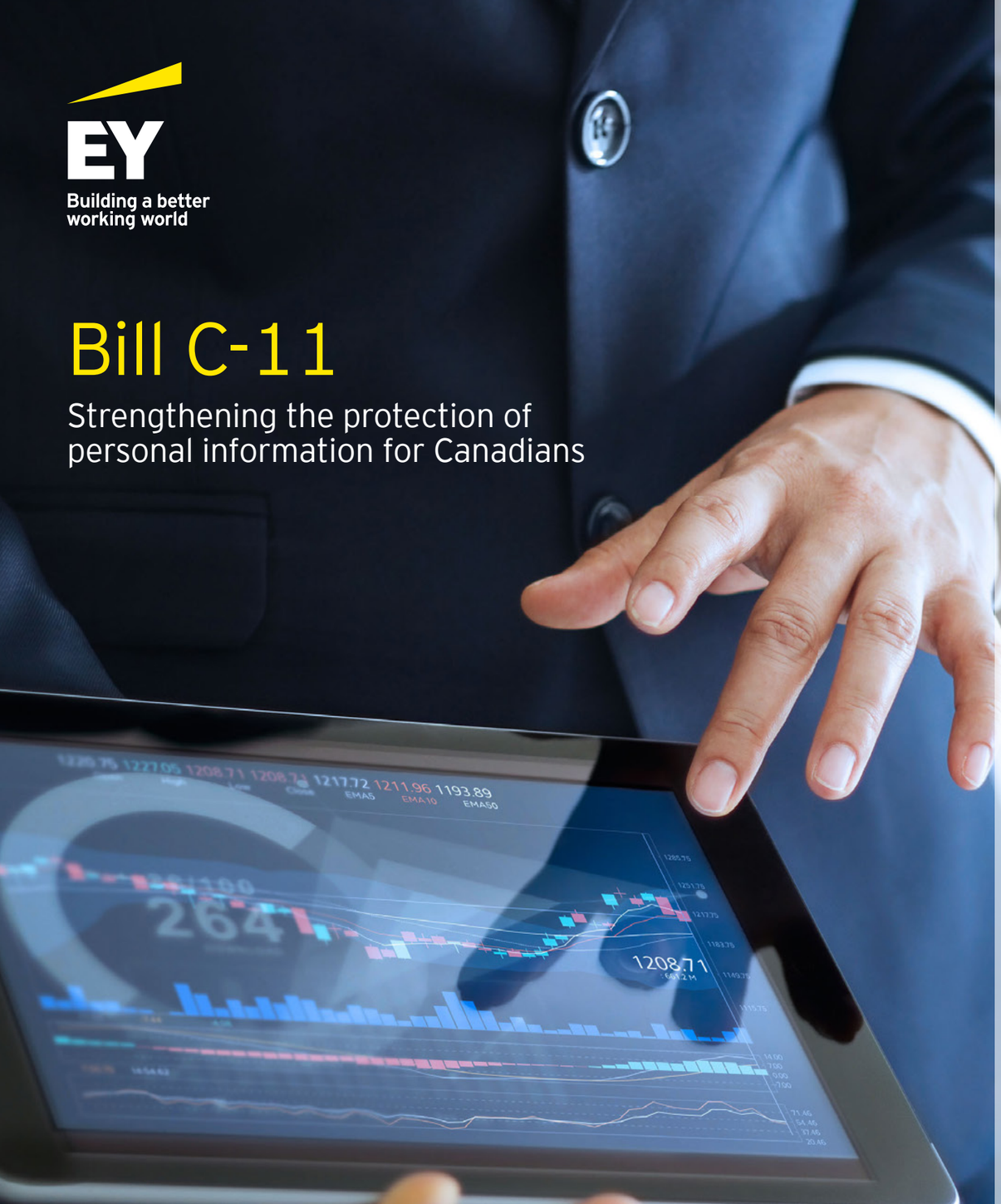
Building a better working world

Bill C-11

Strengthening the protection of personal information for Canadians



EXECUTIVE SUMMARY

Bill C-11, the proposed legislation, known as the *Digital Charter Implementation* Act, seeks to overhaul the framework for the protection of personal information in the private sector. This consolidates the implementation of Canada's Digital Charter[1] and would enact a new privacy law for the private sector, the *Consumer Privacy Protection Act* (CPPA). The law modernizes protections and grants individuals control and transparency over their personal information.

- Increasing control and transparency for Canadians when organizations handle their personal information
- Additional responsibilities for organizations handling personal information
- Enforcement measures through broad order-making powers, increased fines and a new enforcement tribunal

While it's not yet law, the CPPA sends a strong signal that Canada is keeping privacy as a priority. Organizations potentially impacted by the CPPA should start working on understanding and planning for its operational impact and potential opportunities. In doing so, they will have more time to do the proper planning and achieve an effective execution.

1 Canada's Digital Charter, Trust in a Digital World: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html

KEY CHANGES PROPOSED THROUGH THE CPPA

Individual rights

- **Enhanced data subject rights (access, mobility, deletion):** The CPPA would allow Canadians to have clearer and more manageable access to their personal data. Canadians would have the additional ability to share or transfer their data (right to data portability) and demand their information be destroyed (right of erasure).
- **Meaningful consent:** The CPPA would modernize meaningful consent to empower Canadians in exercising more control over the personal information they are sharing and the purpose for which such information is being used. Obtaining consent would need to be done in plain language, ensuring that individuals can fully understand what they are consenting to. The CPPA also seeks to codify and clarify circumstances in which an organization does not have to rely on express consent.
- **Automated decisions:** The CPPA also introduces requirements for more transparency surrounding automated decision-making processes and resulting decisions. This means individuals will have the right to an explanation of any predictions, recommendations or decisions, and how their personal information was obtained.

Organizational responsibilities

- **Explicit privacy management program:** Organizations are required by Section 9 to implement a "Privacy Management Program" that sets out and maintains data protection and privacy policies and procedures that are accessible to the Office of the Privacy Commissioner of Canada.
- **Clear obligations on service providers:** The CPPA would impose specific obligations on service providers, including breach notification requirements.
- **Certification programs:** If passed, the CPPA would create a framework for third-party codes of practice and certification programs. Furthermore, organizations would be able to ask the Commissioner to approve such codes or certification programs.
- **De-identification:** The CPPA would enable organizations to use personal information for certain purposes without the data subject's knowledge or consent, provided they de-identify the information.

Enforcement

- **Increased penalties:** The Commissioner would be able to recommend administrative monetary penalties for an expanded range of offences for certain contraventions of the law. The penalties for CPPA contravention could be as much as $10m or 3% of the organization's global revenue or, for some offences, the greater of $25m or 5% of global revenue.
- **New private right of action:** The CPPA would empower individuals with a private right of action, which would allow them to claim damages for loss or injury that they have suffered as a result of a contravention of CPPA.
- **Enforcement tribunal:** The *Personal Information and Data Protection Tribunal Act* would be enacted to create a Tribunal to hear appeals from the CPPA, and may impose penalties for contraventions, as recommended by the Commissioner.

WHY YOU SHOULD CARE NOW

While the CPPA is not yet law, you should start acting now to understand the operational impact and opportunities it would afford. This will give organizations time to design and implement all the necessary privacy controls while considering the following:

Trust and transparency

As consumer data continues to be a source of competitive advantage, organizations must proactively move towards trust-based and transparent privacy programs that earn and sustain consumer confidence.

Trend

This proposed legislation is a strong signal that Canada looks to keep pace and remain interoperable with other countries' actions in trust and privacy. The CPPA will continue its review process after the Office of the Privacy Commissioner submitted comments to the House of Commons. This also comes on the heels of Québec's Bill 64[2] and Ontario's consultations[3] on strengthening privacy protections.

Operational gaps

You will need to start thinking about the operational capabilities you will need to comply with the expanded rights and responsibilities under the CPPA. You should assess whether your current operating models — including people, data strategy, systems and processes — will be able to support your expanded responsibilities under the CPPA.

Emerging technologies

You will need to understand how the CPPA will impact key technology initiatives (e.g., cloud, artificial intelligence/machine learning). With the upcoming CPPA, complexities regarding these initiatives will only increase over time. For example, organizations will have to realign with third parties on how shared personal information is managed by the various parties involved.

Penalties

The CPPA provides for significant penalties that are among the strongest fines in the G7. Penalties can consist of fines up to the greater of $10m and 3% of the organization's gross global revenue in its prior financial year, or for some offences up to the greater of $25m or 5% of the organization's gross global revenue.[4]

2 June 12, 2020.
3 Conducted August 13 to October 16, 2020, https://www.ontario.ca/page/consultation-strengthening-privacy-protections-ontario.
4 Applies to Section 13, Subsection 14(1), (a) section 13; (b) subsection 14(1); subsection 15(5); (d) section 16; (e) section 53; (f) subsections 55(1) and (3); subsection 57(1); (h) subsections 58(1) and (3).

HOW EY CAN HELP

At EY, we believe that a strong business reputation needs a robust data privacy and trust program. In addition, organizations need to develop processes and capabilities to embed data privacy in day-to-day activities and support compliance efforts across all areas of operations. Our services are rooted in the experience we've gained from assisting organizations around the world to help you address your organization's unique and changing requirements in a flexible way. In addition, EY's Data Trust Framework not only complies with privacy regulations around the world but helps organizations convert their data risk into data trust.

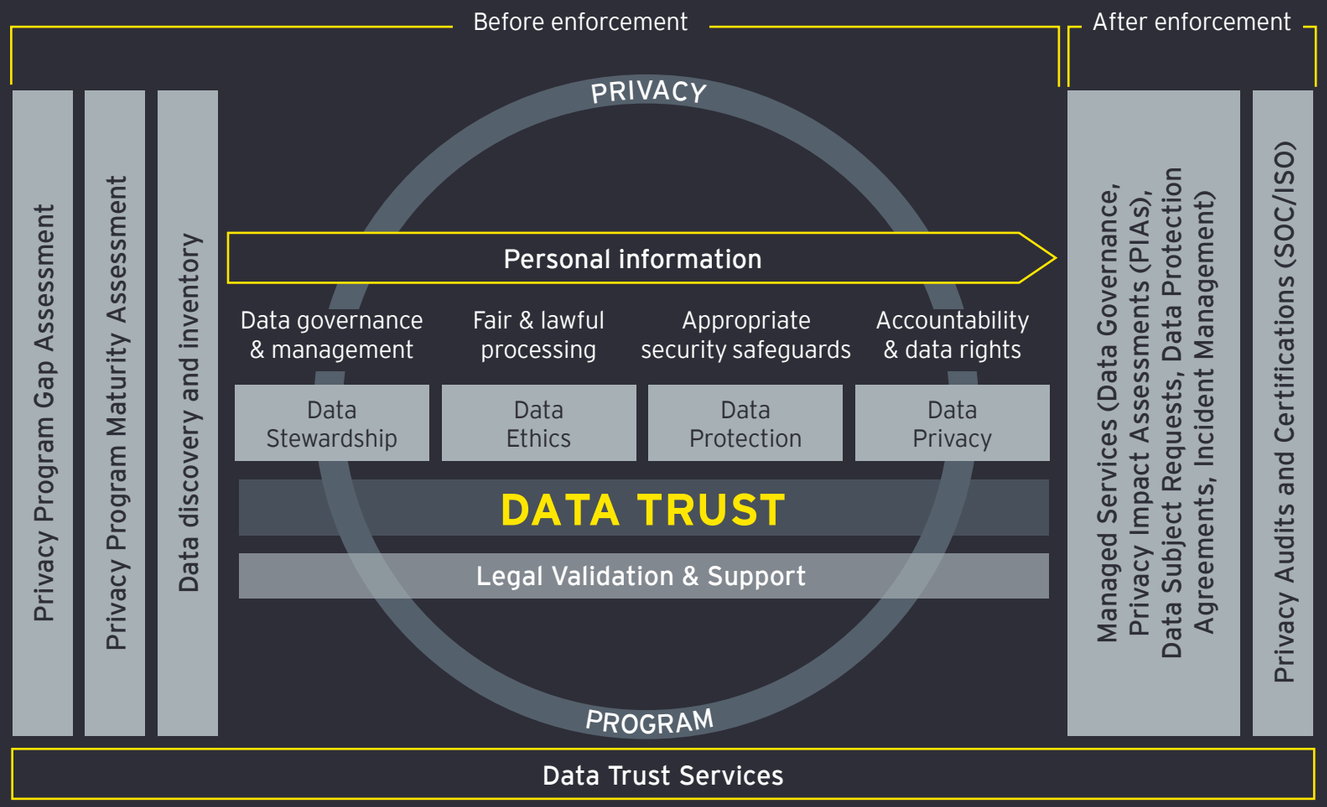
Category	Our services	
Knowing your current state. To define an effective and efficient way to respond to privacy considerations, it's imperative to understand what personal information an organization holds, how it is being managed and where it is maintained.	▸ Personal information inventory ▸ Data mapping ▸ Privacy program assessment ▸ Privacy impact assessment ▸ Artificial intelligence algorithm assessment ▸ Third-party (vendor) assessment	▸ Cross-border data transfer assessment ▸ Internal audit support ▸ Privacy program management office ▸ Define/review policy framework ▸ Design/review processes
Defining your future state: An effective response to privacy regulations requires the definition of a privacy program that enables the continuous demonstration of accountability and compliance. This needs to be enabled through a model that emphasizes accountability, efficiency and effectiveness in the way an organization manages personal information.	▸ Privacy program definition and implementation ▸ Privacy strategy and roadmap design ▸ Digital identity enablement ▸ Data privacy breach management and response ▸ Data retention and records management program design and implementation ▸ Third-party privacy management program design and implementation	▸ Privacy awareness, education and training ▸ Consent program development ▸ Individual's request response procedures design and implementation ▸ Cross-border data transfer protection program design and implementation
Responding to your needs: Depending on the nature of your business or the challenges your organization are experiencing, you may require very specific and specialized assistance. Our professionals can meet your business requirements with the right privacy context.	▸ Privacy managed services ▸ Data portability enablement ▸ Due diligence privacy assessment for mergers and acquisitions	▸ AI governance and ethics program design and implementation ▸ Open banking implementation and privacy strategy ▸ Trust-by-design implementation

DATA TRUST LIFE CYCLE

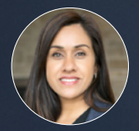
EY's data trust services are executed in a phased approach and offer comprehensive coverage to ensure a robust data trust program.

EY has significant experience in helping our clients to meet their privacy and data trust needs; we help organizations to embed data privacy into day-to-day activities using existing and emerging tools and support compliance efforts across all areas of the organization.

- Multi-disciplinary by integrating the legal, IT, risk and business perspectives of privacy.
- Single EY Legal & Advisory Privacy offering to translate legal requirements into a risk-based, customized approach.
- Identification of pragmatic implementation options for privacy regulation readiness with minimal operational impact.
- Proven success in roll-out in multiple sectors and countries, with EMEIA reach and connectivity to other jurisdictions.



CONTACT US



Roobi Alam
Privacy & Data Trust Leader
roobi.alam@ca.ey.com
+1 416 943 3284

Carlos Chalico
Privacy & Data Trust Senior Manager
carlos.perez.chalico@ca.ey.com
+1 416 943 5338

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

3648855
ED 00

ey.com/ca