RBC Global Asset Management

Data privacy and security in the time of COVID-19

Strong data privacy protections enable corporations to establish boundaries and limit access to information that is protected under data privacy laws. Following the outbreak of the novel coronavirus (COVID-19) and its development into a global pandemic, companies and governments have adopted exceptional measures to safeguard employees, customers, and the public. Some of these measures include the use of technology to enable remote workplaces, and to collect, process, and share personal information in new ways. Companies handling personally identifiable information, financial data, and/or health information must have in place robust cyber security protocols to limit the risk of data and privacy breaches. In addition, the method and type of data collected, how it is used to drive decisions, where it is stored, and for how long, are important considerations for data privacy during the pandemic and beyond.

What is data privacy and how has it evolved over time?

The right to privacy is a "fundamental human right" recognized in the United Nations Declaration of Human Rights, the International Covenant on Civil and Political Rights, and other international and regional treaties. Most countries recognize the right of privacy explicitly within their constitutions. While the definition varies, it may include the privacy of personal data or information (e.g., medical records); the protection of people's bodies (e.g., drug testing) and personal space (e.g., homes); and the privacy of our communications (e.g., mail, telephones). Data security aims to ensure that any personal information that is collected, used, or stored is protected from unauthorized use.

Over the past decade, governments and consumers have become increasingly concerned about data privacy and security, largely due to the rise of globalization, advancements in technology, the use of multimedia, and the evolution of business models that derive financial value from personal data.

Globalization

Globalization has expanded the flow of data, which can be collected, processed, and shared across borders in a matter of seconds, posing a challenge for regulators of privacy laws.

Technological advancement

Technology has increased the power, capacity, scope, and speed of data collection, processing, and sharing. Technological advancements such as the mobile phone, online payment platforms, biometric systems (e.g., voice and facial recognition), and geospatial data can all be used to collect and store personal data.

Multimedia

Personal information can be collected and stored in multiple forms, such as text, audio, images, animations, video and interactive content; these channels provide a wealth of personal data. As of 2019, there were approximately 5 billion mobile users and 3 billion social media users[1], and 4 million hours of video content was being uploaded every day.[2]

Business models

Collecting and processing personal data has become a significant driver of financial value in our economy. The business models of some of the most highly valued companies in the world depend upon their ability to provide targeted advertising based on users' personal data.

[1] Digital 2019: Global internet use accelerates, January 2019, We are Social and Hootsuite
[2] How much data is created on the internet each day, June 2019, MicroFocus

The increased focus on data privacy and security has ushered in a new generation of government regulations. For example, in 2016 the European Union (EU) approved the General Data Protection Regulation (GDPR), which applies to the collection of data from residents by firms inside or outside of Europe. The cost of non-compliance with privacy regulations and requirements can be steep. Companies found to be non-compliant with the GDPR, for example, can be fined up to EUR€20 million, or 4% of a company's annual turnover (whichever is higher).[3] Many companies have been fined in recent years for data privacy violations or breaches, including British Airways (EUR€205 million in 2019), Marriott International (EUR€110 million in 2019), and Google Inc. (EUR€50 million in 2019)[4] under the GDPR, as well as Facebook (USD$5 billion in 2019)[5], Google and its subsidiary YouTube (USD$170 million)[6] by the Federal Trade Commission (FTC).

How does COVID-19 impact data privacy?

The World Health Organization declared COVID-19 a global pandemic on March 11, 2020. Since then, companies and governments have taken unprecedented measures to help contain the virus and protect the population. This includes the use of technology to collect, use, and share data with the goal of limiting infections, establishing effective policies, and enabling vaccine research. Under these circumstances, the right balance needs to be struck between public health and safety and the need for data privacy and security.

Impacts from COVID-19

Collection and sharing of medical, health, and other personal data

Public health authorities may share medical information in order to coordinate their response to COVID-19. In some cases, employers must take action to ensure the health and safety of customers and employees by advising them of infected personnel. When taken, these actions must follow privacy laws and protect the right to privacy of those that are infected.

Tracking and monitoring of individuals' location and status

Governments and private companies are using technology to identify, track, and monitor the spread of COVID-19. For example:

- Chinese public transportation infrastructure is using facial recognition and infrared temperature cameras to identify commuters with fevers.[7]
- South Korea is using a tracking app to inform citizens when they are within 100 meters of an infected person. Information provided includes: the individual's infection date, nationality, gender, age and locations visited.
- Taiwan requires mandatory tracking of mobile phones for quarantined individuals.
- Spain launched a public health app where individuals report daily temperature.

Threats to data security from digitization of processes and practices, and increased risk of cyber-attacks

An increase in remote work and digitization raises risks to data privacy and security. These risks are amplified when new processes (e.g., video conferencing) are implemented quickly, without proper vetting, controls, or processes in place. Perpetrators of cyber-attacks may also seek to take advantage of entities focused on responding to the current crisis. The World Health Organization, for example, has reported a five-fold increase in cyber-attacks since the onset of the COVID-19 crisis.[8] Data security risks may be exacerbated by IT systems and workforces stretched to respond due to the pandemic.

Modification of laws related to data privacy and protection

Governments around the world have implemented emergencies acts, modified existing privacy acts, and issued specific guidance to enable the response to the COVID-19 pandemic. In the United States, the Health Insurance Portability and Accountability Act allows the government to waive privacy rules in case of a public health crisis. While modifications to privacy rights may be enacted through these (and other) legal means, it is not always clear what will happen once the crisis ends.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council, April 27, 2016, European Union Law
[4] GDPR Enforcement Tracker, tracked by CMS Law Tax, accessed April 28, 2020
[5] Facebook fined $5 billion by FTC, must update and adopt new privacy, security measures, July 24 2019, USA Today
[6] Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law, September 4 2019, Federal Trade Commission
[7] China rolls out facial recognition thermometers on buses amid coronavirus outbreak, February 2020, The Hill
[8] WHO reports fivefold increase in cyber attacks, urges vigilance, April 23, 2020, World Health Organization

How will data privacy and protection change as a result of COVID-19?

The COVID-19 pandemic has required governments and companies to adapt quickly to a rapidly evolving situation. While data and technology have an important role to play in helping companies and authorities identify, track, and monitor the spread of COVID-19, data privacy and security must remain important considerations. Once the immediate needs of the crisis have passed, companies and governments will need to:

Verify compliance with privacy laws: Data that may have been collected under emergencies acts, modified laws, or specific guidance related to COVID-19, will need to be identified and assessed to ensure that any ongoing collection, processing, or sharing of data is in compliance with all privacy laws.

Confirm individuals' consent and data rights: In cases where personal data will continue to be collected and/or held, companies and governments should ensure that consent is provided. While implicit consent or voluntary provision of data may have been adequate during the crisis under modified laws or requirements, explicit consent may be required moving forward, especially if the purpose for which the data is collected has changed.[9]

Verify data privacy and security: Technologies or processes, such as video conferencing, remote onboarding, or digital verifications, may have been implemented during the crisis without having gone through an organization's normal third-party risk-management process. Companies should ensure that any gaps in the verification process are filled to avoid potential non-compliance with privacy laws or security violations.

How can companies address data privacy?

A company's exposure to data privacy issues is largely a function of their business model, what data they collect, and how they process, store, and share that data. In order to effectively address data privacy and protect the security of data, a company should:

1. **Establish board oversight and accountability:** Companies should establish clear accountability and responsibilities for data information and security at a senior management and board level. The board, and/or responsible board committee, should receive regular updates on cyber security strategy and processes, and actively seek related expertise when appointing directors.
2. **Know and comply with all laws and regulations:** Companies should identify and monitor regulations in all relevant jurisdictions, and provide public disclosures committing to compliance with all laws. Both the volume and scope of data privacy and protection laws is increasing, as are the fines for non-compliance.
3. **Only collect necessary data:** Companies should collect the minimum amount of data required (data minimization) in order to achieve the purpose for which it is collected (proportionality). If additional information is not required, then it should not be collected.
4. **Understand and receive consent:** Collection of personal information should only be done with the individual's knowledge and consent, with very few exceptions. As such, consent for data collection and use should be built into processes and reviewed regularly.
5. **Implement robust data security management practices:** Any company that collects and uses personal information should have in place policies and practices to protect the data and guard against cyber-attacks. These should include incident management plans that cover both disaster recovery and business continuity, as well as audit processes that cover all operations and third-party providers.
6. **Build awareness of data privacy:** Employees that handle personal information should understand data privacy requirements, as should customers and third parties. Providing regular information and skills training on topics such as consent, protection of credentials, phishing, and cyber security can enhance a company's ability to manage related risks.

[9] COVID-19, Managing privacy and cyber issues, March 2020, McCarthyTetrault

At RBC Global Asset Management, we consider environmental, social, and governance factors to assess the exposure of companies to material ESG risks. The quality and effectiveness of a company's data privacy and security is one factor our investment teams consider in their ESG integration processes. This may include consideration of a company's data collection, use, consent, and monetization process; the strength of its privacy policies; managerial responsibility; privacy and security audits; staff training; reporting; and board oversight. We believe that being an active, engaged and responsible owner empowers us to enhance the long-term, risk-adjusted performance of our portfolios and is part of our fiduciary duty.

For more information, see Our approach to responsible investment.

(05/2020)
016GAM031_05-2020_ARTICLE_DATA_PRIVACY_SECURITY_EN_V1_5 05/06/2020