INSTITUT C.D. HOWE INSTITUTE
Trusted Policy Intelligence | Conseils de politiques dignes de confiance

E-BRIEF

November 20, 2023

INDUSTRY REGULATION AND COMPETITION POLICY

Getting Personal: The Promise and Potential Missteps of Canada's New Privacy Legislation

by Daniel Schwanen

- Canada's governments have been grappling with threats to Canadians' privacy posed by the fast-expanding collection and use of their personal data, enabled in turn by increasingly powerful digital technologies. In this context, Canada's federal Parliament is examining Bill C-27, the *Digital Charter Implementation Act*, which encompasses three new acts plus related amendments to existing acts (Canada 2022). In this paper, I focus on parts 1 and 2 of Bill C-27, respectively called the *Consumer Privacy Protection Act* (CPPA) and the *Data Protection Tribunal Act*, which together update federal privacy rules applying in commercial settings.[1]
- An update to Canada's federal privacy legislation is much needed. But legislators should be wary of proposed amendments that could increase the inevitable costs and uncertainty around the implementation of the new law. They would potentially reduce growth opportunities for Canadians in the data-based economy – at no discernible improvement in the protection of their privacy. Provisions in the legislation for a five-year review can address any actual weakness that might come to light.
- With the bill now making its way through a Parliamentary committee, I review the purpose and contents of the legislation, assess critics' arguments that it should be more restrictive, and suggest four ways in which legislators and regulators can help streamline implementation of CPPA. They are aimed at keeping costs and uncertainty at a minimum while simultaneously helping Canadians to better understand and claim their privacy rights.

The author thanks Benjamin Dachis, Rosalie Wyonch, William B.P. Robson, Tim Brennan, Paul Johnson and anonymous reviewers for helpful comments on an earlier draft. He retains responsibility for any errors and the views expressed.

1 Part 3 of the legislation, the *Artificial Intelligence and Data Act* (or AIDA), puts for the first time a framework around the use of artificial intelligence (AI) in Canada. It complements privacy legislation by aiming (among other goals) to limit the potential for AI systems to use Canadians' personal data in harmful ways. The text of bill C-27 can be found at https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading

The Need to Upgrade Privacy Protections

Privacy protections have been strengthened in recent decades in many countries, including Canada.[2] But the enormous expansion in the ability to collect, store, analyze, use and share personal data,[3] and the lower cost of doing so thanks to the evolution of digital technologies, have made it both easier and more rewarding to exploit such data (Varian 1997). This in turn increases the risk that personal data will be accessed and collected by third parties that use it without sufficient regard for the privacy of persons who shared their information, and without sufficient safeguards in place to prevent its harmful use.

Effective rules regarding how personal data are handled are foundational not just to the ability of individuals to maintain their privacy, but also to the ability of Canadians to benefit from the continuing digital transformation of our economy, which requires trust in how information is collected, used, or shared. However, in pursuing these goals, governments should seek to preserve and even enhance the substantial benefits that Canadians can expect from the digitalization of the economy. These benefits rest not only on the development and application of digital technologies, but also on the data Canadians collectively share with private or public organizations to the extent it can be accessed, combined and analyzed to support useful innovation in the public or private sectors.

Key common elements of privacy laws found in Western jurisdictions include a requirement for organizations to obtain consent from those who share their personal information. This consent must be obtained both for the collection of the information and for its use and further sharing.[4] Rules include requiring organizations to establish sufficient security safeguards[5] around these personal data against leaks and other breaches such as those resulting from cyberattacks. Those safeguards are required to be commensurate with the sensitivity of the information. As well, organizations must identify the purposes for which the personal information is collected, and limit its collection to what is necessary for those purposes. Individuals have the right to know what information is held about them, to have that information corrected if inaccurate, and to have organizations eventually dispose of it. Organizations are responsible for the personal information under their control, and must designate who is accountable for their compliance with privacy rules.[6] Privacy laws typically also include special rules (such as

2 While the right to privacy is often referred to as a "fundamental right," and is recognized as a quasi-constitutional right in Canada, it is not positively defined in legislation and official documents, here or elsewhere. Rather, it is typically described by what its *absence* consists of (invasion of privacy) and by what organizations must do to uphold it. Such descriptions have evolved by leaps and bounds historically, notably following advances in technology (e.g., recording devices).

3 Defined in the proposed CPPA as "Information about an identifiable individual."

4 That said, there are often important exceptions, such as those where consent can reasonably be inferred, for information collected in the context of employment relationships, or for journalistic or other purposes designated as publicly beneficial. In the CPPA, the collection of personal information without an individual's knowledge and consent is allowed for "journalistic, literary or artistic purposes." Also of note, the *Budget Implementation Act* of 2023 also expressly exempts Canadian political parties from the ambit of Canada's privacy laws.

5 Ranging from internal processes to technological firewalls, and rules to ensure continued data protection in the event data are shared with third parties, e.g., in the event of mergers.

6 These common elements are reflected in the Canadian Standards Association Model Code for the Protection of Personal Information (see https://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-7.html#h-417659), which is included in Canada's current privacy legislation, and in turn was informed by 1980 OECD guidelines.

stricter rules for obtaining consent) around the collection and sharing of particularly sensitive personal data – such as financial or health data – and are also especially protective of minors' personal data.

Typically, privacy laws stipulate that an organization that becomes aware of a security breach must report it to privacy authorities if it is reasonable to think that the breach will cause significant harm to the individual or individuals whose data are involved. In turn, the ability of individuals to obtain redress for being harmed by a privacy breach depends on what is meant by "privacy harms," or whether it is possible to show that they have occurred (Citron and Solove 2022).

Canada's current federal legislation, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), features all of these standard protections. But it is widely seen as out of date in light of evolving technology and business practices that might threaten privacy. Numerous privacy breaches have brought to light the insufficient incentives to comply with the law and businesses have complained about the lack of procedural fairness in its application. PIPEDA's consent requirements were seen as simultaneously putting too much of a burden on individuals and overly constraining the uses businesses could make of personal data (Scassa 2020). Additionally, this federal legislation has been falling far out of step with other international and even domestic jurisdictions.[7]

It should be noted here that both PIPEDA and the CPPA allow for the federal legislation to yield to a provincial law that is substantially similar to (or stronger than) the federal one, including sector-specific privacy legislation (typically covering the healthcare sector), which is in place in many provinces. At the same time, the federal privacy legislation applies to all data collected, used or shared inter-provincially or internationally, as well as to "works, undertakings, or businesses" held by the federal government across the country. This potentially confusing jurisdictional mix is a product of Canada's constitution, which assigns property and civil rights to the provinces, but international and interprovincial trade matters to the federal government. One result is that businesses will often have to conform to two sets of privacy laws (Wagner 2023).

What's New on Privacy in Bill C-27

The CPPA will essentially supersede PIPEDA as it applies to the collection, use, and disclosure of personal information in the course of commercial activities.[8] For its part, the *Data Protection Tribunal Act* institutes a tribunal that counter-balances the new powers given Canada's federal Privacy Commissioner under CPPA, allowing organizations to appeal the Commissioner's findings and orders under the CPPA. However, the Tribunal, of which at least half the members must have experience in the field of information and privacy law, will apply a narrow standard of "correctness" for questions of law, and of "palpable and overriding error" for questions of fact. This is unlike the current situation under PIPEDA, where complainants can appeal the Commissioner's findings in federal court, which applies a wider standard of review.[9]

7 For example, the European Union's General Data Protection Regulation (GDPR) and the equivalent United Kingdom's *Data Protection Act*, which both came into effect in 2018, California's *Consumer Privacy Act,* which came into effect in 2020, and Quebec's *Act Respecting the Protection of Information in the Private Sector,* which has come fully into effect in 2023.

8 Leaving the part of PIPEDA that governs the use of electronic governments by the federal public sector in place as a new *Electronic Documents Act* (Canada 2022).

9 A number of law firms analyze key changes brought about by Bill C-27 in publications available on their web sites. The summary in this section draws heavily on Fraser (2022), Thompson (2022) and Gittens, Burns and Promislow (2022).

Key changes in the CPPA compared to PIPEDA include more specific requirements for determining what constitutes valid consent, including: "the need to communicate in plain language; how the information will be collected; the reasonably foreseeable consequences of the proposed collection, use and disclosure; and what types of information will be disclosed and to whom" (Fraser 2022). Organizations will be required to put in place privacy-management programs along lines specified by the legislation, and which should be made available on request to the Privacy Commissioner.[10] Individuals will have the right to explanations of how algorithms treat their data to make predictions, recommendations or decisions about them, and to know organizations will eventually delete their personal data.

The CPPA introduces definitions and requirements for anonymization and de-identification of data that did not exist in PIPEDA (Jares 2023). The distinction between de-identified and anonymized data is an important one. Anonymization ensures that no individual can be identified from the information, whether directly or indirectly, by any means. As is typically the case in comparable jurisdictions, anonymized data will not be regulated under the CPPA. De-identified data means personal information that does not directly identify the individual to which it attaches, but the identity of the individual could still potentially be cobbled back together, for example by cross-referencing various databases. Under the CPPA, companies can use de-identified personal information without the knowledge and consent of individuals when it is used for internal research, analysis and development purposes.

The new law imparts significantly greater enforcement powers to Canada's Privacy Commissioner than does PIPEDA. Once a complaint (brought either by an individual or initiated by the Commissioner) has been investigated by the Commissioner, and it is not resolved or discontinued, or subject to mediation or other dispute resolution mechanism, the Commissioner can refer it to an inquiry. The inquiry must follow rules of fairness and due process. At the end of such an inquiry, the Commissioner can issue compulsory orders to an organization that would bring it into compliance with the CPPA. The Commissioner can also recommend to the new Tribunal that it impose administrative monetary penalties. Under the current legislation, such penalties existed only for cases of breaches of mandated data security safeguards, but under the CPPA, the grounds for imposing penalties are wider and the potential penalties much more severe (the higher of $10 million and 3 percent of the organization's gross global revenue). As well, individuals that have been affected by an organization that was found by an inquiry to have contravened the CPPA will now be able to bring a civil claim in court against that organization, provided those findings were not appealed or were upheld by the Tribunal.

The CPPA will certainly modernize Canada's privacy regime and bring it more in line with that of comparable jurisdictions. Does it strike the right balance for Canadians? Many would like to see its privacy protections strengthened further, and I will explore some of these positions below, before offering some suggestions of my own. But first, it is useful to step back and review some key elements of the interaction between privacy and economic well-being.

10 Organizations can proactively establish an internal code detailing how they will comply with the CPPA, including their privacy management program, which if approved by the Commissioner will constitute the organization's legal compliance obligations.

Privacy and Economic Well-Being

While some economists once saw privacy rules as allowing the "concealment of information," which impeded the well-functioning of certain markets such as insurance (see, e.g., Posner 1981, cited in Acquisti 2023), the channels through which privacy can increase economic welfare are now better understood. Privacy can protect individuals from negative outcomes such as those stemming from discrimination or identity theft. More broadly, privacy contributes to economic well-being by allowing individuals to maintain personal boundaries that underpin their ability to make choices that are appropriate for them (see discussion in Acquisti 2023). Indeed, it has a broad social value in that, for example, it allows for "uninhibited reading, speaking, and exploration of ideas," which in turn can foster innovation (as discussed in Solove 2013, p. 1,881).

Privacy, Trust and Regulation

Privacy allows one to differentiate between trusted and less-trusted interlocutors. In certain circumstances, such as the sharing of one's health information, trust that personal information will remain confidential is critical to the willingness of individuals to share information in the first place, which in this example can be vital to success in medical research or in addressing public health issues (Miller 2023). Indeed, there is a market for privacy: quite independently of legislated and regulatory strictures, firms can and do compete on the basis of the privacy protection they offer consumers and how they are seen to handle personal information.

Personal information can provide the firm with powerful insights about consumer behaviour, especially when it can digitally combine the information of many individuals and cross-reference such information against individuals' business interactions, such as purchases. It is not in the interest of a firm to be perceived as misusing that information, for fear of losing customers or users. Indeed it is in a firm's interest to use the information to provide a satisfactory experience, including through its ability to price discriminate in a way that would yield a benefit, e.g., to lower-income customers. However, by the very same token, such information also gives the firm a greater ability to engage in behaviour that, while rational from a business standpoint, does not necessarily favour individual customers or users induced to reveal information about themselves in their interaction with the firm.

In that context, individuals may have difficulty understanding the potential impact of sharing their personal information to access certain services, or the extent to which they are sharing it. This lack of understanding could mean that the market for privacy – the market for the ability not to share personal data – is not functioning properly. Individuals who might be willing to share x amount of personal information in order to access a good or a service may in fact be sharing more than they believe or know, such as through devices that automatically collect information about their physical or virtual whereabouts. They may not have the time to read complex forms where their consent is required or an organization's privacy policy is communicated. They may not always be practically able to assess or imagine the potential harms to them or to others that may stem from sharing their data.

This is where the economic need for public regulation comes in. It can help enforce privacy rights where individuals are ill-equipped to do so and where companies that collect the data are arguably in a better position to monitor the enforcement of these rights and potential misuse of the data. More generally, it can maintain public trust, which is foundational to the ability of the economy and society at large to benefit from the digital age.

Privacy Self-management

Solove (2013, p. 1,880) refers to the current approach to privacy protection in place in most Western democracies as one of "privacy self-management." This approach requires individuals to "decide for themselves how to weigh the costs and benefits of the collection, use, or disclosure of their information." While seeing it as "laudable and necessary," he criticizes what he sees as over-reliance on this framework, notably because it is impossible for individuals, even well-informed ones, confronted with many entities constantly collecting data about them, to know the full consequences of their choice. After all, many privacy harms are the result of an aggregation of pieces of data over a period by different entities. Privacy self-management, he writes, does not provide people with "meaningful control over their data."

Solove suggests future avenues by which policymakers could address this problem (pp. 1,900-1,903). One would be to harmonize the understanding of consent across different areas of law, so that individuals and other actors can have a more common understanding of what it entails. At the same time, he writes, consent is nuanced and its interpretation can depend on different situations, such as power asymmetries between the person asking for the consent and the person giving it. Privacy law, he says, "needs a new approach that accounts for the nuances without getting too complex to be workable." He rejects paternalism in regulation because it denies individuals their freedoms in the name, ironically, of making them free of worries. Instead, he advocates "nudges" that "seek to architect choices…without forbidding any options or significantly changing [individuals'] economic incentives."

Solove also advocates the use of privacy standards against which people can evaluate their choices in what he calls "Partial Privacy Self-Management." Just like the food we eat and the cars we drive, for which "we trust that these products will fall within certain reasonable parameters of safety," so it should be for privacy. Otherwise, people will find managing their privacy preferences among different entities gathering data on them "a nearly impossible task." Regulators, he says, should focus relatively less on the initial collection of the data, and more on the ability of society to navigate over time between: (1) potentially beneficial changes in the way existing data are used, without constantly having to require consent that might deter such uses; and (2) blanket consent that may open the door to harmful uses that are hard to anticipate or understand.

That said, privacy self-management, while insufficient, would retain a central role in Solove's scheme; it could be made more relevant through "consumer education, more salient notices, and more choices." Ironically, he says, one of the major impacts of the privacy self-management model and its fundamental consent requirement may be "raising self-awareness about data collection and use," with the "salutary effect of creating beneficial structural privacy protections and accountability inside institutions" (p. 1,900).

By and large, the CPPA heeds those observations, and moves Canada in the direction of strengthening the understanding and requirements for consent on the part of both individuals and organizations, as well as protection against current or future nefarious uses of personal data. At the same time, it leaves with individuals the central role of deciding how much they want to share and does not create a system so constraining that Canadians' personal information, once shared, cannot be used to create or offer goods and services that are beneficial to them.

Personal Information held by Private Organizations, and the State

Personal information (including one's communications) is sometimes concealed for nefarious purposes, which requires authorities to be able to compel its production as provided for by the law, or indeed permits an organization to disclose it to authorities if they believe a law is being, or about to be, contravened. Under the CPPA,

any part of a federal or provincial government that identifies its lawful authority to obtain an individual's personal information and indicates the disclosure is necessary to administer a law or conduct an investigation, may obtain that information without the individual's knowledge and consent.

An interesting question for the effectiveness of privacy legislation and its economic impact arises when a government's request for data may seem akin to a "fishing expedition" that compels an organization to produce data it holds about its vendors or customers, without prior evidence that an individual that the company is dealing with has or is about to do, something illegal. An example of an action that raises that type of question is the recent demand by the Canada Revenue Agency to Shopify to share information it holds about its individual vendors. While individuals would understand that their data could be shared with authorities if they are suspected of something nefarious, such as fraud, it is worth reminding them that authorities can also obtain their information without suspecting them personally.

Should Privacy Always be the Priority?

In addition to work by Solove, already cited, an extensive literature illustrates the delicate balance already referred to between preserving the privacy of personal information and policies that support a data-based economy (for a survey see Acquisti 2010).

Governments, businesses, and research organizations need to be able to use personal data – often a combination of them from many individuals – to better provide existing services or to innovate. Indeed, individuals themselves need these data, and data-enabled tools, to make better decisions. The gains for Canadians from the development and uses of digital technologies, including AI, are potentially enormous as they assist human power in fields as diverse as health, logistics, or regulatory enforcement. When governments set rules around the harvesting, using, sharing, or portability of data, they should not make them so unwieldy that they become excessively costly for businesses to navigate, nor so constraining that they make it hard for them to expand in the digital space. After all, Canadians also have the right to partake in the economic growth potential of the data economy. This question goes to the heart of current debates about possible further amendments to Canada's proposed privacy legislation, and should inform the regulations that are still to come and will have a significant impact on how the law affects Canadians.

There are divergent views of the extent to which privacy protection, whether it concern the ability of individuals to control the uses of their personal data or of the state doing it for them, can be legislated and enforced while still allowing Canadians to capture the full potential of digital technologies. At one end, there are those who would expand the control individuals have over the data they agree to share, once it is shared. For example, there are suggestions to further restrict what firms can do with de-identified data and make it more difficult to give or obtain consent. Such suggestions include further limiting instances in which consent can be implied by an organization, or reducing the list of exceptions companies can avail themselves of to avoid being swamped by requests for personal data erasure[11] (see, e.g. Scassa 2022, 04 July, 06 July and 18 July; Office of the Privacy Commissioner 2023).

11 Exceptions such as when they already have a data deletion schedule in place, or when information is de-identified. As mentioned above, there is a demonstrated risk that an entity having or gaining access to multiple databases, each with de-identified data, can triangulate these databases such that it is possible to trace data back to specific individuals. That risk is multiplied by cybersecurity risks. However, given all the other strictures around misuse of data in Bill C-27, the question is whether a reasonable person would consider the risk worth putting additional limits on the use of de-personalized data.

Furthermore, amendments recently proposed by the Minister of Industry, Science and Innovation[12] would refer to privacy, in the preamble and purpose clause of the bill, as a "fundamental right." This follows the recommendations of many critics (see, e.g., Office of the Privacy Commissioner 2023, Recommendation 1; Scassa 2022, 02 August; Short 2022). It is not clear what would be achieved concretely by that change, other than as a signal that privacy should systematically trump beneficial uses of personal data in the event of conflict. But in jurisprudence and for all practical purposes, privacy is already treated as a fundamental, quasi-constitutional right in Canada. There are broad exceptions in the proposed legislation for the use or disclosure of de-identified personal data for purposes designated as socially beneficial or by government-approved organizations, such as a healthcare or post-secondary education institutions. In this context, it is not clear why the economic benefits of supporting private research and innovation, or lowering the costs of producing goods and services, should not carry some significant weight against a systematically expansive interpretation of privacy rights.

Indeed, there are those who, while realizing that privacy rights and data protection need to be upgraded for digital age, nevertheless consider that the extent of government-mandated privacy protection should be weighed against other values, notably that of enabling the economic progress of society as a whole. For this group, the reasonable person standard on which some parts of the CPPA rest (such as when and how to obtain consent,[13] or when implementing data protection measures) is the right standard by which to gauge efforts to comply with privacy rules. This speaks to the importance of fostering a plain mutual understanding between individuals and businesses regarding:

(1) the meaning of, and need for, consent for the collection, use, and sharing of personal data;

(2) confidence in measures in place to ensure data protection;[14] and

(3) confidence that businesses will not divulge or cause to divulge personal information that should remain confidential.

An intense tug-of-war between these views scuttled previous federal legislation (Bill C-11), which in its final form was supported by business but had fallen well short of the positions of many privacy advocates. In the view of many of those who were critical, including Canada's Privacy Commissioner at the time, the many beneficial uses that private researchers and businesses can make of data collected from individuals are desirable but they must, when a possible conflict arises, yield to privacy rights. A similar tussle has continued with respect to C-27.

Critics who believe that the current bill is likely to be passed with few amendments contemplate carrying the fight for even stronger privacy rights to the provincial level (Scassa 2022, 02 August). One reason for the timidity (as they see it) of the federal legislation is the constitutional constraint around federal law-making powers in that

12 See: https://www.ourcommons.ca/content/Committee/441/INDU/WebDoc/WD12633023/12633023/MinisterOfInnovationScienceAndIndustry-2023-10-20-e.pdf

13 For example, the ability to collect and use an individual's personal information without their knowledge or consent, in the course of a business activity, where the information is not collected for the purpose of influencing their behaviour or decisions and a "reasonable person would expect the collection or use" of the information for such an activity."

14 Such as protections against data inaccuracy, theft, misuse, or accidental re-identification.

area. As mentioned, this constitutional constraint means that the federal government explicitly bases CPPA (and AIDA) on its trade and commerce power, carefully avoiding treading on the powers of other jurisdictions.

However, there are three key economic problems with the critics' favoured approaches. First, privacy is not defined in the legislation. Nor should it be. But formally bolstering the view of privacy as a "fundamental right" under CPPA risks open-ended interpretations (notably by the Commissioner of Privacy, or the government when it devises regulations) of where this right sits and of measures needed to protect it. This would potentially enshrine a paternalistic approach decried by experts such as Solove. The risk is that such steps taken in the name of privacy might not be properly checked against the costs to society – in terms of lost opportunities due to unnecessarily constrained access to data.

Second, the new disclosure, data protection, and reporting requirements under the CPPA will undoubtedly increase the cost of doing business. The cost of complying with a predecessor, Bill C-11, which died on the order paper as Canada headed to the polls in 2021, was already seen as creating barriers to entry for smaller firms. That is not to say that the costs are not worth it to society, or that they cannot be reduced by mechanisms such as templates for policies and reports required of organizations. However, here is a good place to pause until we can assess the impact, as businesses large and small institute the transparency, compliance and reporting mechanisms required by this significant reform.

Third, another cost looming large for businesses operating in Canada, and certainly for smaller businesses trying to expand beyond provincial borders, is that stemming from the potential fragmentation of provincial and federal privacy rules. Examples would be differing rules around consent to share personal information, the definition of "sensitive" information, or enforcement mechanisms. As mentioned, the CPPA allows the federal government to cede to provincial legislation whenever the privacy protection it provides is substantially similar or stronger – but this only makes it more important to reduce unnecessary small differences between federal and any provincial privacy rules applying to businesses. Further, even managing to do that would not address the issue of a potential patchwork of provincial laws, not to mention the applicability of federal laws to all interprovincial and international transactions regardless of provincial laws.

Such a patchwork would mean businesses having to decide whether they can afford to maintain distinct privacy policies for individual jurisdictions or pick one policy for their business that would meet the highest provincial/federal (or perhaps international) standard in each facet of the policy. (The latter approach is known as the "California effect" and involves harmonizing to the most stringent, economically large jurisdiction, even if its standards are costlier to implement.) Or, a business might decide to exit smaller jurisdictions that enforce standards that are more stringent than those enforced by larger jurisdictions. Their smaller size might not make it worth the cost of conforming to their specific rules.

Up to a point, there can be gains from experimenting with different models in terms of discovering what the sweet spot is between securing personal privacy and capturing the benefits of freer data flows. Arguably, a province could find a way to meet, or even exceed, the federal standards in a way that also makes it more competitive. But in most scenarios, lack of eventual convergence within Canada would be costly.

An equivalent problem exists across international borders. Privacy legislation that is not recognized as equivalent by foreign jurisdictions that are home to companies also operating in Canada risks disadvantaging the

smaller Canadian market(s). Part of the reason for strengthening Canada's privacy legislation is to make sure that such companies can benefit from the cross-border data flows enabled by such recognition.[15]

Further Addressing the Potential for Harm

An even more encompassing issue raised by critics of the proposed CPPA is whether it sufficiently protects individuals and groups from exploitation that may be facilitated by the collection and use of myriad individual data. For some, "talks of individual consent and control" are a "liberal fiction" if these broader harms are not addressed (Teresa Scassa blog August 2, 2023).

However, privacy legislation on its own cannot fully address these types of issues. Under the CPPA, individuals will have the right to receive explanations of decisions made or assisted by automated decision systems (such as algorithms or AI). Potentially, individuals from an identifiable group who realise through such a process that they are being discriminated against could, alone or collectively, demand that the relevant decision system be appropriately amended, and indeed lawyers anticipate class action lawsuits as a result.

In general, there is a limit to what privacy legislation can do to prevent harmful behaviour. On that score, the prevention of harms should be nested within principles and legislation that cover what is, or is not, acceptable in society as a whole, such as making harmful misrepresentation or hate speech illegal. This, regardless of whether the harm has taken place as a result of exchanges of personal data, made in a commercial setting or not, by electronic means or otherwise. Attempts to prevent harms by limiting the use of technologies that can incidentally cause them, are likely to have costly unintended consequences.

Additional Measures to Include in or Support the Implementation of the CPPA

That said, legislators and governments could help Canadians more easily achieve the balance between privacy rights as protected in C-27 and the benefits of innovation. They could do so by supporting mechanisms that make it easier to enforce and better define privacy rights, while also allowing businesses to confidently acquire and use the data at their disposal to expand the goods and services available to Canadians.

First, as they do in other areas, governments and companies should make wide-ranging efforts to help Canadians understand the benefits and risks for themselves of sharing (or not sharing) their personal data. The legislation already mandates companies to make easily available plain language versions of their privacy policies. But legislators could do more in this respect by mandating support for a joint federal government-business body dedicated to an education campaign (with case studies etc.) and providing and promoting a common understanding of the conditions under which information can be collected and used. These steps could allow individuals to easily detect when a company's policy differs from the norm, save individuals and businesses time in the conduct of legitimate transactions, and get ahead of costly frictions in the interpretation of the new legislation.

15 The need for compatibility between Canada's privacy rules and the EU's GDPR is a case in point. In 2001, the EU recognized Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) as providing adequate protection. According to the Trade Commissioner, "Canada's adequacy status ensures that data processed in accordance with the GDPR can be subsequently transferred from the EU to Canada without requiring additional data protection safeguards." See: https://www.tradecommissioner.gc.ca/guides/gdpr-eu-rgpd.aspx?lang=eng

Second, the federal government should contemplate leveraging its trade and commerce power further to seek harmonized privacy laws in Canada. The federal government should get ahead of the game in this respect, with ideas and mechanisms for harmonization around reasonably robust standards, or for mutual recognition of these standards, and not wait until a costly fragmentation occurs in this still-expanding regulatory field.

The federal government and the provinces are toiling, sometimes laboriously, to reduce barriers in other areas (ranging from training standards to corporate registries and securities laws), and it would be nonsensical to allow such barriers to develop here. Interpretive instruments – explaining, for example, how apparent discrepancies between two pieces of legislation can be navigated by businesses – could be useful in that regard. Provinces that do not have privacy legislation substantially similar to the federal government's should be encouraged to incorporate the federal legislation by reference into their own, highlighting for clarity any aspect of the rules that would be different in their jurisdiction. In the same vein, Canada, in collaboration with the provinces, should continue to pursue international interoperability of privacy rules with our key partners, to the extent this can be done without affecting the privacy protections of individual Canadians, so they can benefit personally or commercially from beneficial cross-border data flows.

Third, legislators and governments should specifically allow and encourage the use of streamlined privacy requirements and procedures and a longer phase-in for small businesses not dealing with sensitive information.[16] These might include supporting the introduction of accepted plain language templates for internal policies (concerning the collection, storage, use and sharing of non-anonymized data), public disclosures, the seeking of consent, and reports to the Privacy Commissioner, all of which will become more burdensome under this legislation.

Fourth, acknowledging that federal and provincial privacy authorities already regularly meet, Canadian governments should establish an advisory Privacy Council comprising the relevant federal and provincial regulators, consumers, and those in the business and the research community that pledge to a duty of care with respect to privacy. This duty of care, extending beyond legislated requirements, would be part of the Code they submit to the Privacy Commissioner under the terms of CPPA (see footnote 11). This Council would:

(1) review the effectiveness of steps taken to protect privacy under the legislation;

(2) raise any cross-cutting questions between different regulatory spheres requiring the use of consumer information;

(3) help institute safe harbor provisions for certain conduct, or regulatory sandboxes (for example, to assist in the development of privacy protection technologies) that are harmonized across Canada; and,

(4) in general, promote a national and open dialogue in the face of continuously emerging new challenges and new technologies.

16 Australia is expected to soon bring its small businesses not dealing in sensitive information under its new privacy legislation. They are currently exempt. However, an advisory panel has recommended a phased-in implementation of the new law for small businesses, on account of its especially burdensome cost for them.

Conclusion

The modernized consent-based framework proposed under CPPA allows consent to be implied for certain standard business circumstances where it is reasonable to think it would be given. It also makes it easier for individuals to understand the possible ultimate uses of the personal information they choose to share, and ultimately extends their control over their personal information held by organizations they do business with. It provides avenues for redress and ultimately the potential for severe penalties for businesses that do not take reasonable measures to prevent unauthorized disclosure or misuse of personal information. The companion *Personal Information and Data Protection Tribunal Act* moderates the new powers given Canada's Privacy Commissioner in that respect, with a new independent Tribunal. Overall, while still subject to improvements as discussed here, the balance in the currently proposed bill can help Canadians achieve the balance between their privacy rights and their ability to reap the economic benefits of the digital age.

References

Acquisti, Alessandro. 2010. *The Economics of Personal Data and the Economics of Privacy*. OECD Working Party for Information Security and Privacy and Working Party on the Information Economy. Joint Roundtable on the Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines. Background Paper #3. Accessed at: https://www.oecd.org/sti/ieconomy/46968784.pdf

_____ 2023. NBER. "The Economics of Privacy at a Crossroads." https://www.nber.org/system/files/chapters/c14785/c14785.pdf

Citron, Danielle, and Daniel J. Solove 2022. "Privacy Harms, 102." *Boston University Law Review*, 793. Accessed at: https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf

Fraser, David. 2022. "Canada's New *Consumer Privacy Protection Act* (CPPA): 12 PIPEDA Differences." McInnes Cooper Insights. June 30. Accessed at: https://www.mcinnescooper.com/publications/canadas-new-consumer-privacy-protection-act-cppa-12-pipeda-differences/

Gittens, Sébastien, Stephen Burns and Ruth Promislow. 2022. "Understanding the Draft of the Consumer Privacy Protection Act and Artificial Intelligence and Data Act". Bennet Jones *Blog*, June 16. Accessed at: https://www.bennettjones.com/Blogs-Section/Privacy-Reforms-Now-Back-Along-with-New-AI-Regulation

Innovation, Science and Economic Development Canada (ISED). 2022. Bill C-27 summary: *Digital Charter Implementation Act*, 2022. Accessed at: https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter/bill-summary-digital-charter-implementation-act-2020

Jares, Cathy. 2022. "Anonymization and De-Identification: A Comparison of PIPEDA and Bill C-27." Aird Bairlis Insights, September 25. Accessed at: https://www.airdberlis.com/insights/publications/publication/anonymization-and-de-identification-a-comparison-of-pipeda-and-bill-c-27

Miailhe, Nicholas, and Cyrus Hodes. 2017. "The Third Age of Artificial Intelligence." *The Journal of Field Actions, Field Actions Science Reports*. Accessed at: https://journals.openedition.org/factsreports/4383#tocto2n1

Miller, Amalia R. 2023. "Privacy of Digital Health Information." NBER. Accessed at https://www.nber.org/system/files/chapters/c14783/c14783.pdf

Office of the Privacy Commissioner of Canada. 2023. "Submission of the Office of the Privacy Commissioner of Canada on Bill C-27, the *Digital Charter Implementation Act*, 2022." Accessed at: https://www.priv.gc.ca/media/5922/sub_indu_c27_202304_eng.pdf

Thompson, Kirsten. 2022. "Canada's New Federal Privacy Bill C-27 – Summary of Significant Impacts and New Proposals." Denton's *Insights*, June 20. Accessed at: https://www.dentons.com/en/insights/articles/2022/june/20/canadas-new-federal-privacy-bill-c27-summary-of-significant-impacts-and-new-proposals

Scassa, Teresa. 2020. "Replacing Canada's 20-year old Data Protection Law." *CIGI Opinion*. Available at: https://www.cigionline.org/articles/replacing-canadas-20-year-old-data-protection-law/

_____. 2022. Blog. Accessed at: https://www.teresascassa.ca/

Solove, Daniel J., 2013. "Privacy Self-Management and the Consent Dilemma." George Washington University Law School Public Law Research Paper No. 2012-141, Accessed at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018

Short, Bryan. 2022. "The Absolute Bare Minimum: Privacy and the New Bill C-27." Open Media post, September 14th. Accessed at: https://openmedia.org/article/item/new-bill-C27

Varian, Hal R. 1997. "Economic Aspects of Personal Privacy." In *Privacy and Self-regulation in the Information Age*, Chapter 1. National Telecommunications and Information Administration. Accessed at: https://www.ntia.gov/report/1997/privacy-and-self-regulation-information-age

Wagner, Wendy J. 2023. "Guide to Doing Business in Canada: Privacy Law." *Insights & Resources*, Gowling WLG, 20 October. Accessed at: https://gowlingwlg.com/en/insights-resources/guides/2023/doing-business-in-canada-privacy-law/

This E-Brief is a publication of the C.D. Howe Institute.

Daniel Schwanen is Vice President, Research, at the C.D. Howe Institute.

This E-Brief is available at www.cdhowe.org.