Lowenstein Sandler

Privacy & Cybersecurity

June 1, 2020

Contradictory Responses by Privacy Regulators Post-COVID-19: Balancing the Economy With Cybersecurity in a Changed World

By Mary J. Hildebrand CIPP/US/E, Edgar R. Hidalgo CIPP/US, and Carly S. Penner CIPP/US

What You Need To Know:

- **The CCPA is currently set to become enforceable on July 1. If your business is regulated by the CCPA, you have 30 days from publication of this alert to comply.**
- **Government authorities have pursued different, frequently contradictory, approaches to enforcing data privacy and cybersecurity regulations during the COVID-19 pandemic.**
- **It is imperative that you understand the data privacy and cybersecurity regulations applicable to your business and develop creative compliance programs that respect the integrity and security of personal information *and* maximize its value to your business.**
- **If the potential for new federal privacy legislation is realized, additional regulations will be forthcoming, including regulation of contact tracing programs to combat the COVID-19 pandemic.**

The COVID-19 pandemic has had a disparate effect on privacy regulators, with varying levels of enforcement advocated by different government entities; the California Attorney General, the U.S. Department of Health & Human Services (HHS), European data protection authorities, and other regulators have taken different, often contradictory, approaches to dealing with the competing interests of a struggling economy and the threat of increased privacy and cybersecurity violations. These contradictions are likely to persist, as competing privacy legislation was recently introduced in Congress to regulate the collection and use of personal information during the COVID-19 pandemic.

On the one hand, businesses struggling with the virus's economic impact are striving to allocate resources for maximum financial benefit, while on the other hand, risks to personal information and privacy rights have increased in a remote global workforce where phishing, malware, and other cyberattacks proliferate and the political pressure to collect and track medical information regarding COVID-19 infections mounts. With the seemingly competing interests of protecting the bottom line and a heightened threat to privacy, some privacy regulators are responding to these new realities by relaxing enforcement efforts, while others decline to do so in recognition of the heightened threats to privacy and information security.

Below is an update on how different regulators have responded regarding enforcement since the COVID-19 national emergency was declared.

The California Attorney General Remains Steadfast on the California Consumer Privacy Act

The California Attorney General has declared that despite the pandemic on top of already intense business pressure, it will not delay enforcement of the California Consumer Privacy Act (CCPA), which is set to begin on July 1st.

In late March, as the extent of the COVID-19 pandemic was becoming clear, a joint industry letter by advertising and adtech trade associations asked the Attorney General's office to delay enforcement of CCPA until 2021. The letter highlighted that "[t]he public health crisis brought on by COVID-19 juxtaposed with the quickly approaching enforcement date for the CCPA places business leaders in a difficult position. They are forced to consider trade-offs between decisions that are best for their employees and the world at-large and decisions that may help the organizations they lead avoid costly and resource intensive enforcement actions."

In an email to *Forbes* magazine, an advisor to the Attorney General responded, "Right now, we're committed to enforcing the law upon finalizing the rules or July 1, whichever comes first … "We're all mindful of the new reality created by COVID-19 and the heightened value of protecting consumers' privacy online that comes with it. We encourage businesses to be particularly mindful of data security in this time of emergency."

Meanwhile, as of the date of this client alert, the Attorney General's proposed regulations have yet to be finalized, having completed a third round of revisions and public commentary on March 27, 2020.

With only 30 days until the enforcement date, businesses subject to the CCPA should ensure that their CCPA compliance efforts remain on track. As a further incentive to ensure your compliance framework is in place, the California Privacy Rights Act (CPRA), commonly referred to as CCPA 2.0, has garnered enough signatures to appear on the November 2020 ballot. Among other measures, the CPRA would create a new enforcement agency, the California Privacy Protection Agency, expand data breach liability, and impose additional obligations on service providers, third parties, and contractors. In a nod to the business community, the CPRA would extent the current moratoriums on certain employee and business-to-business data from 2021 to 2023.

European Regulators Signal Flexibility

The European Data Protection Board (EDPB), an agency created under the General Data Protection Regulation, issued a statement on the processing of personal data in the context of COVID-19. The EDPB stated that even during this pandemic, data controllers and processors must ensure the lawful processing of personal data, but it also noted that an "emergency" might legitimize "the restriction of freedoms provided these restrictions are proportionate and limited to the emergency period."

The EDPB provided clarification on how public health authorities and employers can process personal data in the context of a pandemic, pointing to legal bases such as processing pursuant to a legal mandate of a public authority and compliance with health and safety obligations that are in the public interest.

The EDPB also issued two new guidelines: (1) Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak and (2) Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak. Guidelines 03/2020 allow health data to be processed for the purpose of scientific research with the consent of the data subject, as long as there is not a significant power imbalance, or without consent for the purpose of complying with national legislation. Guidelines 04/2020 discuss the use and collection of location data to map the spread of the virus and contact tracing for notification purposes. The guidelines provide that contact tracing applications should be voluntary, rely on proximity information regarding users rather than tracing individual movements, and grant preference to processing anonymized data where possible. The EDPB emphasized in its guidance that response to the crisis and protection of the right to privacy are not mutually exclusive.

Data protection authorities in nearly all EU member states and the United Kingdom have issued similar guidance on the processing and sharing of personal data related to COVID-19. Organizations should continue to monitor guidance issued by the EDPB, the United Kingdom, and national data protection authorities in the countries in which organizations have a presence.

Department of Health & Human Services Relaxes Enforcement of the Health Insurance Portability and Accountability Act

Perhaps the most critical response to the COVID-19 pandemic has been from the Office of Civil Rights in HHS, which is charged with the enforcement of the Health Insurance Portability and Accountability Act (HIPAA). Compounding the conflict between the conservation of resources to protect the bottom line and heightened privacy concerns in the crisis is a third element in play under HIPAA: the critical role of protecting the privacy and security of personal medical and health information as the crisis escalated.

While covered health care entities must continue to comply with the privacy and security rules under HIPAA, HHS has issued guidance and relied on its discretion to relax enforcement and

waive penalties for community-based testing sites, public health and health oversight activities conducted by business associates, disclosures made to law enforcement and first responders, and telehealth service providers. With the proliferation of telehealth services during the pandemic, it remains to be seen whether HHS will extend its policy of relaxed enforcement after the emergency has subsided.

Federal Trade Commission Warns of Increasing Threat

On May 19, the Federal Trade Commission (FTC) issued a public warning regarding scammers posing as contact tracers hired by state governments to obtain personal information such as Social Security numbers from unsuspecting individuals. A few days later, in coordination with the Federal Communications Commission, the FTC instructed service providers that enable robocalling to terminate services to any customers exploiting the pandemic to obtain sensitive information from individuals, threatening such providers with “serious consequences" for failure to comply. These recent statements by the FTC follow months of warnings of surging complaints since the beginning of the year (upward of 18,000 as of mid-April) related to the coronavirus and signals of increased enforcement activity by the agency.

Congress Proposes Competing COVID-19 Privacy Legislation

Reflecting the larger clash of interests, conflicting privacy legislation is currently pending in both houses of Congress. The COVID-19 Consumer Data Protection Act, introduced by Republican senators in May, seeks to regulate the collection and processing of personal health information, geolocation data, identifiers, and other data during the health emergency. Shortly thereafter, Democratic members of the House proposed the Public Health Emergency Privacy Act, which would broadly regulate “data linked or reasonably linkable to an individual or device, including data inferred or derived about an individual or device." Most notably, the House bill includes a private right of action (a right not included in the Senate bill). Despite their differences, the speed at which these bills were introduced underscores the urgent need to build public trust in contact tracing technologies while holding government and businesses accountable for how collected personal information is used. Congress has not yet succeeded in passing national privacy legislation. Nonetheless, given the current exigent circum-stances, if either of these bills is passed, it could form the basis for a future, more expansive general privacy legislation at the federal level.

We are closely monitoring developments with respect to data privacy and cybersecurity laws and regulations in response to the pandemic. Please stay tuned for future installments in our "Emerging From COVID-19: Data Privacy and Security in a Changed World" series. Our next release will examine the implications of digital contact tracing and the potential impact of recently introduced legislation in Congress.

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..

Contacts

Please contact the listed attorneys 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

EDGAR R. HIDALGO CIPP/US
Counsel
T: 973.422.6418
ehidalgo@lowenstein.com

CARLY S. PENNER CIPP/US
Associate
T: 973.597.2516
cpenner@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