UNIVERSITY OF TORONTO
FACULTY OF LAW

2022

PRIVACY LAW IN THE 21ST CENTURY

Future of Law Lab
University of Toronto Faculty of Law

PRESENTED BY

Sophie Fu
Arshia Hassani
Stephen Hope
Isaac Jonker
Michelle Slipanchuk

FUTURE OF LAW

Privacy law in the 21st century

With technology rapidly advancing, privacy law has struggled to keep up. As a relatively newer body of law, Canadian consumer data protection law has not seen an update in the 20 years since PIPEDA was legislated, where Alan Westin's ideas of privacy were first incorporated into a Canadian privacy context. In 2019, the federal government introduced the Digital Charter which sought to do just that, and Bill C-11 followed a year later to implement those ideas. This move was meant to follow other jurisdictions like California and the European Union which have both enacted strong consumer privacy protection laws. These laws broadly are a response to technological transformation and concerns over surveillance capitalism, where large corporations utilizing algorithms to leverage aggregate data as a business model have proven difficult to regulate; many critique PIPEDA for not ensuring that a meaningful level of consent is obtained from these companies for the data they collect, in part because of a lack of teeth in enforcement. C-11 changes consent on many dimensions, including through provisions on privacy policies and a new tribunal to strengthen enforcement. However, how these changes will look in practice is still an open question.

PIPEDA in action – the Clearview AI investigation

This investigation is a great case study into how effective PIPEDA's existing framework is. There, complaints about PIPEDA violating disclosures of Facebook user data to a third party app (thisisyourdigitallife - TYDL) were made to the commissioner. It was found that Clearview AI had essentially scraped data of the friends of users of that app, where no consent had been obtained from those users. This data was used for targeted political messaging. Given the main thrust of PIPEDA is its focus on ensuring consent in the collection, use, and disclosure of personal information, the investigation found that Facebook had failed to obtain valid and meaningful consent from users of that app for the purposes the data was used, as well as from the Facebook friends of those users whose data was also taken and sold.

While it may to the layperson seem as though the law was sufficient to impugn Facebook here for violating the privacy rights enshrined in PIPEDA, the story is not yet complete. This investigation took place 10 years after a previous investigation by the privacy commissioner, who pointed out that Facebook was non-compliant with PIPEDA in similar ways. Even after 10 years, Facebook's policies were still deficient. Aside from these two censures, no further action was taken against Facebook in respect of these violations. Why? Because PIPEDA was never actually mandatory for businesses to follow. Division 1 section 5 provided that "organization should comply… indicates a recommendation and does not impose an obligation". Given the limited accountability for organizations violating PIPEDA, its power to protect privacy rights becomes more limited year after year.

What's happening with Bill C-11 – the Consumer Privacy Protection Act?

Tabled in 2020, the Bill died on the order paper when the 2021 Federal election was called. While legislators seem to be in no rush to pass any new privacy legislation, privacy pressures are increasing globally, and some would expect Canada to eventually follow the trend. C-11 gave insight as to the kinds of reform Canadian legislatures are contemplating, and formed the best picture of what legislation is yet to come.

Consent in C-11

C-11, like PIPEDA, was organized on the basis of consent. While many small changes were made to the language of when consent can be collected, reversing the onus on implied consent and other provisions, many similar concerns that animated critiques of PIPEDA are still present. Some are concerned about even larger gaps in this regime.

For example, C-11 created a list of exceptions to consent. As long as it would be impractical and a business does not use the data to influence any person's behavior, data can be collected without knowledge or consent pursuant to broad business objectives, like "reducing commercial risk", and where "obtaining the individual's consent would be impracticable because the organization does not have a direct relationship with the individual".

Additionally, the collection of deidentified data has been permitted without knowledge or consent wholesale, despite risks of reidentification and data breaches. These expansions apply for organizations pursuing research and public health purposes, but serve as an expansion of data availability generally, for better or for worse.

Privacy Policies

As the supposed vehicles for valid consent, privacy policies generally have been seen as a failure in respect of policy objectives. It has been demonstrated that incredibly few people read the policies, and even fewer understand what they agree to meaningfully. Even if each user read and understood each one, the cost benefit for users (time taken to read per unit of information disclosed) skews hard to the negative. How would C-11 have changed these?

C-11 continues the role privacy policies play in the framework, though the formal requirements are strengthened in the bill, requiring them to be "in plain language", as opposed to "generally understandable" as PIPEDA requires, seemingly a higher standard. The policies would be required to explain how automated algorithms make predictions, recommendations or decisions about individuals that could have "significant" (which is not a defined term) impacts. They would have to explain which exemptions to consent the organization may use, and whether or not the organization transfers personal information extraterritorially that may have reasonably foreseeable privacy implications (which are not defined terms). They must also provide information for how individuals can dispose of their personal information.

But the strength of these improvements depends on whether people in reality will read the policies, a situation which most readers know to be a fiction in the vast majority of cases.

Enforcement

Perhaps the largest change to the regime contemplated resides here. While a very limited basis exists today for the enforcement of our privacy laws (where censure from the Privacy Commissioner is the only real likely deterrent), C-11 requires compliance and backs this up with some teeth.

The Privacy Commissioner in a C-11 world would have the power to issue binding orders and recommend penalties to a new Privacy Tribunal, which would have appeal powers. Though only some sections could have been enforced through monetary penalties, those penalties match the scale of comparable legislation like the GDPR. Additionally, a (limited – must go through the commissioner) private right of action would have been entrenched.

Would the Facebook investigation look any different under PIPEDA?

Users who installed the TYDL app

Consent would have still been violated. Similar to PIPEDA, C-11 stipulates that a consent will only be valid if the users are provided with the purposes for, methods of and any reasonably foreseeable consequences of the collection, use or disclosure of the personal information. As found by the OPC/OIPC BC, the app screens did not provide explanations as to the purposes for which the information was sought, or the potential consequences that could result from disclosure of that information. There was no clear indication of the ultimate purpose (i.e., political purposes) for which personal information is collected and used.

Facebook friends of the TYDL users

Consent would have still been violated. Similarly to the users themselves, the language in Facebook's privacy policy is too broad and insufficient to constitute consent from affected users to disclosure of their personal information to the app

Would Facebook have had safe harbor in an exception to consent?

Not likely. To use any exception under C-11, the data must not be used for the purpose of influencing individuals. It is likely that the political purpose of the collection would have disentitled Facebook to any exemptions. Even then, Facebook would have to have included a disclosure that they were using such an exception in their privacy policy.

Would Facebook be fined under C-11?

Not likely. Although Bill C-11 allows the imposition of large fines on organizations subject to privacy violations, it restricts finable offences related to consent to two areas only: companies that force a person to give more personal information than necessary in order to receive a product or service; and companies that obtain consent through deception. It seems that Facebook's error was primarily of negligence in failing to obtain consent or enforcing their internal policies through third party apps as opposed to actual deception.

Critical perspectives on issues remaining in a C-11 Canada

The Privacy Commissioner

This article from Fasken discusses the views of the Federal Privacy Commissioner on Bill C-11 and its inadequacy in addressing privacy issues of the 21st century. Importantly, the Commissioner thinks that focusing solely on a consent-model for obtaining data can permit "objectively unreasonable" activities, since what would be required to engage in such activities is just the user's consent. Similarly, focusing mainly on a consent-model to obtain data could undermine the public interest as there may be instances where users refuse to give consent for initiatives valuable to society. Ultimately, the Commissioner thinks that there should be a rights-based framework in combination with regulatory oversight that can accommodate unforeseen yet appropriate uses of data which either serve the public or a business interest, instead of only prioritizing a consent-model. With respect to this rights-based framework, the Commissioner indicates that it would have been favourable for Bill C-11 to have a preamble suggesting that the rules set out in the Bill should function in a manner that recognizes the essential right to privacy.

As well, the Commissioner notes that the current separate data collection regimes for the public sector (Privacy Act) and the private sector (PIPEDA) contribute to private organizations obtaining and using data without necessarily having proper consent. For instance, it is possible for public institutions to legitimately acquire data from individuals, and then have private organizations that are working with that public institution gain access to such data and use it for their own purposes without necessarily acquiring proper consent from the individual. The fact that Bill C-11 merely aims to modernize PIPEDA could mean that this divided regulatory system will still exist and the risk of such privacy infringements may continue.

Additionally, the Commissioner seems especially concerned about the new penalty system of Bill C-11. He seems unsatisfied with the penal provisions, noting that many violations do not have any penalties. Importantly, Bill C-11 does not have penalties for all consent rules that are violated. The fact that Bill C-11 does not effectively punish breaches in this realm may be considered a serious short-coming.

The Privacy Commissioner

Bill C-11 does not include the requirement that individuals completely appreciate what they are consenting to. The bill also allows companies to vaguely describe the reason that they are seeking the user's consent. As such, the bill may not function effectively to promote awareness among users that they know what they are consenting to.

Teresa Scassa

In this article, Professor Scassa notes Bill C-11 also does not explicitly address the privacy rights and interests of children and youth. Obviously, children and youth have unprecedented access to digital technology and they regularly engage with data-collecting applications. The fact that Bill C-11 does not clearly address the interests of children and youth in this realm could be considered an insufficiency of the proposed law, as dealing with consent issues for this age-group is essential to forming an effective and modern data-collection regulatory regime.

International Network of Privacy Law Professionals

Part of Bill C-11 includes creating a Tribunal that would oversee the powers given to the Office of the Privacy Commissioner. In fact, the Tribunal would have the authority to hear appeals on decisions made by the Commissioner and the ability to "set fines on organizations proposed by the OPC." The issue in this accountability structure is that it does not require members of the tribunal to be experts in the subject-matter. Specifically, the proposed law would only require a small portion of the tribunal to be experts in the area of privacy and information law. Clearly, this field is considerably complex and demands a fair amount of knowledge and expertise. This organization is concerned about the fact that some Tribunal members dealing with issues of digital privacy and consent may not have any expertise in the discipline.

The Hill Times

This The Hill Times publication takes the view that Bill C-11 does not effectively contemplate privacy concerns relating to political parties. Particularly, it appears that political parties are not subject to the CPPA and do not face privacy regulations as commercial entities do. There is no doubt that political parties collect significant amounts of data from individuals and use it to advance their personal interests. Specifically, political parties collect information on voters and use it for political campaigning. Numerous states have some form of privacy regulation for political parties; it makes clear sense that such organizations should be governed by some form of privacy regulation. Bill C-11's failure to include political parties in the privacy regulations it proposes is arguably a significant shortcoming. When Minister Bains was asked about this, his office simply stated that political parties already face regulation for data sharing under the Elections Modernization Act. Nonetheless, such a law is fairly limited in properly regulating data sharing/collection for political parties as it merely mandates that parties have and publish privacy policies. As well, one should consider that the elected government is itself a political party, and therefore it has direct interests in the regulation of such organizations. Accordingly, it may be more difficult to form and

pass legislation that effectively upholds the privacy interests of the public in relation to political parties.

What direction is our law heading in?

We are heading closer towards viewing privacy as a right, but still the CPPA stops short of treating it as such (focus is on data protection, not privacy as a right). The legislation, like PIPEDA, still focuses on finding a balance of proportionality between commercial and privacy interests. There are human rights principles (minimal impairment, necessity, proportionality) at the forefront of the legislation, and future legislation may continue inching closer towards crystalizing privacy as a human right (similarly to GDPR). While consent is still the main thrust of the legislation, it is arguable that commercial interests are favored over data subjects when it comes to exceptions to consent.

How does our law compare to other jurisdictions?

Other jurisdictions don't focus on consent as the first line of defence, instead, their laws focus on a rights-based framework. They put more power in the hands of individuals once their data has already been collected - (like the right to be forgotten – to have information about you deleted at your discretion); this is the case in both California and in Europe. But these rights even in more progressive jurisdictions remain limited.
Bill C-11 does also put some power into consumer's hands by allowing them to request access to their personal data and request the removal of their personal information. While PIPEDA users have access powers, the right to request removal is not yet available here.

Conclusion

Although C-11 never saw the light of day, similar legislation might in the near future. C-11 gave us a chance to see what that legislation might look like. Though it makes many innovative strides, like the Tribunal, more effective privacy policies, and meaningful teeth in enforcing the laws over its predecessor PIPEDA, C-11 still posed many problems, like in its outdated reliance on consent and its exceptions to consent. Whether it struck an appropriate balance between the interests of businesses and consumers cannot be said without seeing it in practice, but there is much to be hopeful about; lawmakers for the first time ever proposed legislation that could punish organizations for their arguable exploitation of user data. The concerns of surveillance capitalism, and the growing demand for privacy rights are being at the very minimum contemplated by parliament. But with parliament going in this direction, it's clear that privacy lawyers have a bright future.

Future of Law Lab

University of Toronto Faculty of Law

Web: futureoflaw.utoronto.ca
Twitter: @Futureoflawlab