This report was made possible by the generous support of our sponsors

Platinum

Microsoft

Gold

Algonquin College, Enbridge, Facebook

Silver

LoyaltyOne, University of Ontario Institute of Technology

Google, RBC, Rogers
Over the course of the last 18 months, the Canadian Chamber of Commerce has been collaborating with numerous organizations to examine the state of data governance in Canada.

Our first release, *Data for Good: The $32-billion Boost*, provided context and argued for the freedom to responsibly use data for innovation and growth in the face of increasing pressure to regulate the collection, use and disclosure of information. That paper demonstrated how personal data is used to innovate and create products and services that improve people’s lives and add convenience. It also highlighted the important distinction between sensitive personal data and non-personal data and pressed the need for policy-makers to not conflate the two.

The follow-up release, *A Data Deficit: The Risk of Getting It Wrong*, highlighted how the Equifax data breach and the Cambridge Analytica incident had soured public perceptions of how data is collected and used. It pointed out that there are “good guys” and “bad guys” in the world of electronic commerce and underscored how businesses often lacked the protections private individuals would be afforded if defrauded. It also examined some of the unintended economic consequences of regulating in this new digital era.

In this final edition of our three-part series, we recognize the need to rebuild trust in the online environment and lay out a prescription for keeping the innovation door open.
Privacy and Economic Interest

Both regulators and industry must build trust with stakeholders in the age of the internet economy. The business community values its customers. Without customers, there is no business model because stepping outside of what customers expect will inevitably harm the bottom line; there is a built-in, self-regulating motivation that drives responsible corporate behaviour. Amidst the negative publicity surrounding major breaches of security safeguards, industry has responded with changes in practice and is guided by organizing principles and codes of practice, like the International Chamber of Commerce (ICC) Advertising and Marketing Communications Code.

The ICC notes that:

The value and effectiveness of marketing and advertising depend on consumer trust. Self-regulation protects consumers and provides a cost-effective, accessible and responsive alternative to other legal avenues. Setting and enforcing best practices for industry gives consumers clarity on standards and recourse while freeing up scarce government resources to focus on rogue traders and other fraudulent practices. Self-regulation also allows greater flexibility than regulation, permitting rapid and measured adjustments to changing technologies and other new market factors.1

In A Data Deficit: The Risk of Getting It Wrong, we explained how a prescriptive approach to regulating the collection and use of personal data could have unintended, negative economic consequences. Canada’s privacy legislation, the Personal Information Protection and Electronic Documents Act (PIPEDA), has stood the test of time because it is based on fair information principles (FIP): principles that support both privacy and innovation. This principle-based and technology-neutral law, supplemented by regulatory guidelines and evolving best practices, has required industry in Canada to comply—by innovating responsibly—for nearly two decades. These two policy objectives—privacy and innovation—must continue to be supported by PIPEDA. While no regulatory regime is immune to the passage of time, the current balanced framework is still sound and does not require a fundamental overhaul.

1 https://iccwbo.org/publication/icc-advertising-and-marketing-communications-code/
PIPEDA is a strong law that holds companies accountable. Under PIPEDA, companies are accountable for protecting the privacy and personal information of Canadians. There are strict limits to data collection, use and disclosure. Companies must consider the impact on individuals and the sensitivity of their data. They must be transparent with those whose data they process.

Privacy advocates often cite the European Union’s GDPR as the gold standard for privacy regulation, with some calling for its application here in Canada. Yet, much of what is good about GDPR has been a mainstay of PIPEDA and Canadian business practices for over 15 years. PIPEDA mandates accountability, elements of privacy by design, impact assessments, breach reporting and access rights, but does it in a way that offers enough flexibility for companies to demonstrate how they comply, leaving room for innovative ways of doing so.

The GDPR remains unproven, and many believe it may hinder innovation in Europe, especially among small businesses. Canadians have the advantage of evaluating these initiatives from a distance. Legislation crafted by European politicians to satisfy their own environment and reflect their own culture and legal system may not be easy to transpose, particularly in light of Canada’s other pieces of framework legislation, including the Competition Act and Canadian Anti-Spam Legislation. Canadian framework laws have proven to be interoperable, affording an appropriate degree of flexibility while protecting privacy and personal information in different social and legal contexts.

Canada should continue to foster privacy in a thoughtful way, leveraging private initiatives and regulatory tools where appropriate. What is often omitted in the global narrative on data is that, 95% of the time, the data we are speaking of is the digitization of the information that is readily observable in the analog world, (i.e., hiring students to count cars at an intersection). The sensors that comprise the internet of things are merely a more efficient and accurate way of capturing and managing that readily observable information. As noted by the Centre for Data Innovation in a recent blog vis-à-vis Europe and the GDPR:

“Regulation can help to build confidence in a technology when there is a specific problem with a clear solution. But like a drug, regulation has side effects, is not appropriate in every case, and overdoses of it can be devastating.”

Building upon the previous two reports and the countless hours of stakeholder sounding and research that went into them, the Canadian Chamber of Commerce recommends the following policy solutions to help Canada get its regulatory framework right, ensuring that only appropriate regulatory tools are selected and that they clearly distinguish between personal data and de-identified, non-personal data. Our recommendations focus on three important goals:

2 https://euobserver.com/opinion/
In considering changes to Canada’s privacy laws as a means to build trust in the digital economy, the Government of Canada should:

Fix only what needs fixing

First, distinguish between truly personal sensitive data and the massive streams of non-personal data when considering additional measures or adjustments to current measures in Canada’s privacy legislation or related regulations. Problems regarding existing Canadian privacy laws need to be clearly stated with supporting facts. Then, and only then, should additional measures be considered and evaluated through a cost-benefit analysis. Where there is a vacuum and real need, governments should encourage the creation by industry of voluntary codes of conduct or certification, where industry can lead in developing industry solutions, which is what they do best. Government regulation should be the last resort, not the first implement used.

Use other framework legislation

Canada has many tools at its disposal to address concerns without increasing Canada’s already heavy regulatory burden. For example, competition law addresses some of the imbalances on how data sets are used, such as misleading or deceptive advertising and anti-competitive behaviour. Anti-spam legislation addresses issues of consent for electronic messaging and spam—some of which may lead to the spread of malware.

Encourage education and digital literacy

More rules do not necessarily improve compliance. However, more education and greater outreach improve compliance and encourage best practices that can lead to innovation. This goal could be realized through additional funding for the Office of the Privacy Commissioner (OPC), not as additional enforcement resources but to educate small- and medium-sized enterprises (SMEs) and individuals.

Meet the innovation security challenge

Government should focus on the real overarching problems when it comes to cyber breaches instead of placing blame solely on businesses. We need stronger action against cybercriminals who cause the most harm through identity theft, fraud, cyberbullying and reputational assaults. Government agencies should follow the evidence and prosecute those who commit fraud online. Government should also continue to expand the reach of the Cyber Incident Centre to educate and protect Canadian businesses. The federal government should enlist the help of the business community in pursuing such initiatives.
Holding government accountable

Where new regulation to protect private information is necessary, the burden on companies should be proportionate to the circumstances and targeted to solve a specific problem or gap in Canadian legislation.

While Canada continues to enjoy a high degree of internet freedom—as of 2017, Canada had comparatively fewer government requests for user data—recent events highlight the need for the government to focus on obvious gaps.

Global number of user data requests issued to Google from federal agencies and governments during 2nd half 2017, by country

<table>
<thead>
<tr>
<th>Country</th>
<th>Amount of data requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>32,742</td>
</tr>
<tr>
<td>India</td>
<td>12,171</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>7,455</td>
</tr>
<tr>
<td>Germany</td>
<td>5,067</td>
</tr>
<tr>
<td>France</td>
<td>4,249</td>
</tr>
<tr>
<td>Brazil</td>
<td>2,529</td>
</tr>
<tr>
<td>Italy</td>
<td>2,059</td>
</tr>
<tr>
<td>Poland</td>
<td>1,476</td>
</tr>
<tr>
<td>Pakistan</td>
<td>1,320</td>
</tr>
<tr>
<td>Argentina</td>
<td>1,290</td>
</tr>
<tr>
<td>Canada</td>
<td>1,220</td>
</tr>
<tr>
<td>Spain</td>
<td>1,151</td>
</tr>
<tr>
<td>Mexico</td>
<td>1,084</td>
</tr>
<tr>
<td>Australia</td>
<td>722</td>
</tr>
<tr>
<td>Portugal</td>
<td>679</td>
</tr>
</tbody>
</table>

Source: Google, H2 2017
In 2017, Statistics Canada requested that a private company hand over the credit ratings, including personal identifiers, of millions of Canadians without first seeking their consent. While the agency was within its legal rights and has legitimate information needs that are in the public interest, many viewed the actions of Statistics Canada as a breach of trust by a government agency because it was unexpected and initially unreported. The incident encouraged Canadians questioning whether the government respects their right to privacy. This case clearly highlighted a lack of understanding in the public domain about Statistics Canada’s mandate and approach. It also highlighted the differences between Canada’s public sector privacy regime and Canada’s private sector privacy regime which requires a more robust approach to transparency.

Accordingly, the Canadian government should:

**Amend the Privacy Act**

The government needs to lead by example in how it treats sensitive personal information. Transparency in the collection, use and disclosure of personal data, the scrubbing of sensitive personal information and ensuring informed consent are good principles that should apply to both public and private sectors. The federal government should consider the reform of the Privacy Act by applying the principles of PIPEDA to the public sector and it should include political parties as entities subject to privacy laws. It must end the double standard that undermines the rights of Canadians.
Opening the door to innovation

We need to address the obvious gaps and greatest negative impacts on society that data collection practices have imposed. The conversation must acknowledge that businesses need to continually update data sets to keep them relevant with evolving demographics and new market entrants. There is competition for the ownership of data sets and for the improvement of the quality of data sets and we must ensure an unobstructed path to data innovation. While Canada’s private sector privacy laws have been a model for the world for decades, owing to their principled approach, we must now consider a new paradigm in our approach to regulation:

Regulatory nimbleness

The digital economy evolves far too quickly for a conventional approach to regulatory intervention. The government should consider an adaptive approach to regulation and shift from “regulate and forget” to a more responsive, iterative approach that focuses on outcomes, avoids prescription and has a deliberate and ongoing feedback loop.3

Public and private sector cooperation

We need a more sophisticated conversation between public and private sectors, both in Canada and abroad. One approach would be to consider progressive alternative models for regulatory bodies, such as those of the Philippines4 and Singapore5, which legislate the appointment of senior officials in privacy regulatory bodies based on privacy and economic experience credentials. The creation of an industry ombudsman position within the OPC would help to ensure the practical impact of the office’s actions are fully considered. The government could also support regulatory testing grounds to prototype and test new approaches by creating sandboxes and accelerators.

Oversight without overreach

Government departments are most often mandated to regulate based on specific issues. They too frequently consider the economic impacts of regulatory intervention. There needs to be a shift in departmental mandates to acknowledge economic considerations and that those economic considerations should be evaluated outside the department crafting the regulation. There should also be a requirement that regulation should be risk-weighted, moving from one size-fits-all regulation to a data-driven, segmented approach.

5 https://sso.agc.gov.sg/Act/POPA2012?Provido=P1ll-#pp5-XX-pr5-
Regulate Smartly for the Fourth Industrial Revolution

To remain competitive in the global digital economy, we must not cloud opportunity with an overactive regulatory imagination. Canada already suffers from one of the more burdensome regulatory regimes in the G20, far behind its closest trading partner. According to the 2017-18 World Economic Forum Competitiveness Sub-index on Regulatory Burdens, Canada is number 38 globally and number eight within the G20. Data, as well as the techniques and technologies employed to collect and analyze it, will allow Canada and the world to solve pressing global economic, social and environmental problems. Data is now the engine of economic growth and prosperity.

Countries that promote data’s availability and use for societal good and economic development will lead the fourth industrial revolution and give their citizens a better quality of life. To seize this opportunity, people and businesses must be able to share their data with one another.

The right framework for Canada’s data economy is one that creates trust and enables innovation. In this new world, we cannot ignore the role companies that have not even yet been created will play as both innovators and wealth creators. Canada’s framework for the data economy must help SMEs start up, grow and become world leaders in the digital space for the long term.