ONTARIO SOCIETY OF PROFESSIONAL ENGINEERS

The Current State of the Law: Data Regulation in Canada

Sujoy Chatterjee, J.D., Certified Information Privacy Professional (Canada) (CIPP/C), Certified Information Privacy Manager (CIPM)

Executive Summary

1. Canadian law is going to change to align with General Data Protection Regulation (GDPR).
2. Change will happen at the federal and provincial level. Be prepared for both and watch for the harmonization of privacy laws internationally.
3. Have infrastructure in place on your teams to manage privacy as a program within your organization. This includes having a privacy office that manages requests in line with legislative requirements.

Bill C-11 commentary - Privacy Considerations

For OSPE members, how you collect, use, retain, and disclose the personal information of your clients, employees, and other stakeholders is an important business consideration. Significant changes were proposed in the 43rd session of parliament under what was then called Bill C-11: *The Digital Charter Implementation Act, 2020* (DCIA). The September 2021 election effectively put an end to any progress on Bill C-11 and it is unlikely that this Bill will become law before the end of 2022 (Shah et al., 2020). Nevertheless, it is important to discuss Bill C-11 for what it represents: a much-needed overhaul of private sector legislation relating to privacy, and data protection.

This Chapter discusses business considerations for Professional Engineers if the successor to Bill C-11 becomes law. New requirements around de-identification of data, data portability requirements, and consent impact how Professional Engineers manage private sector customer data. OSPE members should consider the following rules and behaviours in light of the proposed legislation. Now is an excellent time to plan for the changes that are likely to come as Canada looks to harmonize and catch up with privacy laws such as the European Union's General Data Protection Regulation (GDPR).

Background and existing legislative framework

Bill C-11 is a bellwether that we can use to understand where privacy laws are going in Canada over the next several years. The federal government is not alone in proposing changes to privacy legislation – Ontario is in the early stages of modernizing its privacy laws and benefits from the commentary and discussion that have surrounded Bill C-11.

Private sector businesses currently operate under the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). Bill C-11 proposed repealing parts of PIPEDA and replacing it with new legislation, namely the federal *Consumer Privacy Protection Act* (CPPA), the *Personal Information and Data Protection Tribunal Act* (PIDPTA), and the *Electronic Documents*

Act (EDA) (Government of Canada, 2020). PIPEDA would still exist, with its emphasis shifting to electronic documents and e-commerce instead of consumer privacy (Schober & Thompson, 2020).

Changes to Privacy requirements for businesses under the CPPA

The CPPA is of relevance to OSPE membership at large. Some of the key components of the CPPA are summarized below in **Table 1.** The changes that are highlighted include either entirely new sections, or sections of the CPPA that have been significantly modified from the corresponding section under PIPEDA.

Note that this section paraphrases what is written in Bill C-11 and is not a word-for-word transcription of the changes in the Bill. As such, interpretations of what is written below may differ slightly from the actual wording in the Bill. The language is modified for brevity and clarity.[1]

Table 1: Summary of Significant Changes to the Consumer Privacy Protection Act

Requirement	**Section(s) of the CPPA**	**Commentary**
Establishment of a Privacy Management Program	Section 9	Requirement for all businesses to establish/maintain policies and procedures for training personnel in privacy program management and ability to explain policies
Same protection of information	Section 11(1)	If your organization transfers personal information to a third-party service provider, the organization must ensure that the service provider provides substantially the same protection of the personal information as your organization.
Consent	Section 15	Requirement to obtain explicit consent from consumers at the time of data collection. Consumer must be made aware of the purpose of data collection, be able to understand the specific type of information that is being collected, used, or disclosed, and the names of any potential third parties to which the information may be disclosed.

[1] For a more precise depiction of the changes in the bill see the work of Teresa Scassa, https://dataverse.scholarsportal.info/dataset.xhtml?persistentId=doi:10.5683/SP2/ZVXFHY

Requirement	Section(s) of the CPPA	Commentary
Consent obtained by deception	Section 16	An organization must not obtain an individual's consent by providing false or misleading information or using deceptive practices. This includes the business providing a service to the individual, conducting due diligence, for security or information management purposes, safety, or in a situation where obtaining consent would be impracticable.
Business Activities	Section 18	An organization may collect or use an individual's personal information without their knowledge or consent for business activities.
Internal Research	Section 21	An organization may use an individual's personal information without their knowledge or consent for the organization's internal R&D purposes if the information is de-identified before use.
Prevention, detection, or suppression of fraud	Section 27(2)	An organization may collect an individual's personal information without their knowledge or consent if the information was disclosed to it in relation to fraud detection, suppression, or prevention.
Socially beneficial purpose	Section 39(1)	Disclosure without consent is permissible if personal information is de-identified. Information can be disclosed to certain public institutions such as a health care institution, post-secondary educational institution, public library in Canada or other organization with a mandate to carry out a socially beneficial purpose.
Initiative of organization — national security, defence, or international affairs	Section 48	For national security matters, defence of Canada, or international affairs, an organization may disclose an individual's personal information without consent to a government institution.

Requirement	Section(s) of the CPPA	Commentary
Disposal at individual's request	Section 55	If an organization receives a written request from an individual to dispose of personal information, the organization must dispose of the information as soon as feasible unless disposal relates to personal information of another person, or the organization is prevented from disposing of information by contract or law.
Service providers	Section 61	A service provider must notify as soon as possible when there is a privacy breach
Policies and practices	Section 62(3)	If the organization used an automated decision system to make a prediction about an individual, the individual can request an explanation of the prediction, recommendation, or decision and how personal information was used to achieve that.
De-identification of Personal Information – proportionality	Section 74	An organization that de-identifies personal information must ensure any technical and administrative measures applied to the information are proportionate to the purpose for which they information is de-identified as well as the sensitivity of the personal information.
Prohibition (on use of de-identified information)	Section 75	De-identified information cannot be used to re-identify an individual unless an organization is testing the effectiveness of safety and security measures.
Code of practice approval	Section 76 (note: this applies to sections 77- 81 which relate to administering a code of practice and are all new sections	An organization or entity can apply to the Federal Privacy Commissioner for approval of a Code of Practice for protection of personal information

Requirement	Section(s) of the CPPA	Commentary
	proposed under Bill C-11.	
Complaint (Investigation of)	Section88 (note: sections 82-102 address the complaint process	This section allows the privacy commissioner to conduct an inquiry after a complaint is made about an organization.
Nature of inquiries	Section 90(1)	The complaint investigation process may be a private inquiry. The Privacy Commissioner is not bound by any legal or technical rules of evidence in conducting an inquiry; this is an informal process meant to be expedient, with considerations for fairness and natural justice.
Penalties (recommendations)	Section 93	The Privacy Commissioner can make decisions about penalties (e.g., amount and whether a penalty is warranted) for organizations that have contravened the CPPA.
Promoting purposes of Act and Prohibition — use for initiating complaint or audit, respectively	Sections 109 and 110	The Privacy Commissioner has to develop educational materials to inform the public of the CPPA. This includes developing guidance materials for organizations to understand how to comply with the CPPA. An organization may request guidance from the Office of the Privacy Commissioner (OPC) with respect to their Privacy Management Program. The information obtained when providing guidance to an organization must not be used by the OPC to initiate a complaint or conduct an audit of the organization.
Offence and Punishment	Section 125	For an indictable offence (i.e., a serious criminal offence), fines of up to $25 million and 5% of the organization's gross global revenue may be imposed for breach of security, failure to retain records, improper use of de-identified information, or obstruction of an inquiry or investigation.

Requirement	Section(s) of the CPPA	Commentary
		For an offence punishable on summary conviction (i.e., a lesser offence) the maximum fine is $20 million and 4% of an organization's gross global revenue).

New requirements under the CPPA

Consent

The CPPA applies to protection of personal information that is collected, used, or disclosed in the course of commercial activities (CPA, 2002, s.6.1.a). Consent to the collection and use of customer data is a significant aspect of the CPPA and in particular there is an emphasis on providing easy to understand, plain language communications about how a business will be collecting, using and sharing information (CPA, 2002, s.15.3). Essentially, consumers should be able to understand how a business will use personal information and how the consumer has control to withdraw consent or have their information removed from company databases all together.

Bill C-11 addresses the consent-to-use-of-information issue more broadly by allowing an organization to rely more upon implied consent. Under PIPEDA (the existing private sector legislation), the knowledge and consent of the individual are not required for the disclosure of personal information. In limited circumstances, information collected for one purpose may be used for another related purpose.[2] There is indication within Bill C-11 to simplify how an organization obtains permission to use personal data. The implied consent model recognizes that an individual may not think about or understand all the different ways in which their information may be used in a complex information economy. Implied consent is used in processes such as preventing or detecting fraud – an organization should not require consent from an individual if it is acting to protect the individual's personal information from a potential criminal act. That said, with implied consent, the Office of the Privacy Commissioner has called for greater accountability by calling for privacy policies to be registered and reviewed by the Commissioner for organizations that are holding personal information.[3]

De-identification of data

The CPPA allows for the use of de-identified data for internal R&D and socially beneficial purposes without the consent of the individual (Shah et al., 2020).[4] Bill C-11 uses the term "de-identified data" as personal information that has been modified by using technical processes to

[2] See section 7(3) of the Personal Information Protection and Electronic Documents Act
[3] For more information, see Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the Digital Charter Implementation Act, 2020.
[4] Also see sections 20 and 21 of CPPA

ensure that the information does not identify an individual. Data that has been de-identified could not be used in reasonably foreseeable circumstances, alone or in combination with other information, to identify an individual.

This use has implications for data analytics, AI, machine learning, and B2B interactions. Organizations that that process data has to have an ability to use de-identified customer data. De-identification is also an element in the purchase or sale of a business. While PIPEDA currently allows organizations involved in the purchase or sale of a business to share personal information about their customers without consent, under the CPPA, the seller would be required to de-identify data before providing information as part of due diligence in the transaction. For small businesses (and start-ups in particular) investors and potential business partners will want to know the strategy around due diligence. It is prudent for businesses to have de-identification measures in place before it becomes a legal requirement (Shah et al., 2020).

Privacy Management Program

The CPPA requires maintenance of a Privacy Management Program for each organization. A Privacy Management Program must have policies and procedures explaining how your organization protects personal information, how you manage privacy complaints, privacy training for personnel, and an explanation of all privacy related policies and procedures. Small, data-intensive organizations may find it particularly challenging to implement these privacy practices.

Right to disposal

In other jurisdictions, the Right to Disposal is called the “right to be forgotten” or “right to erasure” wherein an organization is required to have a mechanism for the removal of personal information of individuals from their systems. The right is not absolute and is subject to legal retention obligations. In other words, an individual may request that a company remove personal information from company databases, as long as there is no legal obligation to keep that information.

Whether you are an organization that collects information directly from individuals, or you work with data processing and management along the supply chain, there are practical challenges to meeting this requirement (Shah et al., 2020). The right to disposal involves understanding record keeping, data storage, and employee access procedures. Organizations need to know where their data is stored, including redundancies. In order to ensure total removal of personal information relating to an individual, these systems must be audited and maintained. Doing so gives consumers more control over who has their data.

Data Portability

The CPPA casts data portability as a right for individuals. If an organization transfers personal information to a service provider, the organization must ensure that the service provider allows for substantially the same protection of personal information as the original organization (CPA, 2002, s.11.1). There is an opportunity here for OSPE members, particularly those in the start-up space.

More freedom for consumers to move their data to other organizations and the requirement to maintain similar privacy protection and data standards is a boon for companies that require customer data. The corollary is that start-ups will have to develop compliant data management frameworks with the purpose of distinguishing between the information organizations directly collect from individuals as compared to data created by your organization. Further information is needed about the CPPA's planned data portability framework before OSPE members can be advised on best practices to execute this. A starting point would be to look to the financial sector and how fintech based companies may be working on this data portability framework (Shah et al., 2020).

Trans-border data flows

Related to data portability, the flow of data across international borders has been highlighted by the Office of the Privacy Commissioner and others as a gap in Bill C-11 (Therrien, 2021). As practitioners, you may be familiar with "adequacy requirements" under the European Union's General Data Protection Regulation (GDPR). If data protection measures are deemed adequate, this permits a cross-border transfer of data outside of the EU. Bill C-11 has been critiqued for not having adequate protections in place for data transferred to third parties (Therrien, 2021). If this portion of the bill is strengthened, expect changes to requirements for data protection and consistency in security measures between other organizations that OSPE members would do business with.

New powers for the Office of the Privacy Commissioner: Penalties, fines, and investigative powers

Bill C-11 expands the powers of the federal Office of the Privacy Commissioner (OPC) to impose penalties for non-compliance, fines, and to allow for a private right of action after a finding of non-compliance by the OPC. Penalties and fines are delivered through the Personal Information and Data Protection Tribunal - this body would also be responsible for hearing appeals of orders issued by the OPC (Government of Canada, 2021).

Penalties

The OPC may recommend that an organization comply with the CPPA and publicly document its privacy practices to show compliance with OPC orders. Penalties for non-compliance can be significant – up to $10 Million or 3% of an organization's gross global annual revenue for contravening processing provisions or security safeguards. These are significant increases in the penalties for non-compliance as compared to PIPEDA, which currently limits penalties to $100,000 per indictable offence. OSPE members should be mindful of these requirements and consider how best to achieve compliance in a start-up or small business context.

Fines

Distinct from penalties, the OPC can also administer fines for when an organization knowingly contravenes the CPPA, whether in relation to a privacy breach, misuse of de-identified data, or failing to respond to an access request from a member of the public. Denying whistleblower

protection or obstructing OPC proceedings may also result in significant fines – up to $25 Million or 5% of gross global revenue, depending on the nature and severity of the offence. Mitigating this risk involves proper business insurance as well as legal and privacy advice. Also consider the reputational risks of having a conviction under the CPPA and what that would mean for the viability of business operations in the future (Shah et al., 2020).

Related Ontario legislation

Bill C-11 was not developed in a vacuum. Specific mention of the Federal Privacy Commissioner's comments on Bill C-11 have fed into Ontario's own modernization of privacy legislation. In June of 2021, the Government of Ontario released its White Paper discussing uses of data based on legitimate need and limiting use. There is also consideration of Artificial Intelligence and machine learning. While this is in its earliest stages, some consideration of what may be in the Ontario legislation includes:

- **Right to be forgotten:** also known as right to erasure, the requirement for an organization to remove data at the request of an individual
- **Data mobility and portability:** the ability to move data without loss of privacy protection rights.
- **Safe use of automated decision-making:** relating to surveillance, algorithmic bias, and Artificial Intelligence.

It will be difficult to predict how federal and provincial legislation will interact, given the positioning of Bill C-11 within the House of Commons, and the newly elected federal government. Both legislative efforts pose significant generational changes for privacy in Canada.

Conclusions and Questions for the Engineering Community

It will likely be several years before Canada's private sector privacy legislation changes to be more in line with EU and various U.S. privacy laws at the state level (i.e. in Colorado, Virginia, and California). The legislation proposed via Bill C-11 speaks to the consent and data management issues that are relevant for a variety of business organizations. Continued monitoring of legislative change across Canada is essential. Strategies can be developed to respond to new legislative requirements and minimize the disruptions faced by OSPE affiliated organizations. OSPE members should seek out resources to advise on the fast-changing landscape in privacy and information management.

Works Cited

Consumer Protection Act. (2002). Government of Ontario. https://www.ontario.ca/laws/statute/02c30

Government of Canada. (2020). Bill summary: Digital Charter Implementation Act, 2020. Government of Canada. https://www.ic.gc.ca/eic/site/062.nsf/eng/00120.html

Government of Canada. (2021). Bill C-11: An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make related and consequential amendments to other Acts. *Government of Canada.* https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c11.html

Schober, K. & Thompson, K. (2020). Canada's proposed new privacy law – Summary of business impacts. *JDSupra.* https://www.jdsupra.com/legalnews/canada-s-proposed-new-privacy-law-99504/

Shah, R., Reynolds, M., & Trivun, M. (2020). Bill C-11 and Startups: The Good, The Bad, and The Ugly. TORYS. https://www.torys.com/Our%20Latest%20Thinking/Publications//2020/12/bill-c-11-and-startups/

Therrien, D. (2021). Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the Digital Charter Implementation Act, 2020. *Office of the Privacy Commissioner of Canada.* https://priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ethi_c11_2105/