CANADA'S OUT-OF-DATE ONLINE PRIVACY RULES AREN'T PROTECTING YOU

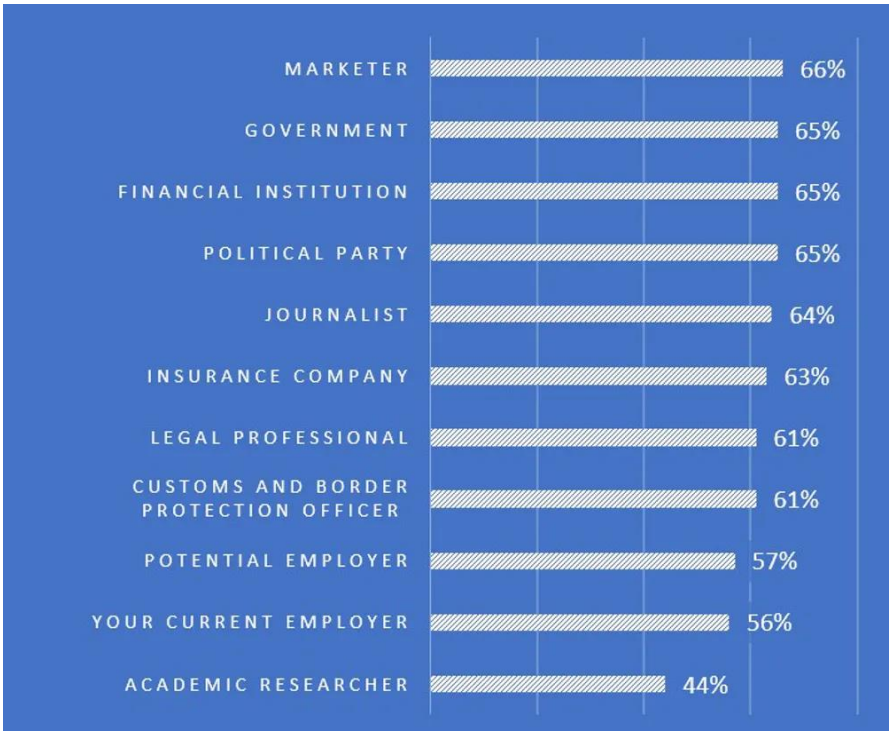
Anatoliy Gruzd | August 19, 2020

With so many of us stuck at home due to the pandemic, people have been spending a lot more time online in general and on social media in particular. This is not surprising, considering that 99 per cent of Canadian households have access to broadband internet and 94 per cent of online Canadian adults have an account on at least one social media platform, making Canada one of the most connected countries in the world.

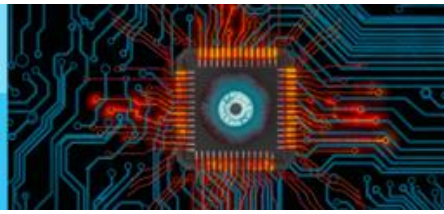
However, as we increasingly rely on these platforms to connect us and mediate our relationships, we are also creating more data about our interests and habits. This treasure trove of data about us and the people in our network is being used by a wide variety of stakeholders, including social media platforms and many third parties.

Increasing discomfort

In this context, it is not surprising that social media users are becoming increasingly uncomfortable with how much data is being collected about them and how it is being used. For example, in our survey of 1,500 Canadians, 65 to 66 per cent of respondents said they are uncomfortable with marketers, government, financial institutions and political parties accessing information about them or posted by them on social media.



The percentage of 1,500 respondents who are uncomfortable with third parties accessing publicly available social media data posted by or about them. (Ryerson University Social Media Lab's Social Media Privacy in Canada Report, 2018), Author provided



This lack of comfort is one of the signals telling us that Canadians' online data are not adequately protected under the current Personal Information Protection and Electronic Documents Act (PIPEDA).

PIPEDA is 20 years old, and bringing it in line with the principles set forth in Canada's new Digital Charter is one of the stated priorities for this government. However, the process has been delayed first by the federal election and now by the pandemic. The pandemic itself has also escalated the development and deployment of emerging data-greedy digital tools and techniques such as contact tracing and facial recognition, making a revamp of PIPEDA more critical than ever.

A new privacy and data protection regulation should also account for emerging technologies and their applications that will drive our digital economy in a near future.

Lessons from elsewhere

When the European Union enacted the General Data Protection Regulation (GDPR) in 2018, it found itself in conflict with a whole class of emerging technologies that are based on blockchains. Blockchain is the same technology used to create Bitcoin, but it is not limited to just cryptocurrencies. It also powers social media sites like Steemit, Minds and Memo, which give users more control over their personal data.

The decentralized nature of these blockchain-based sites makes it challenging to comply with GDPR, which assumes that there is a single data controller (either a person or legal entity) that collects personal data from individuals and is responsible for protecting such data. In peer-to-peer blockchain networks, the ledger that stores all data is distributed across multiple nodes and is not controlled by a single entity.

In effect, this constitutes "joint controllership," which is challenging to apply and interpret within the GDPR framework. The decentralized design also conflicts with GDPR's principle of data minimization, requiring data controllers to minimize the amount and types of data collected and stored about individuals.

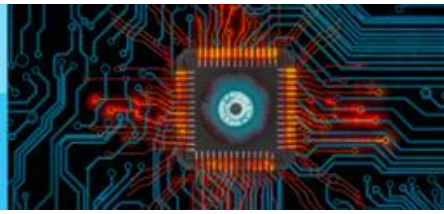
Another design feature of blockchains to protect data from modification or deletion contradicts the "right to be forgotten" provision of GDPR, which assigns people the right to request deletion of their personal data "without undue delay."

Future protections

Current regulations will need new guidelines that address decentralized, user-driven data collectives like blockchain-based social media sites. But even though these efforts are still underway in the EU, here in Canada there are a couple of lessons we can learn from this example.

First, it is crucial to make sure that updating PIPEDA does not only focus on today's technologies but also what is on the horizon. This is because emerging technologies such as blockchains are changing the power dynamics between data controllers and subjects by creating new ways for user data to be created, collected, accessed and shared.

The second lesson is that ensuring flexibility and accountability to allay Canadians' concerns about the ways that personal data is used will require creativity in working with all stakeholders, including users, governments, platform providers, data brokers, data-driven industries, app developers, researchers, civil society groups and others.



Doing so will allow Canada to foster the next wave of digital innovation while still protecting and empowering Canadians' data rights.

The Royal Society of Canada has established the Infoveillance Working Group to consider the implications of surveillance, data, privacy and equality. The working group has begun work in analyzing a transition from individualistic notions of 'privacy protection' to the arrival of surveillance capitalism, which refers to an economic system of accumulation based on the commodification of personal data. Surveillance capitalism has many features including datafication (social action transformed into quantified data), dataism (a naïve belief in the capacity of data to solve human problems), dataveillance (using data for surveillance of populations and individuals), and discriminatory profiling (with particular implications for people from already-marginalized communities).

The Working Group Members are: Jane Bailey (University of Ottawa); Benoît Dupont (Université de Montréal); Anatoliy Gruzd (Ryerson University); and David Lyon (Queen's University).