INQ DATA LAW

Privacy Law for the Digital Economy:
The new Digital Charter Implementation Act

The Canadian government has introduced a new bill that proposes major reform to Canada's privacy law and introduces initial regulation of Artificial Intelligence ("AI").

Executive Summary

If you have less than one minute to read about Canada's new privacy bill, this summary tells you what you need to know by answering two questions: (1) what are the major changes proposed under this new Bill? (2) what does this mean for your business?

What are the major changes proposed under this new Bill?

The DCIA was tabled in the House of Commons on Tuesday, November 17, 2020 as Bill C-11. This Bill, if passed, would further balance privacy interests with the recognition that data are fuel for Canadian competitiveness and innovation. The Bill's significant provisions are as follows:

1. Part I of Canada's current *Personal Information and Protection of Electronic Documents Act* ("PIPEDA") would be replaced by the new *Consumer Privacy Protection Act* ("CPPA").

2. The CPPA is being introduced under Part 1 of the DCIA. Part II of the DCIA introduces the Personal Information and Data Protection Tribunal ("Tribunal"), a new administrative tribunal empowered to levy significant fines for non-compliance with the CPPA.

3. The CPPA introduces some significant changes to Canadian private sector privacy laws, including:

    a. right to explainability and algorithmic transparency for all automated decision systems that assist or render decisions about an individual (see section 1 below);

    b. new exceptions to consent that would permit the collection, use and disclosure of personal information without consent for various purposes including new business operations (see section 2 below);

    c. stronger accountability requires including the codification of a privacy management program for all applicable businesses (see section 3 below);

    d. right to data mobility, which allows individuals to move their data from one platform to another (see section 4 below);

e. right to data deletion, in which an individual can both request that their data be deleted and, in some cases, withdraw consent for use of their personal information (see section 5 below);

f. new codes of practice and certification scheme on how the business will comply with the CPPA that can be pre-approved by the Privacy Commissioner (see section 6 below);

g. new private right of action for violation of the Act. This private right of action after the Privacy Commissioner refers the matter to the new Tribunal and either there is no further administrative recourse under the DCIA (see section 7 below);

h. stricter enforcement powers for the Office of the Privacy Commissioner as well as a new Tribunal capable of levying fines up to 5% of global revenue or C$25 million, whichever is greater (see section 7).

The DCIA aligns more closely with Europe's *General Data Protection Regulations* ("GDPR") while distinguishing Canada in important respects, namely regarding requirements for algorithmic accountability and by maintaining a principle-based approach to data protection.

The implications of this new law are far-reaching including the reconsideration of what it means for all provincial privacy laws such as the *Personal Health Information Protection Act* ("PHIPA") in Ontario to maintain its status as substantially similar to existing federal law.

What does this mean for your business?

Bill C-11 established in law the importance of good data governance practices. The Bill, if passed, would require a clear and well-documented privacy management program for all applicable organizations. This privacy management program should not be construed too narrowly. This Bill is starting to regulate technologies like artificial intelligence. More is yet to come.

Good data governance means documenting policies and procedures that follow the flow of data from collection to use and documents the various intentions and practices. Simply, this means your program should not focus narrowly on personal information but should start conceptualizing its program more broadly to include uses of data (both personal and non-personal information) within the organization. It is important to document:

- intentions; *i.e.* why your business seeks to use data for particular business objectives and applications (data/AI strategy);

- uses; *i.e.* where your data comes from and how it is being / will be used (both in terms of the business objective and application); and

- controls; *i.e.* what your business is doing to ensure data are being used as intended and that the uses (through AI or otherwise) are not causing harm or that potential harms are reasonably identified and mitigated.

INQ Data Law is supporting clients with a future-looking approach to privacy management programs that contemplate this diligent and robust approach to good data management practices. Contact us at cpiovesan@inqdatalaw.com or noel@inqdatalaw.com for more information.

Background: How we got here

May 2019 saw the release of Canada's first Digital Charter. The Digital Charter is a statement of ten principles that rearticulates Canadian values in the digital economy. The Digital Charter balances principles of control over one's personal information (principles 2-4) with promoting data as a fuel for competitiveness (principle 6) with enabling Canada to be a modern, ethical and accountable country for data use (principles 1, 5, 7-10).

At the time of its release, the Digital Charter was accompanied by a White Paper on reform of Canada's privacy law, "Strengthening Privacy for the Digital Age: Proposals to modernize the *Personal Information Protection and Electronic Documents Act*". In recent years, PIPEDA has been widely criticized for being outdated and unfit for a digital-first Canada. The new *Digital Charter Implementation Act* (Bill C-11) proposes to address many of the issues that have plagued PIPEDA for the several years, mainly as described in the White Paper.

Bill C-11: The Digital Charter Implementation Act (DCIA)

On November 17, 2020, the federal government tabled a long-awaited Bill in the House of Commons (Bill C-11) proposing major reform to PIPEDA that would more closely align Canadian private sector privacy laws with Europe's GDPR.

DCIA is an omnibus data protection Bill that not only regulates the collection, use and disclosure of personal information, but also regulates aspects of AI and establishes a new adjudication body, the Personal Information and Data Protection Tribunal, that can levy significant fines. Major developments under Bill C-11 are discussed in the following seven sections.

1. Regulating Automated Decision Systems

The adoption of automated decision systems is increasing in Canada and around the world. These systems raise a number of ethical and legal considerations about the fairness and transparency of the decisions, the right to object to decisions made by automated systems, and the right to meaningful recourse with a disputed automated decision. The CPPA addresses these concerns through a broad right to algorithmic transparency and explainability.

What are automated decision systems?

The CPPA adopts an expansive definition of automated decision systems, being: "any technology that assists or replaces the judgement of a human decision-maker using techniques such as rules-based systems, regression analysis, predictive analytics, machine learning, deep learning, and neural nets." This definition includes a wide range of possible computer systems as well as a broad scope of

applicability to "assists or replaces the judgement of a human decision-maker". This will implicate a large and growing number of computer systems and uses.

What obligations arise from using automated decision systems?

The obligations arising from automated decision systems under the CPPA are as broad as the definition itself. Section 63(3) of the CPPA proposes that, "if the organization has used an automated decision system to make a prediction, recommendation or decision about the individual, the organization must, on request by the individual, provide them with an explanation of the prediction, recommendation or decision and of how the personal information that was used to make the prediction, recommendation or decision was obtained." Arguably, this is qualified by s. 62(2)(c) which inserts language of "significant impacts on them [individuals]". Interpretation of applicability remains to be seen.

To put this in perspective, consider similar provisions in the context of GDPR. Article 22 of the GDPR is widely cited as leading regulation of automated decision systems. Article 22, however, is restricted to those decisions made "solely" by an automated system (unlike CPPA which is to *assist* or replace human judgment) and "which produces legal effects concerning him or her or similarly significantly affects him or her" (CPPA could be read as simply "about an individual"). Depending on the interpretation of scope under the CPPA, Canadian law could be more far-reaching that Europe's GDPR.

Moreover, s. 63(3) of the CPPA does not appear to be scaled according to the possible risk of the system. This is interesting given work already done by the Government of Canada in developing a Directive on Automated Decision-Making that requires an Algorithmic Impact Assessment to determine appropriate safeguards based on risk.

What does this mean for your business?

Under the CPPA, companies would be required to develop guidelines on algorithmic transparency and explainability for all computer systems caught by the new requirements under s. 63(3). Practically, this means that organizations should:

1. develop (or augment) policies on algorithmic transparency and explainability;
2. prepare a general account of how the organization makes use of automated decision systems
3. document criteria for a meaningful explanation in context of various use cases (s. 62(2)(c));
4. develop guidelines for explainability according to a risk continuum from low to high risk applications, with justification for the risk classification of the system and actions taken to mitigate risk;
5. appoint an appropriate steward to devise and draft (or produce) a meaningful explanation (noting s. 66 requirement for plain language); and,
6. develop complementary AI governance policies and procedures to support the broader AI strategy.

INQ DATA LAW

2. Beyond Consent

After much debate and discussion over several years, the CPPA seeks to change PIPEDA's reliance on consent as the basis for collection, use and disclosure of personal information in two main ways. ***First***, the CPPA seeks to make consent, when applicable, more meaningful for individuals. The CPPA includes requirements for clear, plain language about privacy practices. Currently, under PIPEDA, clear formatting and language about privacy is a best practice but not a regulatory requirement.

Second, the CPPA has identified a number of exceptions to the consent requirement. Notable is the new Business Operations exemption that includes the following exemptions to consent:

a) *business activities (s. 18(1))*. "Business activities" is triggered once a two part-test is met. The two part-test can be broken down as: (i) the reasonable person would expect their data to be collected or used in the intended manner; and (ii) the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions (e.g. not for direct marketing). This second part of the test if extremely broad and will be subject to much discussion. A list of business activities is provided for in the CPPA and more are likely to be identified in future regulations. For now, however, this list appears to be exhaustive and includes activities such as: delivering a product or service requested by the individuals; exercising due diligence in response to a commercial risk; and, where obtaining the individual's consent is impractical.

b) *transfer of information to a service provider (s. 19)*. This provision, permitting the transfer of personal information to a service provider for the purposes of assisting the primary data custodian, is a carry over from PIPEDA and helps to codify certain cross-border transfers that was otherwise a best practice under PIPEDA.

c) *de-identification of personal information (ss. 20, 74-75)*. This is a substantial inclusion in the CPPA. The definition of de-identified data includes modifying or creating new information that, among other things, cannot be used to in reasonably foreseeable circumstances to re-identify the individual. These provisions are in response to the ongoing confusion as to whether PIPEDA permits de-identification without consent.

   Under the CPPA, consent to de-identify would not be required ***but*** de-identified data would remain within the ambit of the CPPA. This is new and will need some clarification. Under all privacy law, once the information no longer about an identifiable individual (i.e. not personal information) it falls outside the jurisdiction of privacy law until issues of re-identification emerge. It would appear that's not the case under CPPA.

d) *research and development (s. 21)*. The research and development provision would permit the use of personal information without the consent of the individual if the information is de-identified.

e) *prospective or completed business transactions (s. 22)*. Section 22 would permit the use and disclosure of personal information without consent if (i) it is de-identified first, (ii) there is a written contract about the data between the parties and (iii) the information is necessary for the purposes of the transaction.

There are a number of additional permitted uses or disclosures without consent (see ss. 25 (public interest), 40 (investigations), 43 (disclosures to government), 49 (required by law), and 51 (publicly available information), most of which are found in PIPEDA or are otherwise an existing best practice.

No consent for new purpose

The CPPA's s. 12(4) also suggests that consent is not always required when an organization is to use personal information for a new purpose from the one disclosed upon collection. Whereas PIPEDA is explicit that consent is required if an organization is to use personal information for a new purpose (Schedule 1, 4.2.4: "unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose") this would no longer be the case under the CPPA ("If the organization determines that the personal information it has collected is to be used or disclosed for a new purpose, the organization must record that new purpose before using or disclosing that information for the new purpose").

What does this mean for your business?

Practically, this means your business will be permitted to collect, use and disclose personal information in certain circumstances without the need for consent. Organizations will need to put in place strong documentation practices to determine the reason consent is not required and the policy and legal structures to protect the use and disclosure of such information. Documentation is critical as the Privacy Commissioner can audit your practices.

3. Elevating Accountability Requirements

The CPPA's accountability requirements are more robust than those currently found in PIPEDA. In particular, requirements related to privacy management programs and documenting openness and transparency practices would be required by law.

Section 9 of the CPPA requires a clear and well-documented privacy management program that must include documenting:

a) the protection of personal information;

b) how requests for information and complaints are received and dealt with;

c) the training and information provided to the organization's staff respecting its policies, practices and procedures; and

d) the development of materials to explain the organization's policies and procedures put in place to fulfil its obligations under this Act.

The nature of the privacy management program will depend on the volume and sensitivity of the data. In addition, the CPPA seeks to impose on the Privacy Commissioner the obligation to provide guidance on

the organization's privacy management program, on request (s.109(e)). It will be interesting to see the volume of requests that the Privacy Commissioner will need to process.

What does this mean for business?

This requirement means a clearly document privacy management program that includes a full suite of privacy, security and AI policies and procedures.

4. Permitting Data Mobility

Sections 72 and 120 of the CPPA require organizations to, on request of an individual and as soon as feasible, disclose all information collected about that individual to an organization designated by the individual, as part of the new data mobility framework. This new requirement is intended to enhance the control individuals have over their data. The CPPS does not provide a lot of detail on this new requirement but notes that the data mobility framework will be subject to future regulation.

What does this mean for your business?

Mobility of data is becoming an international practice. There are technical and administrative challenges with permitting meaningful data mobility, particularly in the absence of stronger national and international technical interoperability and data harmonization standards. Nevertheless, businesses should develop as part of its data governance program technical and administrative processes for quickly promoting data mobility.

5. Right to Deletion and Withdrawal of Consent

Under s. 55, the CPPA allows individuals to request that organizations dispose of personal information they hold. In addition, in many cases, the CPPA would also permit individuals to withdraw consent for the use of their information (see s. 17). These obligations are new to the Canadian privacy landscape and align more closely with obligations under the GDPR.

What does this mean for your business?

If your business is already GDPR compliant, it is likely that your practices align with obligations under the CPPA. If not, you will need to develop technical and administrative policies and procedures to enable data deletion and to explain the consequence of withdrawal of consent (s. 17(2)).

6. Codes of Practice and Certification Scheme

The CPPA enables organizations to develop their own codes of practice or certification schemes in how they propose to comply with the law. These codes of conducts would be submitted to the Commissioner for approval. It is not exactly clear what the benefit of this would be for organizations, given that compliance with their own code of practice or certification program will not relieve them of their obligations under CPPA. This is an area that will be interesting to follow.

What does this mean for your business?

While there are still few details about what these codes of practices might look like, organizations should proactively think about what developing (or augmenting existing) codes or schemes, particularly to include those decision regarding de-identification standards and algorithmic risk assessment frameworks. By starting to establish these processes, your business will be better placed to promote consistency in practice between various jurisdictions in which you operate, build and maintain public trust, and mitigate foreseeable risks associated with data use.

7. Stricter Enforcement

One of the biggest changes being proposed in the CPPA relates to enforcement mechanisms that would be vested in the Privacy Commissioner. For example, the Privacy Commissioner now would have order-making powers. This has been an outstanding issue and topic of discussion for several years. Order-making powers would include an ability to order a company to stop collecting or using personal information or issuing recommendations for monetary penalties. Note the severity of the penalties that could be recommended by the Privacy Commissioner: 3% of global revenue or $10 million for non-compliant organizations; 5% of global revenue or $25 million in cases of serious breaches or violations.

The CPPA also includes provisions to create a new Personal Information and Data Protection Tribunal. The Tribunal will hear appeals of Privacy Commissioner orders. It will also have the power to issue its own penalties and overrule the Commissioner's determinations, where appropriate.

Finally, the CPPA provides for a private right action for non-compliance with the law. The right of action is limited in that it can only be triggered when i) the Privacy Commissioner has made a finding that the organization is in contravention of the CPPA; ii) the determination is not appealed or that the appeal has been dismissed; and iii) that the action be brought within two years of the ruling.

What this means for your business?

The CPPA provides for a private right of action that could expose your business to the possibility of legal action for violation of the CPPA. Greater enforcement powers and the new Tribunal means that you business could face substantial administrative monetary penalties, rivalling those found under the GDPR. Getting your business ready from a technical and administrative perspective to track, justify, manage and document data is essential to Canadian and international compliance.

Conclusion

The CPPA, if passed, would usher in long-awaited reform to Canada's privacy laws. This new law seeks to balance the individual rights over their personal information with recognition that data are a fuel for competitiveness and innovation. This law would help position Canada as a global leader in responsible innovation. There are several major proposed changes, most notably in the enforcement of the law. Businesses need to be ready for these changes to the law in Canada and, increasingly, around the world.

The CPPA is just the beginning of what we can expect to see in the regulation of data use using emerging technologies like artificial intelligence. Getting ready now will set up your business for smoother, more compliant and more trustworthy processes under new law.

Carole Piovesan is a partner at INQ Data Law. In 2018, Carole served as a digital leader at the request of the Minister of Innovation in the national consultations that led to the Digital Charter.

Noel Corriveau is senior counsel at INQ Data Law. Noel was the principle architect of Canada's Algorithmic Impact Assessment and senior advisor to the Chief Information Officer of Canada.

Many thanks to Ellen Xu for her contributions to this article.