DEBATING THE RIGHT BALANCE(S) FOR PRIVACY LAW IN CANADA

Summary and Discussion of Two Roundtables

January 2022

PUBLIC POLICY FORUM

PPFORUM.CA

The Public Policy Forum works with all levels of government and the public service, the private sector, labour, post-secondary institutions, NGOs and Indigenous groups to improve policy outcomes for Canadians. As a non-partisan, member-based organization, we work from "inclusion to conclusion," by convening discussions on fundamental policy issues and by identifying new options and paths forward. For more than 30 years, the PPF has broken down barriers among sectors, contributing to meaningful change that builds a better Canada.

Suite 1400, 130 Albert Street
Ottawa, ON, Canada, K1P 5G4
Tel: 613.238.7858
www.ppforum.ca

ISBN: 978-1-77452-102-1

WITH THANKS TO OUR PARTNERS

TELUS®/MD

Johnson & Johnson
FAMILY OF COMPANIES IN CANADA

APIC
Alliance for Privacy and Innovation in Canada
Alliance pour la protection de la vie privée et l'innovation au Canada

CONTENTS

AUTHOR

VASS BEDNAR

Vass Bednar is the Executive Director of the Master of Public Policy in Digital Society at McMaster University and an Adjunct Professor of Political Science. She is also a Public Policy Forum Fellow. As an enthusiastic and perpetual student of the policymaking process, she has held leadership roles at Delphia, Airbnb, Queen's Park, the City of Toronto, and University of Toronto. Vass is recognized as a creative, data-driven thinker and was the Chair of the federal government's Expert Panel on Youth Employment.

A graduate of McMaster University's Arts & Science Program, Vass holds her Master of Public Policy (MPP) from the University of Toronto and successfully completed Action Canada and Civic Action DiverseCity Fellowships. Passionate about public dialogue, she was also the co-host of "Detangled," a weekly pop-culture and public policy radio show and podcast that ran from 2016-2018. She currently writes a newsletter about Canadian startups and public policy called "regs to riches" and was recently recognized as an outstanding alum with a McMaster "Arch" award.

EXECUTIVE SUMMARY

In fall 2021, the Public Policy Forum convened a group of academics, lawyers, representatives from the private sector and members of civil society to revive discussions around modernizing privacy law in Canada under the Chatham House rule.

These conversations sought to explore five key questions of interest:

1. How is Canada situated compared to other jurisdictions and countries, and with respect to inter-provincial differences?
2. What are the priorities for changes to a modified *Bill C-11: An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts*?
3. Where are the widest gaps among experts and stakeholders on C-11, and are there different approaches, directions or principles that will help bridge them in effective legislation?
4. Are there steps outside of modernized legislation that the private sector should be taking?
5. Can a human rights approach co-exist with data-driven, private sector innovation?

On the question of how Canada is situated compared to other countries and jurisdictions, and with respect to inter-provincial differences, many participants expressed concern that a "patchwork" of frameworks is emerging as a few provinces (Alberta, British Columbia, Ontario and Quebec) have started to take the lead in modernizing Canada's private-sector privacy laws. This may be an expression of policy impatience, whereby provinces are unwilling to "wait" for Canada's federal government to modernize privacy law (through a revised Bill C-11) and instead seek to solve perceived gaps in private-sector privacy regulations.

So while this is a national conversation, it is increasingly a provincial one as well. Though the word "patchwork" came up with some frequency, it is possible to reframe this federated approach more positively as a productive opportunity for inter-provincial collaboration to develop a truly pan-Canadian, harmonized and interoperable private-sector privacy law that can both better protect Canadians' privacy rights and better support innovation and the growth of business.

Our roundtables reflected the challenge that highly knowledgeable participants came with particular perspectives, and the instrument for integrating them — a draft piece of legislation — is highly imperfect. Modern privacy and consumer protection legislation will need to operationalize the balance of these interests in a larger and broader debate regarding the "legitimate commercial use" of data inside legislation. Many discussants felt that further substantiation of this carve-out was required and observed that it lacked sustained championship. Policymakers need to build and protect both the trust of individuals and organizations so that Canadian innovation flourishes and thrives. It is difficult to have a comprehensive innovation conversation within a piece of privacy legislation. Further, the efforts to "protect" consumers may be read as charged or accusatory by private actors that are anticipating new restrictions on their potential ability to innovate through the collection of data, or are concerned about the costs imposed by potentially new requirements, such as through the strengthened right for consumers to request access to personal data held by an organization, and request that the organization delete it, or transfer it to another organization. Many discussants expressed that the broad business exemptions included in the proposed legislation are a source of potential weakness and concern. However, if this debate is framed as one between businesses and the state, we lose the centrality of the digital citizen. Ultimately, conversations about Bill C-11 are about power and revising the rights that people have regarding how their personal information is collected and used.

Due to some regulatory inertia — many discussants expressed agitation, disappointment and surprise that the proposed legislation was abandoned to "die on the vine" — the passing of time may act to normalize or pseudo-legitimize business practices that may otherwise not "fit" under the previously proposed legislation. It is easy to understand why that is likely to agitate business leaders that have been investing in talent and systems to maximize the value and derive insights from big data that can contribute to their economic growth to have those "innovative" norms called into question. At worst, it may seem disingenuous for the state to almost retroactively revise privacy norms in a pushback against surveillance capitalism.

The roundtables discussed priorities for changes to Bill C-11. Participants focused on the mechanisms for creating new accountabilities between businesses and individuals who have a data relationship with them. Another facet of the potential revised legislation that was of interest to discussants was related to resourcing and investments enforcement to avoid situations like the lack of capacity detailed in the 2020 report from Brave, a privacy-preserving browser that looked at "How Europe's Governments are Failing the GDPR," and detailed data protection authorities" (DPAs) capacity to enforce against tech infringements of the GDPR. There was alignment in the aspiration to both enhance individual's individual privacy rights while also supporting the needs of business and other organizations in the pursuit of responsible innovation.

In terms of some of the widest gaps among experts and stakeholders on C-11, there was skepticism regarding the utility of a new privacy Tribunal that could be separate from that of the privacy commissioner. Bill C-11 grants order-making enforcement power to the Privacy Commissioner (subject to approval by a Tribunal body) that could bring more teeth to legislation. Another profound gap was simply regarding what the "legitimate commercial use(s)" of data are — both currently, and what they could or should be in the future. Again, this interpretation is the crux of the privacy law conversation in Canada and must be discussed with greater clarity; perhaps in connection to the broader [political] narrative that many discussants felt was absent from the previous introduction of the Bill.

Regarding the approaches, directions or principles that could help to bridge these gaps: a more frank and direct conversation that engages everyday people regarding how their data may be used, how it is protected and how this may contribute to innovation is warranted. Other policy interventions may better empower consumers to make decisions about how they want to engage online. These interventions would be adjacent and complementary to privacy legislation reform.

The two roundtable conversations did not directly address non-legislative interventions. That being said, the private sector could be leading on supplementary work to protect consumer privacy and empower their customers with new abilities to tailor their online experiences. For instance, to what extent could a **commitment to data minimization** act as a competitive advantage for a firm? Often businesses argue that consumers benefit from the data that businesses collect about their habits and purchase history, so that they receive more appropriate or efficient ads. This may be true in many cases, but customers deserve **the ability to turn "off" these targeting practices**. We saw the remarkable response to this when Apple gave iPhone users the ability to turn off the "Personalized Ads" toggle and directly asked iOS users to opt-in to track their activity within each individual app.

New policy interventions for algorithmic transparency, accountability and auditability are privacy-adjacent and worthy of exploration in a Canadian context. For instance, Canadian policymakers are only beginning to engage in conversations about competition and the role of consumer data in creating or maintaining barriers to market entry, or new ways to potentially abuse dominance.

Many aspects of the previously proposed Bill C-11 were promising, such as the right to an explanation of why an artificial intelligence (AI) system made a decision about a person, or the right to opt out of having data collected in the first place — simply having better explanations available will be useful. But it still places a high burden on the individual to seek understanding on a case-by-case basis, which is time-intensive and may be irrational to expect. However, should individuals have a desire to more proactively manage their online engagements, perhaps they should have the power to reject recommendation systems. This could come in the form of a stand-alone piece of legislation, such as the recently proposed legislation Filter Bubble Transparency Act ("A bill to require that internet platforms give users the option to engage with a platform without being manipulated by algorithms driven by user-specific data") that would enable end users on social media to reject a recommender system.

Another area worthy of further discussion is related to collective data rights and intermediaries. California's consumer privacy law includes a mechanism for this kind of collective representation. And, in a recent proposal by the EU Commission, Europe is considering something similar. Perhaps Canada should do more to put people directly in charge of their data as individuals seek to demystify the bargain between themselves and digitally driven firms. The new legislation will help people both understand what may be done with their data, and why, and give them the ability to opt-out.

With regards to whether a human-rights approach — whereby the privacy of individuals is treated as a fundamental right — can co-exist with data-driven, private sector innovation, some participants expressed optimism that this was possible, and generally held the view that a human-rights approach was not incompatible with innovation. Canadians crave better custodianship of their information, more transparency over how it is used and more rights to manage their information online.

Another area of misalignment that should be corrected going forward is related to the legislation potentially exempting political parties from new requirements placed on the private sector. Non-profit and charitable organizations similarly manage and mine large volumes of information. Given that Ontario's Information and Privacy Commissioner has recommended that Ontario's privacy law apply to provincial political parties and federal riding associations, consistency would be valuable. More discussion of data management in automated decision systems (ADS) would also be welcome. Canadians should understand fairness, transparency, security and accountability rules for the responsible use of their personal information in these systems.

Finally, the enthusiasm and good will toward continued efforts at modernizing privacy law should be noted. Not only can we continue to learn from international peers, but we have the benefit of being informed by more recent approaches put forward by some of the provinces. Achieving harmonization through interoperability and re-introducing a coherent privacy framework that better protects consumers and empowers responsible innovation is achievable with sustained political championship.

BACKGROUND

This paper summarizes two virtual roundtable discussions convened by the Public Policy Forum in the fall of 2021.

The first roundtable took place on September 29th, following the federal election, and focused on generally setting the stage in terms of where the government, businesses and the public are regarding contemporary privacy issues in Canada.

The second roundtable took place on October 13th, and focused on navigating the relationship between privacy and economic growth with learnings from international perspectives.

Canadian policymakers are working to modernize privacy laws in order to respond to the shift to a more digital economy, and to meet the challenges posed by new technologies that are built from people's data, such as automated decision systems, data analytics, facial regulation, social media and more.

Part of the motivation for the roundtables was the anticipation that the Government of Canada will continue to advance some version of the previously-introduced Bill C-11 — An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts (2020). The below is an excerpt from the Liberal platform:

We will move forward on legislation that will implement the Digital Charter, ***strengthen privacy protections for consumers*** *and provide a clear set of rules that ensure fair competition in the online Marketplace.*

There is a second reference of "privacy" in the Liberal platform, when the prospect of a "Digital Policy Task Force" is mentioned.[1] Perhaps this document can be a productive artefact for the Task Force as it seeks to stimulate continued policy progress on this important file.

INTRODUCTORY NOTES

It is clear that the new economy is putting stress on existing privacy frameworks in Canada. There are a number of presumed or cautioned trade-offs associated with modernizing our privacy regulations. One of these is convenience for consumers, who have been alleged to be potential victims of a stronger privacy regime. The other is innovation as an economic engine. Some stakeholders contend that strengthened privacy rights could impede wealth creation in Canada. This claim is cause for pause, and perfectly captures the new tension as the government seeks to find balance between legitimate consumer interest(s) and the public interest.

Privacy creates a critical set of challenges because it is fundamentally about power and protection, and we need clear, enforceable guardrails to improve transparency and accountability between consumers and companies. Activity facilitated by the internet is primarily funded by the collection, analysis and trade of data — the "data" economy or the "digital" economy. Harnessing data means firms can achieve the power to influence consumers in the decisions they make when shopping or the information they consume online.

Discussion of and concerns related to privacy have only heightened in the pandemic. Recently, Shosana Zuboff — the renowned academic who helped to establish the parameters of "surveillance capitalism," of which Big Tech is a significant part — wrote in the New York Times that we are the "Object(s) of a Secret Extraction Operation." In this opinion editorial, she notes that, "our democracies have allowed these companies to own, operate, and mediate our

information spaces unconstrained by public law. The result has been a hidden revolution in how information is produced, circulated, and acted upon."

New and novel data monetization models are not well-addressed in Canada's current privacy regime.

The policy progress on privacy in Canada has been decidedly incremental. The Digital Charter launched in 2019 as a precursor to later legislative proposals. Bill C-11 was introduced in November 2020, but did not advance in the legislature ahead of the election call nine months later. A series of privacy-related policy proposals from various provinces (Ontario, Quebec, British Columbia and Alberta) have continued the conversation in Canada during a moment of federal inertia.

While these developments have generally been productive in stimulating debate of optimal design and new accountabilities, they have also created concern that Canada is inadvertently creating an inconsistent "patchwork" regime. This potential for a convoluted approach further intensifies the need for federal action.

At the same time, there may also be a feeling that one piece of legislation alone will be insufficient to address the implications of the business models of social media platforms. Since the roundtables were held, Facebook rebranded as "Meta," and shared its vision for a future with a "metaverse" (a hypothesized iteration of the internet that is experienced through virtual and augmented reality). Facebook's patent filing reveals an economy where there is a real-time online ad-auction system that turns "organic options" that resemble objects in the world within a virtual world into "sponsored objects," whereby an advertiser has invested in the object in anticipation of interaction. Similar processes for advertisers to bid on "sponsored locations" within the metaverse are described. Innovation such as this creates more urgency and interest in the privacy file when considering current and future uses of data.

PRIMER: HOW PRIVACY IS REGULATED IN CANADA

- **PIPEDA**
  - Governs the topic of data privacy, and how private sector companies can collect, use and disclose personal information.
- **The Privacy Act (1983)**
  - Regulates how federal government institutions collect, use and disclose personal information. It also provides individuals with a right of access to information held about them by the federal government, and a right to request correction of any erroneous information.
- **Access to Information Act**
  - Gives citizens the right of access to information under the control of government institutions. The Act limits access to personal information under specific circumstances.
- **Freedom of Information Act**
  - Designed to make governmental institutions more accountable to the public, and to protect individual privacy by giving the public the right of access to records.
- **Provinces with recently introduced privacy regimes and frameworks**

BRITISH COLUMBIA:
Bill 22, which amends the Freedom of Information and Protection of Privacy Act

ALBERTA:
Public consultations on the province's statutory privacy protections, which include Alberta's Personal Information and Protection of Privacy Act (AB PIPA)

ONTARIO:
Whitepaper on Modernizing Privacy in Ontario

QUEBEC:
Bill 64, an Act to modernize legislative provisions as regards the protection of personal information

- **Personal health *only***
  - Ontario: The Personal Health Information Protection Act (PHIPA)

As it stands, the burden on the individual to navigate privacy legislation is fairly high. One benefit of updating privacy legislation could be citizens having a stronger sense of their data rights and more ownership rights that they can effectively exert, if they choose.

> **"This year, we have also seen "app stores" function as a regulator of sorts. This past spring, Apple required that apps like Facebook obtain permission from customers to allow them to track individuals across other applications."**

While this is generally a positive intervention from a privacy perspective, it can be argued that it is bad for private businesses, which may lose the ability to capitalize on the data that they have been collecting. The true cost and implication(s) of a new privacy regime for the ability of firms to innovate with data is unknown and yet often cited anecdotally.

THE PPF PROCESS

The Public Policy Forum gathered experts and practitioners across academic, legal, private and civil society stakeholders for a Chatham House discussion.

Roundtable 1: Setting the Stage

One of the speakers offered an overview of common categories for businesses' use of personal information in a context of big data and increased personalization. They asked whether the notice and consent model is sustainable. While this question lingered, the conversation did not directly return to it. Perhaps this is another facet of the ongoing privacy conversation that could be revisited.

A case study on a retail loyalty program was considered as a vehicle to discuss Personally Identifiable Information (PII)[2] and purchase history, as well as how information is obtained, stored and shared with third parties. The case study reminded participants that while volunteered information may be used to provide discounts and target marketing, it may also be combined with aggregate demographic information based on neighbourhood to improve marketing effectiveness, to plan new store locations in order to be closer to existing and potential new customers or to assist in detecting possible fraudulent purchases based on what is being purchased by location. Having so many concurrent applications of consumer information is another pressure on privacy legislation modernization. Further dialogue around a firm's potential inability to clearly articulate all future uses and how to update consumers is warranted. However, as scholars Daniel

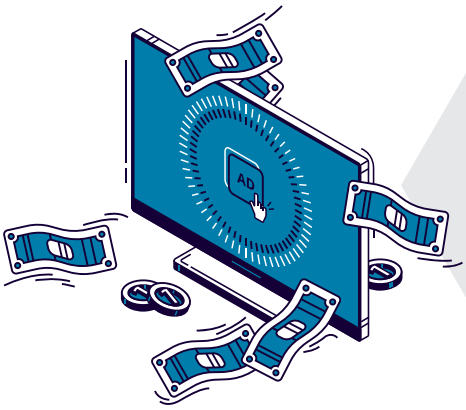
Solove and Danielle Citron note in a recent publication on privacy harms, "When individuals are not given important information, they are harmed because they lose their ability to assert their rights, to respond to issues involving their data, or to make meaningful decisions regarding the use of their data."

A notable comment during the case study discussion acknowledged that an organization may not be able to foresee, in detail, all the future uses of a personal information element. It was further suggested that the complexity of business processes and uses makes effective disclosure on behalf of private firms to individuals and meaningful consent challenging. This is a significant insight, and illuminates the need for businesses to update their stakeholders about how they may wish to leverage information held by the company for new uses.

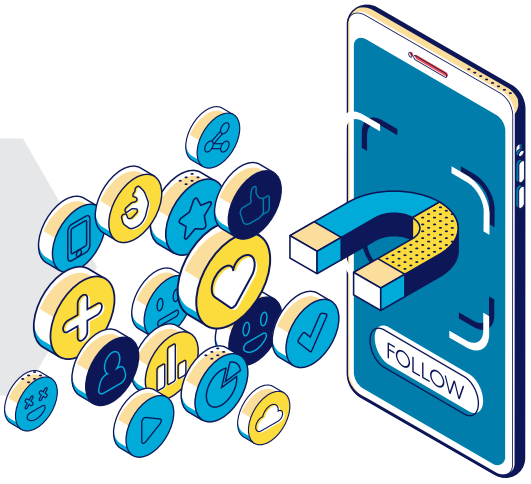
This case study led to a brief discussion on whether targeted advertising is even effective. In an online article, "Ad Tech Could Be the Next Internet Bubble," Gilad Edelman noted that:

There are piles of research papers in support of this idea, showing that companies' returns on investment in digital marketing are generally anemic and often negative.

> **One recent study found that ad tech middlemen take as much as a 50 percent cut of all online ad spending.**



Brands pay that premium for the promise of automated microtargeting, but a study by Nico Neumann, Catherine E. Tucker, and Timothy Whitfield found that the accuracy of that targeting is often extremely poor.



In one experiment, they used six different advertising platforms in an effort to reach Australian men between the ages of 25 and 44.

Their targeting performed slightly worse than random guessing. Such research indicates that, despite the extent of surveillance tech, a lot of the data that fuels ad targeting is garbage."

Another presentation focused on how policymakers can foster trust and accountability in privacy reform. The key theme from these remarks was that we need to ensure that we have **effective enforcement** of the law and appropriate penalties that can be imposed if a firm fails to comply, and that a better law would also do a better job of ensuring compliance through incentives. The lack of order-making power for the federal Privacy Commissioners has long been cited as an outlier when compared to provincial commissioners or privacy and data protection commissioners around the world, and support was expressed for the proposed Bill's "opening of the door" to order-making powers for the commissioner. Another comment about enforcement was that the long timelines associated with complaints diminish the regime's effectiveness.

There is consensus that the current privacy law is dated, but many unanswered questions persist regarding the mechanics of the potential Personal Information and Data Protection Tribunal, such as how hearings will be conducted, who would be on the Tribunal and how long the Tribunal process will take (including the fact that Tribunal discussions would still be subject to judicial review). Many questions were raised regarding whether the new Tribunal would be useful or valuable in terms of achieving greater accountability.

There were also questions raised regarding administrative purpose.[3] The discussants further considered the future context of a Digital Safety Commissioner and a Data Commissioner. A participant commented that it seemed as if the government had "cherry-picked" from the Digital Charter. Finally, there was disappointment and surprise that the Digital Charter currently lacks a strong political advocate.

Participants reflected that privacy reform in Canada seemed to lack a clear strategy and that politicians were not sharing a clear vision for how information should play a role in our economy. This lack of vision could create mistrust.

Some wondered about the practicality of a separate Data Commissioner, and questioned the ability of this new function to "inform government and business approaches to data-driven issues to help protect people's personal data and to encourage innovation in the digital marketplace." Others defended it, arguing that such a role better aligns the government with businesses that integrate a "Chief Data Officer" into their firm, and pointing out that the concept was based on one piloted in Australia. A desire for a common framework for public and private regulation was expressed, and many participants were optimistic that the federal government would directly address and respond to provincial movement(s) on privacy that have occurred since the introduction of Bill C-11.

Discussants also pushed on why we maintain distinction(s) between public and private sector privacy law. Participants cautioned that "data protection" and "privacy reform" are too often conflated. Another distinction made was between privacy rights in the context of state surveillance and intrusion and political manipulation of thought. The realities of power asymmetries between consumers and large technology firms was acknowledged, as was the ongoing context of the pandemic for spotlighting privacy issues. The more distributed governance model in the U.S. was brought up as a comparison to Canada. Again, the need for federal leadership was consistently emphasized, as was the desire for more of an "ombuds" model that could ensure stronger safeguards for citizens.

The session concluded by asking whether there can really be a "vision" when we have competing interests in Canada. One under-explored aspect of the reform conversation is the pressure to maintain adequacy status,[4] while the desire for consumers to have data mobility rights and achieve the right to be forgotten seemed to be satisfied. Another area of opportunity for continued conversation in the privacy space is the role of privacy impact assessments as a privacy instrument.

The point was made that many firms do not currently comply with existing legislation — many do not explain to individuals how data is collected, what will be done with it, who has access to it, how it's going to flow, etc. — and an attendee cautioned that participants should beware the presumption that firms are acting in the public interest. It was further asserted that these basic elements (such as what data is collected and why) were not substantively reinforced in Bill C-11.

Another participant advocated for a private right of action under future privacy law. It was suggested that privacy laws should protect the strongest possible autonomy and control over how people's information is collected and how it is used. The concept of "informational self-determination," established through the German constitutional court was also referenced.

Roundtable 2: Navigating Privacy and Economic Growth

The second roundtable took an international perspective and was more forward-looking and less rooted in Bill C-11. The conversation was rooted in securing privacy in the digital economy while facilitating innovation.

To anchor the discussion, a 2011 Economist article, "The clash of data civilisations," was referenced.

> **A discussant reviewed the evolution of Canadian versus foreign privacy law. It was noted that Canada takes a principles-based (rather than rules-based) approach to privacy governance.[5] This means that our regulator is more like a mediator. Our approach is grounded in accountability in Canada, and in contrast, is grounded in regulatory frameworks in other countries.**

Another distinction is that we take an "ombuds" model in Canada, whereas other nations take an enforcement model. Lastly, there are separate public/private sector privacy laws in Canada, whereas other countries tend to have one privacy law.

These distinctions in a global context create pressure for Canadian privacy law reform. It was noted that globally the unprecedented power imbalance between individuals and the organizations that hold their data spurs strengthening of both privacy rights and the powers to enforce them.

While the General Data Protection Regulation, 2016 (GDPR) and the California Consumer Privacy Act, 2018 (CCPA) are often cited as the policy inspiration in Canada, the GDPR is firmly grounded in human rights law while the CCPA is rooted in consumer protection law. It was noted that the federal government was deliberate in naming the federal privacy law proposed in C-11 the "Consumer Privacy Protection Act."

It was observed that the GDPR has a "magnetic pull" on Canada, which has led to calls to maintain the adequacy and achieve the ability to receive personal data that a firm may hold on you based on this new precedent from the E.U. It was also noted that the U.K. is adopting the approach of the GDPR in its Data Protection Act. The other major legislative precedent is the CCPA. It was emphasized that as Canada prepares to continue work on privacy legislation, we are in a "moment of divergence," and we need to think carefully about where we may differ from international peers. Another observation was that Canada seems to be moving *towards* an enforcement model and away from the "ombuds" approach.

The presentation continued to survey areas of convergence and divergence between Canadian and foreign privacy law. In terms of convergence, there is merging alignment around strengthening consent mechanisms, increasing transparency obligations, creating new privacy rights, moving to an enforcement model, providing for certification measures and codes of practice to demonstrate compliance, regulating automation decision making, and — as exemplified in Bill 64 — the maintenance of "adequacy."[6]

The divergences over time and relative to other jurisdictions reviewed were balancing individual rights and organizations' interests, being principles-based and technologically neutral, and free cross-border data flows.

Finally, new divergences are creating new opportunities for policy consideration, such as data trusts (Ontario), sandboxes (CPPA), allowing cooperation between different regulators in privacy issues and regulation information that no longer relates to an individual.

A range of reflections was shared based on helping countries scope their data laws. Some discussion focused on how to best centre the citizen in the design of the privacy regime. For instance, it was observed that the "consumer lens" can be a bit limiting, and that the activity of purchasing an item should not be required in order to hold certain privacy rights. The benefits of a human rights approach were also espoused, and the point was made that governments should view data as an extension of the person. Privacy rights were also connected to other rights, such as the right to dignity and the right to free expression.

Discussion also delved into the details, specifically considering implementation. It was observed that you can have the "best" law, but it will not matter if it is not properly enforced. Lawmakers seem to be learning this from the GDPR, which has been lauded for including privacy by design and explicit consent, but is being under-enforced. Discussants felt that the government truly has to be "all in" in order to follow through on the ambition of new privacy laws.

In this discussion of implementation and enforcement, the topic of corporate capture was raised. Participants felt that corporate capture extends beyond private actors lobbying against privacy reform, such as the "secret war" that Amazon has waged on privacy reform in the U.S. recently detailed in a Reuters investigation. The point was that it goes all the way to compliance. A presenter cautioned Canadians regarding the investment of private firms to potentially skew the design and implementation of new privacy or data protection rules.

One discussant shared reflections from working with companies on compliance regimes. The global privacy policy patchwork was cited as a challenge for companies that want to build to a standard that will allow them to comply in markets outside of Europe (for example). The state-based approach in the U.S. was also reviewed, with one participant observing that it could be preferable for the U.S. to take a national approach to privacy law.

The question of *global* "patchwork" was raised in the context of interoperability and harmonization. It was felt that true harmonization would not occur but that privacy regimes will have to be interoperable.

Some participants felt optimistic that a human rights approach could *enhance* economic growth. They were also cautious about identity anonymization, noting that it is "messy" and may be something that brings us "back to the drawing board" in Canada.

Discussants also considered how small and medium-sized enterprises could be better supported in achieving compliance with new privacy regimes, such as through learning resources. Exceptions for small companies were cautioned against, with the reflection that they are confusing. The importance of supporting firms with compliance was emphasized, for example having sufficient implementation timelines and guidelines that could support smaller firms in building compliance into their products to benefit from the advantages of building in data management early on.

Discussants anticipated that Canada would diverge from the GDPR so that we could achieve better privacy protection, and better individual control over data.

Presenters reminded the audience that no nation on earth has the "ideal" privacy law.

It was conveyed that the ideal law must be principles-based, technology neutral and be absolutely clear on the rights of the individual to evolve with the law. A modernized privacy framework will still demand an ongoing dialogue that ensures it is responsive to the changing needs of the individuals. Perhaps we should anticipate that regulators will need to be more responsive on the privacy file, and could consider scheduling a pre-determined review of the new legislation in order to evaluate its implementation and effectiveness.

Privacy reform was also compared to regulating the use of algorithms in the public and private sector, an adjacent and necessary policy issue that would be complementary to much of the privacy discussion. It was acknowledged that regulators need to do many things in parallel in order to properly align accountability models with the digital economy with an "abundance mindset." Another massive gap related to privacy that was raised was transparency in systems. Discussants felt that we need systemic transparency around the public sector's use of algorithms. It was also emphasized that privacy *can* be a gateway to greater transparency via algorithms (and Quebec's Bill 64 was referenced in this regard, as it grants individuals the right to have access to the information that was used to make an automatic decision about them, the parameters of that decision, and the right to present observations).

Other areas of discussion included:

- Whether Canada's Privacy Commissioner receives enough funding;
- Whether the Privacy Commissioner's mandate is broad enough;
- Whether the Privacy Commissioner's funding is commensurate with the current mandate;
- Whether we have the appropriate digital taxation models in place;
- Whether we have explored and learned from the potential of more collective approaches to data governance;
- Whether a human rights approach is inherently at odds with corporate interests;
- Whether the policy process with regards to privacy will be a constant iterative process in order to identify gaps and fill them;
- Whether we have considered the opportunity to learn from Indigenous approaches to data rights, such as the right to self-determination; and
- Whether we can be incremental with privacy reform and pilot interventions, or is it an "all or nothing" approach?

ADJACENT POLICY OPPORTUNITIES

The ongoing discussions related to **open banking** in Canada, insofar as they reference data portability, remain relevant to the opportunity for privacy reform.

Consumer protection may be another vehicle for greater transparency. For instance, Canadian policymakers may want to explore "dark patterns," a term examined in a workshop recently held by the FTC that describes a range of potentially manipulative user interface designs used on websites and mobile apps.

Competition policy also has intersections with privacy considerations that could be further explored.

The new **Data Commissioner** will add another dimension to these data and privacy conversations and can be a champion for responsible innovation and potentially a champion for re-introduced legislation.

Other, related topics that have been under-explored in Canada include **fiduciary duties for data holders**, **data trusts**, and the potential to create **a registry of data brokers** as other jurisdictions have explored.

Another discussion point that we were not able to examine further in plenary was whether the notice and consent model is sustainable for complex businesses, and whether there are effective alternatives to this model.

Challenging or Redefining "Legitimate Business Needs"

The data-driven, intangibles economy is here, and consumers may at times make a false trade-off between their privacy and convenience. Though these issues were not explicitly discussed during the roundtables, there are countless examples of emerging data-monetization models that will further challenge Canada's existing privacy regime. While the ethics of facial recognition technology are being vigorously debated, the biometric of voice data and the upcoming "voice marketing revolution" has been under-considered in the Canadian context. Unlike some U.S. states, Canada does not regulate data brokers. And "wearables" fall outside of Health Canada's "medical device" framework, exempting technology firms from more robust privacy protections under HIPPA.

CONCLUDING NOTES

We should recognize that we may need to continuously update and review our privacy regimes, rather than endeavoring to achieve the "perfect" piece of legislation. Technology continues to advance rapidly and people's attitudes towards their own information are changing. The law needs to reflect that fluidity.

The regulatory lag and associated uncertainty that has come to characterize the relationship between innovators and the state are failing citizens and creating discomfort. Legislative ambiguity risks inadvertently legitimizing business behaviours that have become normalized but may not be desirable. At the very basic level, firms need to continue to dialogue not just with policymakers regarding their perspectives related to the presumed trade-off between innovation and privacy, but also directly with the citizens and consumers that they leverage data from. The prospect of privacy policy modernization is a somewhat tense policy space where continued commercial interests may fundamentally be at odds with the goals and expectations of the public.

At the time of the drafting of this report — prior to federal cabinet ministers' mandate letters being released, but upon Minister of Innovation, Science and Industry François-Philippe Champagne sharing that updated privacy rules are a priority — there is a general sense of impatience with the lack of progress on this urgent policy file. It seems disingenuous for politicians to simultaneously move forward on this file while exempting themselves from the clarity and consumer empowerment that it promises. It is no secret that political parties use rich data sets to micro-target voters. True political leadership and courage would see a new privacy regime apply to all political parties in order to create alignment with new expectations that may be placed on private actors.

Canadian decision-makers can benefit from being a "secondary" mover on this file, extracting insights from the early experiences of international peers that have enacted new privacy frameworks, such as Europe's GDPR and California's CCPA — arguably the most visible new regimes. We can also learn from within, building from the privacy-relevant policy progress from some of the provinces.

ENDNOTES

1 "Establish a digital policy task force, comprised of industry experts, academia, and government, to integrate efforts across government and provide additional resources in order to position Canada as a leader in the digital economy and shape global governance of emerging technologies, including with respect to data and privacy rights, taxation, online violent extremism, the ethical use of new technologies, and the future of work."

2 Under PIPEDA, the following is considered sensitive or Personally Identifiable Information (PII) and is explicitly protected under the law: Age, name, ID numbers, income, ethnic origin, blood type, opinions, evaluations, comments, social status, or disciplinary actions.

3 Is the use of personal information about an individual "in a decision making process that directly affects that individual" (section 3). This includes all uses of personal information for confirming identity (i.e. authentication and verification purposes) and for determining eligibility of individuals for government programs. Source: Directive on Privacy Practices.

4 In 2001, the E.U. recognized Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) as providing adequate protection. Canada's adequacy status ensures that data processed in accordance with the GDPR can be subsequently transferred from the E.U. to Canada without requiring additional data protection safeguards (for example, standard contractual rules) or authorization to transfer the data. Source: The European Union's General Data Protection Regulation.

5 In the Canadian context, the way that a firm achieves that valid consent is up to them.

6 This refers to the right to receive personal data from the E.U.


PUBLIC
POLICY
FORUM