itworldcanada.com

Understanding Canadian Cybersecurity Laws: Legislative Modernization — Responding and Adapting to Technological Change in a Global Domain (Article 9)

Melissa Lukings and Arash Habibi Lashkari

20-25 minutes

Introduction

One year ago: We had just launched into a new decade, in a time marked by rapid technological innovation, marketplace globalization, and polarizing social change. And then we froze. In what seemed like an instant, our sense of normalcy — in our social networks, our workspaces, our education, and the way we interact with others — shifted in the face of a global pandemic. With the viral wave, came the movement of our daily activities into the digital sphere. As we all learned to social distance, and gatherings of any size became few and far between, having the means to access and connect through digital technology became more of a necessity than a privilege. It has been almost a year since those initial days of panic and uncertainty.

As we approach the one year anniversary of the beginning of

widespread lockdowns (here in New Brunswick, it started with the March 13 announcement of school closures), we can all surely agree that the last 12 months have demonstrated how reliant we have become on our digital technology and how important it is to make sure that the technology we use and the ways that we use it are safe.

As in any market transaction, there must also be a level of trust by the consumer, that any personal information collected will be protected. Since its implementation in 2000, the *Personal Information Protection and Electronic Documents Act* has been the standard for commercial privacy practices relating to, among other things, the use, retention, and disclosure of any personal information collected during the transaction. As our needs have adapted to the growth of the digital marketplace, many longstanding cybersecurity concerns have now been brought to the forefront of legislative discussion, particularly so over the last few years. The Canadian response to this is the newly-proposed Digital Charter.

On November 17, 2020, the Canadian federal government launched a proposal for a Canadian Digital Charter, through the tabled proposal for the *Digital Charter Implementation Act, 2020*. This initiative was developed with the goal of fostering an interconnected Canadian digital economy while also preserving and reinforcing consumer trust.

The premise for developing and implementing a Digital Charter comes from the understanding that a national digital economy can only thrive if it takes on a principled and pragmatic approach to consumer privacy. That is, an approach that is based on fairness, accountability, openness, and transparency. Put simply, the *Digital*

Charter Implementation Act, 2020, as proposed, aims to keep pace with a modern and increasingly-digital society while continuing to provide the programs and services that help to enrich the lives of many Canadians.

In our previous articles, we explored the legal landscape of the current Canadian privacy and cybersecurity laws. The previous articles are included here:

- Understanding Canadian Cybersecurity Laws: The foundations (Article 1)
- Understanding Canadian Cybersecurity Laws: Privacy and access to information, the Acts (Article 2)
- Understanding Canadian Cybersecurity Laws: Privacy protection in the modern marketplace — PIPEDA (Article 3)
- Understanding Canadian Cybersecurity Laws: Interpersonal privacy and cybercrime — Criminal Code of Canada (Article 4)
- Understanding Canadian Cybersecurity Laws: 'Insert something clever here' — Canada's Anti-Spam Legislation (Article 5)
- Understanding Canadian Cybersecurity Laws: Peer-to-peer privacy protection — 'Intrusion Upon Seclusion' and the Protection of Intimate Images (Article 6)
- Understanding Canadian Cybersecurity Laws: Deep, dark, and undetectable – Canadian jurisdictional considerations in global encrypted networks (Article 7)
- Understanding Canadian Cybersecurity Laws: Measuring up — Outlining existing federal cybersecurity legislation in Canada, the UK, Australia, and the US (Article 8)

In this article, we will discuss the *Digital Charter Implementation Act, 2020,* which was tabled by the government on November 17, 2020*,* along with its progeny: the *Consumer Privacy Protection Act (CPPA*) and the *Personal Information and Data Tribunal Act.* We will outline the foundational premises of these new legislative regimes, how they will apply to organizations and businesses operating within Canada, and the corresponding legal implications for businesses and consumers.

Foundational principles of Canada's proposed Digital Charter

The Canadian National Digital and Data Consultations took place between June and October of 2018 and featured: Contributions from 6 Digital Innovation Leaders; 30 roundtable discussions; over 550 participants; and more than 1900 online engagements received through the associated website and online consultation platforms. From these consultations, the ten principles for Canada's *Digital Charter* were proposed. These Ten Principles of Canada's *Digital Charter* are:

(1) Universal Access

All Canadians will have equal opportunity to participate in the digital world and the necessary tools to do so, including access, connectivity, literacy and skills.

But what does that mean?

Increasing access to the internet and digital technology across Canada.

(2) Safety and Security

Canadians will be able to rely on the integrity, authenticity and security of the services they use and should feel safe online.

But what does that mean?

Requiring businesses that operate within the Canadian market to improve their data security practices.

(3) Control and Consent

Canadians will have control over what data they are sharing, who is using their personal data and for what purposes, and know that their privacy is protected.

But what does that mean?

Businesses may need to offer more clear and meaningful choices to customers about the ways and reasons why their personal information may be used.

(4) Transparency, Portability and Interoperability

Canadians will have clear and manageable access to their personal data and should be free to share or transfer it without undue burden.

But what does that mean?

Businesses may be required to help individuals move their personal information to another company, in some circumstances.

(5) Open and Modern Digital Government

Canadians will be able to access modern digital services from the Government of Canada, which are secure and simple to use.

But what does that mean?

The Government of Canada will provide more digital services.

(6) Level Playing Field

The Government of Canada will ensure fair competition in the online marketplace to facilitate the growth of Canadian businesses and affirm Canada's leadership on digital and data innovation, while protecting Canadian consumers from market abuses.

But what does that mean?

There will be new measures to increase competition and drive digital growth.

(7) Data and Digital for Good

The Government of Canada will ensure the ethical use of data to create value, promote openness and improve the lives of people—at home and around the world.

But what does that mean?

Businesses will be expected to take an ethical approach to using personal information.

(8) Strong Democracy

The Government of Canada will defend freedom of expression and protect against online threats and disinformation designed to undermine the integrity of elections and democratic institutions.

But what does that mean?

There may be new measures implemented to tackle interference in democratic processes and to assist in curbing the spread of misinformation disguised under the pretence of being a legitimate news story.

(9) Free from Hate and Violent Extremism

Canadians can expect that digital platforms will not foster or disseminate hate, violent extremism or criminal content.

But what does that mean?

There may be new rules for social media and other digital platforms to regulate hate speech and criminalize abusive online content.

(10) Strong Enforcement and Real Accountability

There will be clear, meaningful penalties for violations of the laws and regulations that support these principles.

But what does that mean?

There will be new powers granted to enforce Canadian privacy law.

We can summarize these principles in the table below.

Principle	Application to the Digital Charter	What It Means
Universal Access	All Canadians will have equal opportunity to participate in the digital world and the necessary tools to do so, including access, connectivity, literacy and skills.	Increased access to the internet and digital technology across Canada.
Safety and Security	Canadians will be able to rely on the integrity, authenticity and security	Requiring improvements to data security

	of the services they use and should feel safe online.	practices for businesses that operate in Canada.
Control and Consent	Canadians will have control over what data they are sharing, who is using their personal data and for what purposes, and know that their privacy is protected.	Requiring more clear and meaningful choices for customers regarding their personal data.
Transparency, Portability and Interoperability	Canadians will have clear and manageable access to their personal data and should be free to share or transfer it without undue burden.	Requiring businesses to help individuals transfer their personal information.
Open and Modern Digital Government	Canadians will be able to access modern digital services from the Government of Canada, which are secure and simple to use.	More digital services provided by the Government of Canada
Level Playing Field	The Government of Canada will ensure fair competition in the online marketplace to facilitate the growth of Canadian	New measures to increase competition and drive digital growth.

	businesses and affirm Canada's leadership on digital and data innovation, while protecting Canadian consumers from market abuses.	
Data and Digital for Good	The Government of Canada will ensure the ethical use of data to create value, promote openness and improve the lives of people—at home and around the world.	Requiring businesses to take an ethical approach in using personal information.
Strong Democracy	The Government of Canada will defend freedom of expression and protect against online threats and disinformation designed to undermine the integrity of elections and democratic institutions.	Implementation of new measures to curb the spread of misinformation disguised under the pretence a legitimate news story.
Free from Hate and Violent Extremism	Canadians can expect that digital platforms will not foster or disseminate	New rules for social media and other digital platforms to

	hate, violent extremism or criminal content.	regulate hate speech and criminalize abusive online content.
Strong Enforcement and Accountability	There will be clear, meaningful penalties for violations of the laws and regulations that support these principles.	New powers granted to enforce Canadian privacy law.

Digital Charter Implementation Act, 2020

In November 2020, the Honourable Navdeep Bains, Canadian Minister of Innovation, Science and Industry, introduced the *Digital Charter Implementation Act, 2020*, which serves to modernize the framework for private sector protection of personal information. This Act will take important steps to ensure that Canadians are protected by a modern and responsive law and that innovative businesses will benefit from clear rules, even as technology continues to evolve. It involves a three-step process:

Step One: Creation of the *Consumer Privacy Protection Act* to modernize Canada's existing private sector privacy law;

Step Two: Creation of the *Personal Information and Data Protection Tribunal Act* to establish an administrative tribunal to impose penalties for privacy violations;

Step Three: Repeal of Part 2 of the *Personal Information and Protection of Electronic Documents Act* to turn it into a distinct stand-alone legislation: the *Electronic Documents Act*.

Consumer Privacy Protection Act (CPPA)

The *Consumer Privacy Protection Act (CPPA)* was introduced in an effort to update and improve Canada's existing private sector privacy law and to increase the protection of Canadians' personal information by giving Canadians more control over how companies handle their information. The *CPPA's* legislative foundation is anchored by five core pillars:

1. Providing plain-language information for consumers so they can fully understand and meaningfully consent to the ways in which their data will, or will not, be used;
2. Providing the ability for consumers to transfer their private data between multiple private entities;
3. Providing the ability for consumers to be able to withdraw their data-usage consent and have their personal information be properly and permanently disposed of;
4. Providing increased algorithmic transparency requirements, with an emphasis on any systems relying on artificial intelligence or implicated in automated decision-making; and
5. Providing the ability for consumers to have personally identifiable information about themselves removed in certain circumstances.

Personal Information and Data Protection Tribunal Act

The *Personal Information and Data Protection Tribunal Act* will be enacted as proposed by the *Digital Charter Implementation Act, 2020* to create an administrative tribunal which will to hear appeals

of orders issued by the Privacy Commissioner and apply the administrative monetary penalty regime as it will be created under the *Consumer Privacy Protection Act*.

Together, the *Consumer Privacy Protection Act* and the *Personal Information and Data Protection Tribunal Act* are anticipated to:

1. Increase Canadians' control and transparency when their personal information is handled by commercial organizations;
2. Give Canadians the freedom to move their information from one organization to another in a safe and secure manner;
3. Ensure that when consent is withdrawn or information is no longer necessary, Canadians can demand that their information be destroyed;
4. Provide the Privacy Commissioner with broad order-making powers, including the ability to force an organization to comply and the ability to order a company to stop collecting data or using personal information; and
5. Provide for the strongest fines among G7 privacy laws.

Organizational implications and recommendations

Implication: Higher penalties

Currently, the PIPEDA only authorizes penalties for breach of the *Digital Privacy Act,* which are markedly lower than those authorized under the CPPA. The maximum fine for breaching the *Digital Privacy Act* is $100,000 per violation.

But soon there will be significant penalties for non-compliance with the *Consumer Privacy Protection Act*. It authorizes administrative monetary penalties and fines of up to 5 per cent of global revenue

or $25 million, whichever is higher, for the most serious offences. The maximum penalty for all of the recommendation contraventions, taken together, is the higher of CA$10,000,000 or 3 percent of an organization's gross global revenue in the financial year prior to the one in which the penalty is imposed.

Implication: Greater enforcement powers

Currently, individuals may file complaints or the Commissioner can initiate a complaint on its own initiative. Under PIPEDA, the Privacy Commissioner only has the power to make recommendations to a breaching organization and has the following powers:

1. To carry out investigations in respect of a complaint;
2. To enter into compliance agreements with organizations who are in contravention of the statute; and
3. To conduct audits regarding an organization's compliance with the statute.

But soon, the *Consumer Privacy Protection Act* will give the federal Privacy Commissioner broad power to make orders against organizations and to recommend penalties to a new "Personal Information and Data Protection Tribunal." The new "Personal Information and Data Protection Tribunal" will determine and levy any penalties – which will have the effect of a court order – and hear appeals from orders of the Privacy Commissioner. As under PIPEDA, the *Consumer Privacy Protection Act* provides that individuals may file complaints or the Commissioner can initiate a complaint on its own initiative. The Privacy Commissioner maintains the powers as given in PIPEDA:

1. To carry out investigations in respect of a complaint;
2. To enter into compliance agreements with organizations who are in contravention of the statute; and
3. To conduct audits regarding an organization's compliance with the statute.

However, the *Consumer Privacy Protection Act* also grants the Privacy Commissioner new powers:

1. To conduct an inquiry after investigating a complaint or in respect of the non-compliance with a compliance agreement.
2. To render a decision following an inquiry; and,
3. To issue a compliance order or a recommendation that the Tribunal impose a penalty if the Privacy Commissioner finds that organization has contravened the CPPA, including ordering for organizations to do the following:

(a) Take measures to comply with the statute;

(b) Stop doing something that is in contravention of the statute;

(c) Comply with a compliance agreement; and

(d) Make public any measures to correct its policies, practices or procedures.

The *Consumer Privacy Protection Act* also grants complainants and organizations a right to appeal any decision issued by the Commissioner in which it finds that the organization has contravened the CPPA before the Tribunal. This extends to any compliance order issued by the Commissioner against the organization and any decision issued by the Commissioner in which it decides not to recommend the imposition of a penalty.

Implication: Stronger consumer rights

The *Consumer Privacy Protection Act* creates a new privacy breach legal claim, in the form of a civil right of action. Where the Privacy Commissioner has decided that an organization violated an individual's privacy under the CPPA, and that finding is upheld by the Personal Information and Data Protection Tribunal, that individual can then sue the organization for compensation for the violation. This would be in addition to any penalties imposed by the Tribunal.

It also provides for new individual rights of data portability and deletion. Consumers can require an organization to transfer their data to another organization (subject to regulations that aren't yet available), likely to be a boon to open banking. Individuals can also require that an organization delete the personal information it's collected about them, subject to some limitations, in what appears to be a limited form of the "right to erasure".

Implication: Accountability

The *Consumer Privacy Protection Act* requires algorithmic transparency, in that consumers would have the right to require an organization to explain how an automated decision-making system made a prediction, recommendation, or decision. As well, the CCPA aims to simplify consent requirements for organizations by making some exceptions to when an organization must obtain an individual's consent to the collection, use or disclosure of the individual's personal information.

The *Consumer Privacy Protection Act* allows private organizations to establish a "code" and internal certification programs for complying with the law that the Privacy Commissioner will

approve. Once approved, the code will establish the organization's legal compliance obligations and make new rules around the de-identification of data – this includes allowing for organizations to use an individual's personal information without their consent in order to de-identify their data. Under certain circumstances, organizations can also disclose de-identified data to public entities for socially beneficial purposes.

Recommendations

1. Consider whether all your consent requests are meaningful and appropriate.
2. Review your Terms and Conditions and other legal agreements to remove any clauses that force your customers into giving consent.
3. Provide information about how you use and share your customers' personal information each time you request consent.
4. Set up a way to provide your customers with a copy of their personal information in an accessible format.
5. Think about how you can facilitate your customers' requests for the deletion of the personal information you hold about them.

Conclusion

The new law takes an expansive approach to applicability, expressly applying to all personal information an organization collects, uses or discloses, including interprovincially or internationally. This reflects the increased digitization and globalization of the global economy, which knows no border, and which the COVID-19 Pandemic has accelerated. It is notable that the federal government has not provided any indication with

respect to the timeline for adopting its proposal nor with respect to the transition period that will be afforded to businesses, once Bill C-11 is enacted, in order to adapt their practices before being exposed to new and potential onerous enforcement mechanisms.

In the next —and final — article in our Understanding Canadian Cybersecurity Laws series (Article 10), we will briefly return to the previous nine articles in this series, in a journey from the *Privacy Act* back in 1985 to the modernized Canadian Digital Charter of the near future.

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