal information” includes any factual or subjective information, whether recorded or not, about an identifiable individual and gathered during the course of commercial activity. This personal information can include your age, name, ID numbers, annual income, ethnic origin, blood type, opinions, evaluations, comments, social status, disciplinary actions, employee files, credit records, loan records, medical records, etc. The PIPEDA does not apply to the contact information for a business, including an employee’s name, title, business address, and the telephone number or email addresses that is used for the purpose of communicating with that person solely in relation to their employment or business.

The PIPEDA applies to private-sector organizations across Canada that collect, use or disclose personal information in the course of commercial activity. For the purposes of this legislation, the law defines a commercial activity 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. It also applies to all businesses that operate in Canada and handle personal information that crosses provincial or national borders, regardless of the province or territory in which they are based, including provinces with substantially similar legislation, and to federally regulated organizations that conduct business in Canada, such as airports, aircrafts and airlines, banks, transportation companies, telecommunications, offshore drilling, radio and televisions, etc.

The provisions set out in the *Personal Information Protection and Electronic Documents Act* **do not apply to not-for-profit or charity groups or political parties and political associations** unless they are engaging in commercial activities that are not central to their mandate and involve the access and use of personal information. It is also worth noting that fundraising is not considered to be a “commercial activity” in the context of applying the PIPEDA provisions to not-for-profit organizations, charitable organizations, foundations, societies, clubs, or sporting associations.

Exemptions to PIPEDA arise when a province already has its own privacy legislation. Those provinces are currently: Alberta, British Columbia, and Quebec. PIPEDA provisions can also be applied specifically to personal health information collected or handled in the provinces of: Ontario, New Brunswick, Newfoundland and Labrador, and Nova Scotia. These exemptions to PIPEDA apply only where the commercial activity actually took place within the relevant province. Additionally, an organization can be exempt from PIPEDA if they are collecting the personal information solely for “journalistic, artistic or literary purposes”.

If you consider the table below, we can see that the entities collecting personal information that are bound by the PIPEDA are: federally-regulated and private-sector **commercial organizations** and, in some cases, **health care professionals**. Those who are **not bound** by PIPEDA are **government institutions** at any level, **non-profits**, **charities**, **political parties**, and **individual citizens** (including specified political persons).

Which Privacy Law Applies?

Who is Collecting Personal Information?	**Examples**	***Privacy Act* or *PIPEDA*?**

Federal Government Institution	• Governmental Departments and Ministries • Port Authorities • Royal Canadian Mounted Police (RCMP) • Canadian Border Services Agency (CBSA) • Canada Revenue Agency (CRA) • Canadian Human Rights Commission (CHRC) • Canadian Radio-television and Telecommunications Commission (CRTC) • Correctional Service of Canada (CSC) • Parks Canada Agency • Public Health Agency of Canada • Statistics Canada	*Privacy Act*
Federally-Regulated Commercial	• Banks • Airports • Port services	*PIPEDA*

Organization	• Marine shipping • Ferries • Interprovincial railways and roadways	
Provincial, Territorial, or Municipal Institution	• Hospitals • Libraries • Universities • Public schools • Local transit • Municipalities	Neither. Provincial / territorial **public sector laws** will apply.
Private Sector Commercial Organization	• Stores • Restaurants • Entertainment • Tourism • Service business	*PIPEDA*
Not-for-Profit or Charitable Organization	• Canadian Red Cross • Heart and Stroke Foundation • Habitat for Humanity • Community groups • Professional/trade / service groups and societies	Neither. Provincial / territorial privacy legislation **may** apply.

	• Foundations • Social clubs and associations	
Health Care Professional	• Family doctors • Dentists • Psychologists • Physiotherapists • Specialists • Medical clinics	Determined on case-by-case basis. Either the *PIPEDA* **or** provincial / territorial **public sector laws** will apply.
Federal Political Persons (unless engaged in commercial activity fundraising excluded)	• Federal political parties • Political party campaign staff • Elected members of parliament • Staff of members of parliament	Neither.

Individuals (not acting in the capacity of any of the above)	• Friends • Family members • Colleagues / coworkers • Acquaintances • Peers • Strangers	Neither.

Purpose and Principles

The purpose of the *Personal Information Protection and Electronic Documents Act (PIPEDA)* is to build trust in your specific commercial enterprise and to build and maintain trust and confidence in the marketplace and in the digital economy.

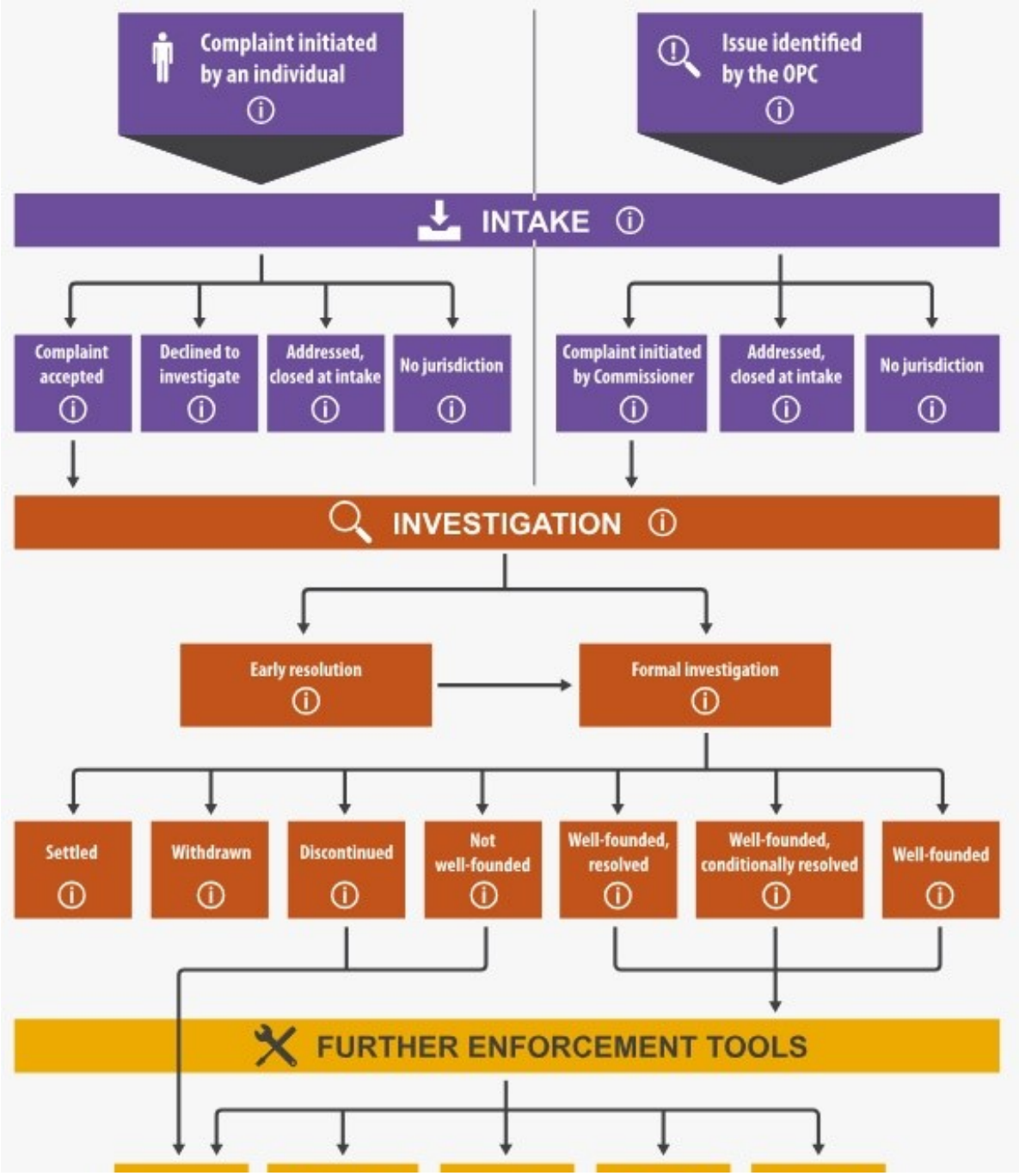
The ten main “fair information” principles that have been identified under the PIPEDA are: (1) accountability; (2) identifying purposes; (3) consent; (4) limiting collection; (5) limiting use, disclosure, and retention; (6) accuracy; (7) safeguards; (8) openness; (9) individual access; and (10) challenging compliance.

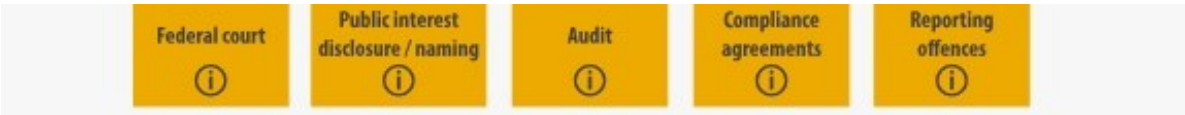
The general outcomes from combining these principles is that individuals from whom personal information is being collected must: give informed consent to the use of their personal information for the specific purpose, be able to access and correct the information, and feel assured that their information will be kept safely and their privacy respected. if the information is later sought to be used for a different purpose, fresh consent must be given to use the information for that new purpose. Organizations for whom PIPEDA applies are expected to adequately safeguard the

information against being used for any purpose without consent or from being disclosed to other parties.

Compliance

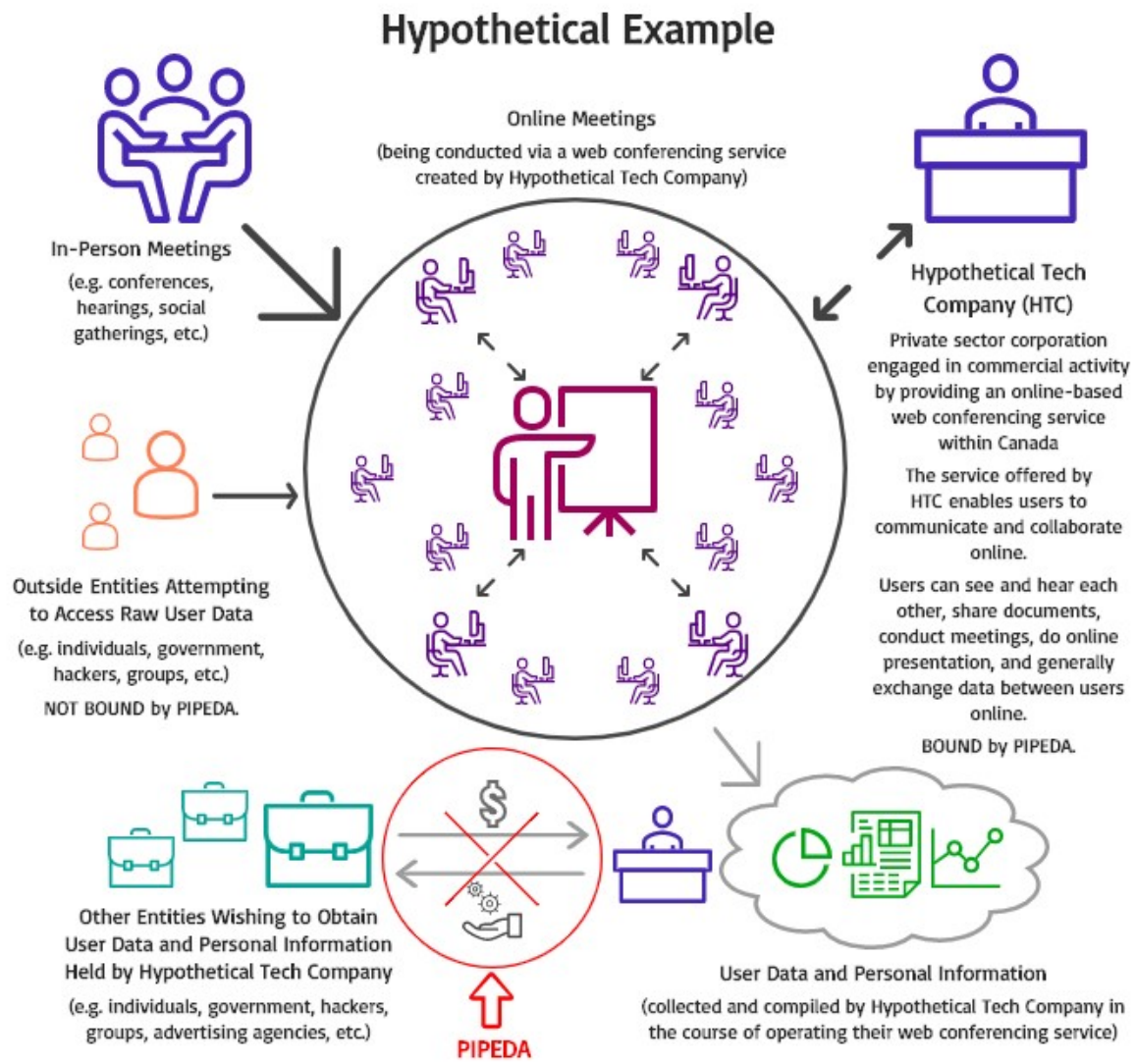
When a privacy breach occurs within the private sector, there are a range of possible outcomes. These are nicely summarized in this visually pleasing flowchart from the Office of The Privacy Commissioner of Canada:





Application in the real world

Since the outbreak of COVID-19, more and more people are moving their work and social activities online. The rapid development of online-based web conferencing programs and downloadable data sharing apps have become a necessary part of maintaining the global economy during a time of strict social distancing and isolation. This has raised questions among many as to the security features of such applications and the company policies regarding data protection.



As a hypothetical example of how the PIPEDA may apply in the real world, we can look at a made up example of Hypothetical Tech Company (HTC). In our example, HTC is a private-sector corporation engaged in commercial activity by providing an online-based web conferencing service to users within Canada. The service offered by HTC enables online communication, allowing its users to see and hear each other, share documents, conduct meetings, collaborate on material in real-time, and generally exchange data between users from the comfort of their own homes. HTC does not charge for access to the basic features of their service, but does have a user fee to access some extra features. HTC makes additional income through revenue gained from offering advertisement space on certain publicly-accessible areas of their user interface.

In this made-up scenario, HTC must comply with the provisions given in the PIPEDA regarding their collection, use, and disclosure of user data and personal information obtained during the course of operating their web conferencing service. The parties who are NOT bound by the PIPEDA in this scenario are: (1) the individual users of the web conferencing service; (2) outside entities attempting to access the information without consent; and (3) government institutions.

Conclusion

When you make a purchase, subscribe to a service, or otherwise engage in commercial activities, you want to be able to trust that any personal information obtained by that organization is kept in confidence and used appropriately, for whatever purpose for which

you agreed to give your personal information. It's also important to remember that the protection of personal information in the form of data is merely one part of privacy protection realm. As our technology advances and our world becomes smaller through the online global economy, we see the desire from both governmental bodies and private sector for other forms of citizen surveillance and personal monitoring. Quoting from Justice La Forest in the Canadian Supreme Court case of *R v Wong*:

"[I]n view of the sophistication of modern eavesdropping technology we can only be sure of being free from surveillance today if we retire to our basements, cloak our windows, turn out the lights and remain absolutely quiet."

Private-sector compliance with the PIPEDA and strict adherence to the principles of data protections given within PIPEDA is more important now than ever before. The global marketplace is vast and expanding. Technology has been shown to be a unifier of humanity during times of isolation. In our world of rapid technological change, emerging global health care crises, and a massive influx of the workforce suddenly moving online, we must remain vigilant in protecting user data and personal privacy in order to maintain the confidence of our consumers, our subscribers, our service users, and everyone within our national economy.

Would you recommend this article?

Thanks for taking the time to let us know what you think of this article!

We'd love to hear your opinion about this or any other story you read in our publication. **Click this link to send me a note →**

Jim Love, Chief Content Officer, IT World Canada

Related Download

Sponsor: **CanadianCIO**

Cybersecurity Conversations with your Board – A Survival Guide

A SURVIVAL GUIDE BY CLAUDIO SILVESTRI, VICE-PRESIDENT AND CIO, NAV CANADA

Download Now