Apr 5, 2019,
6,187 views | 08:58pm

How Privacy Laws Are Changing To Protect Personal Information

Carole Piovesan Contributor
COGNITIVE WORLD Contributor Group
AI & Big Data

DEPOSITPHOTOS ENHANCED BY COGWORLD

Over 2.5 quintillion bytes of data are created each day. Much of this data consists of information that would allow people to be personally and individually identified (or, personal information).

There are currently over 2 billion active Facebook users. Every minute, approximately half a million snapchat users share photos while Instagram adds another 50,000 photos to that total. There are half a million tweets sent every minute. The amount of personal information that is being exchanged each day is staggering and growing.

At the same time that we share our personal information, there is growing concern with how that information is being gathered, stored, used and shared at scale. While many jurisdictions like Canada and the EU have privacy laws dating back to the mid 1990s, changes to data practices in the past five years have motivated governments to review or update existing laws to reflect current realities. In the US, new legislation has either been introduced or is being considered at federal and state levels.

Changes to privacy laws are being fuelled in part by growing public concerns with

the idea of unfettered data accumulation and use. For instance,

- earlier this year, Ipsos and the World Economic Forum released, Global Citizens and Data Privacy, which found that 1/3 of global citizens are ignoran about how their personal information is used by companies and governments and that trust is lacking. The report also found that citizens do not trust companies or governments to use their personal data in "the right way";
- a 2019 report by the Centre for the Governance of AI - Future of Humanity Institute, Oxford University, entitled, Artificial Intelligence: American Attitudes and Trends, found that the majority of Americans identify data privacy, AI-enhanced cyber attacks, surveillance, and digital manipulation, as being among the governance challenges most likely to impact large numbers of people; and,
- a 2017 Pew Research Centre, Americans and Cybersecurity, showed that 50% of Americans believed their personal data is less secure today than it was five years ago.

Regulation, often slow to adapt to the pace of innovation, is starting to catch up with the extent of personal information being transmitted every minute.

How privacy regulation is adapting to innovation and why we care

Privacy laws are changing to address the real and perceived risks of harm resulting from the under- or unregulated data economy.

The EU's General Data Protection Regulation (GDPR)

The EU has introduced significant reform to legislation aimed at protecting privacy, promoting competition and wrestling the ever-growing power out of the hands of the few. The GDPR, which came into effect in May 2018, replaced the European Directive 95/46/ec and introduced strict requirements for those that control or process the personal data of EU residents. The GDPR's stated objectives focus on th

protection of personal information, “the free movement of personal data” and “the fundamental rights and freedoms of natural persons to the protection of their personal data”.

Here are a few things that are particularly striking about the GDPR:

- extraterritorial reach, meaning that the GDPR is applicable to companies collecting or using the personal information of EU residents, regardless of whether the processing takes place outside the EU (Art. 3);
- the right to be forgotten, which includes the right to have one’s personal data erased from a company’s system on certain grounds (Art. 17);
- the right to move data from one controller to another under certain circumstances and where technically feasible (Art. 20);
- the right not to be subject to automated decision-making including profiling (Art. 22);
- mandatory reporting of a personal data breach unless the breach is “unlikely to result in a risk to the rights and freedoms of natural persons”. Notification is required within 72 hours after having become aware of the breach (Art. 33)
- significant penalties for non-compliance of up to 4% of annual global turnover of the preceding financial year or €20 Million, whichever is greater (Art. 83(5)).

While the stated objectives of the GDPR are grounded in values of self-determination and protection of privacy, among others, another point of view holds that the EU’s main motivation is much simpler: competitiveness.

A recent article in The Economist, Why big tech should fear Europe, reported that the US is home to 15 of the world’s valuable technology firms, whereas Europe is home to one. Europe has enacted such far-reaching legislation to restore stability

and control to governments and their peoples and to prevent anti-competitive behaviour where data (and thus power) are accumulated by a few.

The Economist's article summarized the point well:

...the EU is pioneering a distinct tech doctrine that aims to give individuals control over their own information and the profits from it, and to prise open tech firms to competition. If the doctrine works, it could benefit millions of users, boost the economy and constrain tech giants that have gathered immense power without a commensurate sense of responsibility.

The United States

Certain US states are also entering the ring in the fight for control over personal dat – California being out front. The *California Consumer Privacy Act* (CCPA), which comes into effect on January 1, 2020, aligns with GDPR principles to provide greate control to individuals over their personal information. The CCPA establishes "a lega and enforceable right of privacy for every Californian" and will:

- require businesses to make disclosures about the collection of personal information, the categories of personal information collected, the purposes for collecting and selling personal information, and the categories of third parties with which personal information is shared;
- authorize consumers to opt-out of having their personal information sold by business while prohibiting that business from discriminating against the consumer for exercising this right;
- authorize businesses to offer financial incentives for the collection of persona information;
- prohibit businesses from selling the personal information of consumers under the age of 16 years;

- require data breach notification.

According to the NYU Journal of Intellectual Property and Entertainment Law, a number of US states have passed or are actively considering privacy legislation. And this localized approach to regulating privacy is prompting calls from members of the federal government as well as industry for a harmonized federal privacy law. The argument goes that a federal law would avoid inconsistent and overlapping legislation, as is the case with breach notification laws that vary across all 50 states.

This past fall, it was reported that representatives from Amazon, Apple, AT&T, Google and Twitter urged Congress to implement federal privacy legislation. There is a sense that privacy legislation is on the near horizon in the US.

Canada

Canada has also undergone review and change of some of its privacy regulation. Canada has overlapping federal and provincial laws as well as sector-specific privacy laws (namely regarding personal health information). This past summer, the federal Minister of Innovation launched data and digital transformation consultations to better shape Canada's approach to innovation. As one of six experts appointed by the Minister to conduct consultations on his behalf, I heard a number of companies, academics and civic organizations talking about greater national and international harmonization of privacy laws as well as deeper investments in cybersecurity, among other things.

On November 1, 2018, an amendment to Canada's federal privacy law, *Personal Information and Protection of Electronic Documents Act* (PIPEDA), introduced mandatory reporting obligations for data breaches that rise to a real risk of significant harm. All data breaches must be documented by the company and that document must be retained for up to two years.

A few months later, the federal Privacy Commissioner issued guidelines for obtaining meaningful consent that focus as much on substance as they do on form

(i.e. just-in-time information when obtaining consent). The guidelines were the result of public consultations as well.

Also in 2018, the House of Commons Standing Committee on Access to Information Privacy and Ethics released a detailed report after conducting its own review of PIPEDA. The report included several significant recommendations including measures to improve algorithmic transparency (understanding how automated decisions are made) and reflections on the usefulness of maintaining a consent-based model.

These are three examples of jurisdictions that are actively pursuing more progressive privacy laws. One important consideration is to harmonize global standards for best practices involving the collection, storage and use of personal information. This will ease compliance across border, enable greater certainty of the rules of engagement with personal data, and will provide a valuable signal to the public that governments are keeping pace with rapid change.

Carole Piovesan

Carole is a Partner and co-Founder of INQ Data Law where she focuses on data governance, privacy, cybersecurity and artificial intelligence. Prior to co-founding INQ, Ca... **Read More**

COGNITIVE WORLD

COGNITIVE WORLD is a think tank, knowledge hub and ecosystem for AI transformation.