Information Privacy in the Digitized World

By S. Balasubramanya, LLM Student, Gould School of Law, USC, Los Angeles – March 27, 2020

In a time when most of our daily processes have gone digital — from socializing, to banking, to ordering pizza — issues around information privacy have become more acute and complex.

We constantly exchange our personal information, including names, addresses, phone numbers, email addresses, passwords and more. Third parties can easily gain access to this information, which is a potential violation of our privacy. So how do we protect ourselves from the misuse of our personal information? How does the law protect against such misuse and how can a breach of privacy be rectified?

The importance of privacy

In today's commercial environment, sellers of products and services — including the government — are eager to reach their target customers more effectively with refined advertisements. They need accurate and specific personal details, including habits and past transactions, to alter and fine tune their offerings to align with their customers' changing needs. In the digitized world, such information, including locational details, can be sourced from "data brokers," who extract customers' personal information, sliced and diced across various attributes, and sell it to digital advertising entities.

This selling of citizen or consumer data has become politically charged in recent elections, and data brokers have gained influence over lawmakers to ensure their services can continue.

A privacy breach exposes an individual's personal information to the public. This exposure can be misused by hackers who can get unauthorized access to bank accounts, send offensive communications using stolen credentials, send ransomware to demand payment, cause cyberattacks on critical infrastructure to bring down essential services like utilities, and more. The impact of such a breach can affect a few individuals or millions — and there have been many instances of large-scale data breaches over the last five years.

Protecting your private information

Personal information is data that can uniquely identify a person: name, date of birth, place of birth, address, social security number, driver's license number, passport number, mobile phone number, email address, bank account numbers, credit card numbers, marital status, etc.

There are multiple ways personal information can be protected.

Individuals can make sure they provide personal information only on a need-to-know basis to trusted entities, with explicit consent. However, this by itself does not ensure full protection. What if the data gets stolen or leaked? Trusted entities are expected to protect individuals' personal information through suitable technologies, like data encryption, safe data storage and collection of only the minimal personal information required, as well as providing individuals with opt-in and opt-out capabilities.

An additional approach would be state legislation regarding the protection of individuals' data and in the event of a breach, and to penalize the responsible entity and perpetrators.

It is important for the public to understand the consequences of such a breach, as well as what rights they have to protect their personal information, and what compensation can be expected if they suffered damages as a result.

Legislation around the world

In tune with technological changes, legislative changes to accommodate and address potential benefits and issues emanating from such technological change is necessary. Though the concept of privacy has existed for centuries, the more recent concept of data breaches in a digitized world requires specific legislation to address data protection.

More than 100 countries have adopted data protection legislation around the world. Examples include the 2018 California Consumer Privacy Act, (CCPA), the 2016 European Union General Data Protection Regulation (EU-GDPR) and the 2019 Personal Data Protection Bill of India (PDPB). There are significant differences among them in terms of how the privacy dimension is treated in different jurisdictions.

The CPPA took effect in January 2020 and secures new privacy rights for California consumers. The law is taking the lead in a big way to define new contours of privacy by granting a set of new rights to California consumers:

- The right to know what personal information is collected, used, shared or sold
- The right to delete personal information held by businesses and their service providers
- The right to opt-out of sale of personal information and also to direct a business that sells personal information to stop selling it (Children under the age of 16 years must provide opt in consent, with a parent or guardian consenting for children under the age of 13 years)
- The right to non-discrimination in terms of price or service when consumers exercise a privacy right under this legislation

The legislation applies to specified businesses with revenues exceeding $25 million and which buy, receive or sell personal information of 50,000 or more consumers, households or devices. Additional obligations apply if any businesses handle the personal information of more than 4 million consumers or derive 50% or more of annual revenue from selling consumers personal information.

Businesses subject to CCPA must provide notice to consumers at or before data collection and create suitable procedures to respond to requests from consumers to opt-out, including deletion of data after due verification of consumers making such requests, as well as maintain appropriate records. Businesses must also disclose the financial incentives offered in exchange for the retention of a consumer's information and how it is calculated, as well as furnish a comprehensive privacy policy.

The state also has the California Electronic Communication Privacy Act, which limits government authorities' ability to seek electronic information for law enforcement purposes.

At the national level, the U.S. has privacy laws including the 1998 Federal Trade Commission Children's Online Privacy Protection Act, for parents to control what information websites can collect from their children; the 1996 Health Insurance Portability & Accountability Act, for safeguarding medical information; the 1999 Gramm-Leach-Bliley Act, for financial institutions dealing with private information of individuals; and the Federal Communication Commission's 2017 amendment for privacy and data security regulations of broadband internet services providers.

Europe's GDPR came into effect in May 2018 and applies to all member states of the European Union. The law replaces the earlier Data Protection Directive 95/46/EC, defines privacy as a fundamental right and harmonizes data privacy laws across Europe.

GDPR applies to all businesses that process personal data of data subjects and people residing in the EU, regardless of where the business is located. Non-EU businesses processing the data of EU citizens have to appoint a representative in EU.

The law stipulates that data subjects must provide explicit consent to the data controllers for specific purposes and be notified within 72 hours of controller or processor becoming aware of any data breach affecting their personal information. GDPR also gives data subjects the right to obtain confirmation from the data controller as to whether or not their personal information is being processed, where and for what purpose, and the controller must provide a copy of the data. Data subjects are also given the "right to be forgotten."

Under the GDPR, organizations need to adopt "privacy by design" approach — to minimize data collection and processing to only that which is necessary. They must also appoint a mandatory Data Protection Officer.

Data controllers and processers can be fined either 2% of their annual global revenue or 10 million euros (whichever is higher) for less severe infringement or 4% of their annual global revenue or 20 million euros for more serious infringement.

The parliament in India is reviewing the 2019 Personal Data Protection Bill of India. In its current draft, the bill prescribes privacy as a fundamental right protected by the state and establishes the independent Data Privacy Authority. The rights are an extension of the constitutional right to freedom of speech and expression and right to information.

Like the GDPR, India's bill calls require consent from the subjects to allow collection of personal information, and a higher level of consent is needed for sensitive data — like medical information. Data subjects are also granted the "right to be forgotten."

Transfer of personal information outside of India likewise requires consent of the subject and can be permitted with additional specific consent for sensitive personal information.

The bill calls for children's data to be subject to greater protection and for data subjects to be notified in event of a serious breach, as soon as possible.

Finding clarity — and justice

For today's digital businesses and global citizens, it can be challenging to determine what rights and restrictions are enforced in which jurisdictions. What type of data processing can be done where? What constitutes a cross-border data transfer? How do we deal with any potential or actual breach?

Even for corporate, business or data fiduciaries, it is a very complex issue. Some of the more onerous requirements are for data residency and data retention within the geographical jurisdiction. It is common for both corporations and individuals to use a cloud data service provider — like Google Drive or Amazon Web Services — which provides internet-based computing and storage facilities that don't store data in one physical geographical place.

The complexity increases in terms of breach notification, documentation and other supervisory controls. Data travels globally, and there is increased need for lawyers from different countries to be familiar with similar regulations in other parts of the world. Without a deeper understanding of these privacy laws, it would be challenging for lawyers to advise their clients properly to enable them to collect and process their customers' data.

Becoming our own data advocates

With blurring physical boundaries in the digital world, the laws and procedures for implementing privacy protections at an international scale is going to be a big challenge, especially in a time when data, the new currency of the 21st century, is growing in value.

But every individual can, and should, take the lead in protecting his or her own personal data from potential misuse. By maintaining effective control over personal information, individuals can minimize their risk of a breach.

Sources:

United Nations Conference on Trade and Development

California Consumer Privacy Act (CCPA) Fact Sheet - Office of the Attorney General, California Department of Justice

Comparing privacy laws: GDPR v. CCPA

Comparative Table of Personal Information Protection Laws

Comparison: Indian Personal Data Protection Bill 2019 vs. GDPR

CCPA and GDPR Comparison Chart