Lowenstein Sandler

Privacy & Cybersecurity

May 27, 2020

# Emerging From COVID-19: Data Privacy and Security in a Changed World

By Mary J. Hildebrand CIPP/US/E

As millions have moved their professional and personal lives online, in-person contact during the COVID-19 pandemic has become a memory except for "essential" public services. To receive medical care or an education, be entertained, conduct business, shop for essentials, and engage in online gaming, Americans have few options but to fill in the blanks with their personal information. Individuals, consumers, and business contacts are becoming acutely aware of the risks. Their oft-repeated concerns extend beyond traditional data breaches, identity theft, and/or misuse of sensitive information.

There is a strong sense that businesses are benefiting financially from the influx of personal information by expanding its use beyond providing the promised product or service to include the businesses' own commercial benefit. Governmental and regulatory authorities are taking note of public sentiment.

- The California Consumer Privacy Act (CCPA), which became effective on Jan. 1, requires disclosure of any financial incentives offered by businesses in exchange for personal information.
- The Dashboard Act, bipartisan legislation introduced last year in the U.S. Senate, sought to require major online platforms such as Facebook, Google, and Amazon to disclose the monetary value of personal information to their users, and would have authorized the SEC to develop data valuation methodologies for public companies.
- The New York Privacy Act, introduced for the second time in 2020, provides for a private right of action allowing "anyone injured" through violation of the law to file a lawsuit seeking damages.
- Despite intense pressure from businesses seeking to delay enforcement of the CCPA beyond July 1, the California Attorney General declined, and the California Legislature will soon be debating CCPA 2.0.
- Consumers have also filed suit against Zoom, alleging that a series of publicized security incidents violated the CCPA.

**Unprecedented Volume of Data.** While data is rocketing to the top of valuable assets—and data privacy concerns have hit the headlines—the nature and volume of personal information collected has escalated sharply during the COVID-19 pandemic. These disclosures are far broader than most consumers realize, because the once-reliable line between personal and nonpersonal information has largely been erased by the raft of new data protection laws. Among other data points, online identifiers (e.g., device ID, IP address, geolocation data, Ad-ID), biometric data (e.g., eye scans, photographs, fingerprints), business contacts (e.g., employees of your customers, suppliers, and service providers), and consumer profiles (e.g., reflecting the consumers' preferences, characteristics, psychological trends, predispositions, etc.) are deemed "personal information" protected to the same extent as Social Security numbers.

**Data Protection Laws.** Among industrialized nations, the U.S. is one of the few without a national law to protect the privacy and security of personal information. Comprehensive data protection laws in the EU, Canada, Singapore, Russia, and South Korea, for example, provide a reliable legal framework for data collection and commercialization efforts. U.S. states are moving rapidly to fill the void, with the CCPA becoming the first and most far-reaching data

protection law in the country. According to the National Conference of State Legislatures, over 150 consumer privacy bills were introduced in 25 states and Puerto Rico in 2019. Additionally, states have already passed privacy laws applicable to certain industries, such as insurance, education, health care, and financial services, and specific categories of data, such as biometric data.

Initially, many businesses viewed the new data protection laws purely as compliance challenges, and focused on policy modifications, training, and related functions. Nothing could be further from reality. As has now become clear, these laws also re**quire fundamental changes in businesses' data practices, and operate to restrict collection, disclosure, and commercial use of personal information across industries. Transparency regarding data collection and intended use is mandatory, and individuals have the right to control use of their personal information, including for commercial purposes. Any business without an enterprise-wide strategy to address data protection laws may find that its ability to leverage personal information and related data is severely constrained or nonexistent.** Moreover, even where individuals have consented or there exists another valid legal basis for processing the data, individuals may rescind their consent and/or direct that their personal information be deleted.

**As Trends Converge ...**

Headlines across the country reflect the convergence of these key trends.

- As businesses moved online and remote working became the norm, executives recognized that controlling security risks, without necessarily controlling the work environment, required new and creative solutions.
- The Department of Health and Human Services, Office of Civil Rights (OCR) responded to consumer concerns during the pandemic not by tightening data protection measures, but by relaxing enforcement of certain privacy and security standards applicable to protected health information. In weighing the value of enhanced availability of medical services during the pandemic against the risk of exposing protected health information, the OCR opted to encourage medical practitioners to provide online care.
- The COVID-19 pandemic has also sparked intense discussion on both sides of the Atlantic on the use of GPS data from smartphones to track individuals who have potentially been exposed to the novel coronavirus, and the legal and privacy implications of digital contact tracing apps.

We will be closely following developments, so please continue to check back for updates on digital contact tracing during the pandemic, new biometric data laws, and data monetization strategies.

**Conclusion**

U.S. businesses emerging from the stunning impact of the COVID-19 pandemic confront a radically changed landscape. Zoom, Skype, Webex, Netflix, Hulu, Instacart, Amazon, telehealth, telemedicine, and a host of other services are now integral to daily life. These services, and the commercial, social, and health needs they address, are critically dependent on the availability and accuracy of massive amounts of sensitive data and personal information. From startups to multinationals, the trend of viewing data as a separate and valuable asset has become reality across business sectors. **Now is the time for businesses to develop a sound strategy that complies with new and evolving data protection laws and maximizes the financial value of their data assets.**

***To see our prior alerts and other material related to the pandemic, please visit the Coronavirus/ COVID-19: Facts, Insights & Resources page of our website by clicking here.***

***About Us***
*In today's digital world, where data has become a key asset for conducting business, companies continue to face greater privacy and cybersecurity challenges. At Lowenstein Sandler, our Privacy & Cybersecurity team helps clients navigate the rapidly evolving, increasingly complex privacy and security law landscape in the United States, the EU, and around the world. We deliver innovative privacy and security solutions that meet our clients' critical business needs including the commercialization of data assets in a legally compliant manner. Our targeted counsel is relevant to companies across diverse industry sectors, and public and private companies from start-ups to global enterprises.*

# Contact

Please contact the listed attorney for further information on the matters discussed herein.

**MARY J. HILDEBRAND CIPP/US/E**
Partner
Chair, Privacy & Cybersecurity
**T: 973.597.6308**
mhildebrand@lowenstein.com



This Alert has been prepared by Lowenstein Sandler LLP to provide information on recent legal developments of interest to our readers. It is not intended to provide legal advice for a specific situation or to create an attorney-client relationship. Lowenstein Sandler assumes no responsibility to update the Alert based upon events subsequent to the date of its publication, such as new legislation, regulations and judicial decisions. You should consult with counsel to determine applicable legal requirements in a specific fact situation. Attorney Advertising.

© 2020 Lowenstein Sandler LLP | One Lowenstein Drive, Roseland, NJ 07068 | +1 973.597.2500