Lowenstein Sandler

Privacy & Cybersecurity

June 22, 2020

Privacy Concerns Multiply as Digital Contact Tracing Spreads: U.S. Tech Industry Takes the Lead as Congress Fails to Act

By Mary J. Hildebrand CIPP/US/E

What You Need To Know:

- **Digital contact tracing (DCT) is a potential game changer in the COVID-19 pandemic. However, the sensitive personal information collected by DCT applications ("DCT apps") largely falls through the cracks of existing U.S. data protection laws.**
- **The California Consumer Privacy Act (CCPA) may be the only current legal model that encompasses the data privacy aspects of digital contact tracing. Any business regulated by the CCPA that intends to use DCT apps should carefully evaluate the potential impact of this law on its obligations to California residents, including notice, transparency, the purpose of collection, and consumer rights.**
- **As businesses across the country begin to reopen and DCT expands, the glaring absence of any national consensus on data protection is impossible to ignore.**
- **Organizations need to remain vigilant regarding evolving state, federal, and foreign laws that may impact one or more aspects of DCT apps and the information they collect.**
- **Meanwhile, the tech giants that develop these technologies have been tagged by state attorneys general to fill the regulatory void by monitoring and enforcing the privacy standards established by the tech companies themselves. *Is this the approach the U.S. wants to take?***

DCT is a Game Changer

As businesses and other organizations in the private sector cautiously open their doors in the wake of the pandemic, DCT enables more efficient tracing of infected employees and notification to those at-risk. DCT also offers public health authorities a potentially valuable tool to supplement (and perhaps eventually replace) traditional, labor-intensive contact tracing.

However, as reliance on DCT increases, serious concerns have been raised regarding the privacy and security of vast amounts of sensitive health information collected by DCT apps. Thus far, Congress has failed to achieve consensus on appropriate legislation, leaving the tech industry and government authorities to pursue their own ad hoc solutions to this challenge.

DCT Marketplace

A robust marketplace for DCT technology has emerged since the U.S. declared a national emergency in mid-March, with dozens of platforms and mobile apps available. The DCT technology platform jointly released by Apple and Google is among the most well-known. The Apple-Google platform provides a framework for development of contact tracing applications for iPhone and Android devices.
After DCT apps built on the Apple-Google

platform are downloaded, users may opt-in to notify health authorities of their positive COVID-19 test, and/or to receive notification of exposure to infected individuals. User data is stored on the device, and cannot be disclosed to third parties without user consent, which may be revoked at any time. The Apple-Google platform relies on Bluetooth technology, bars collection of GPS location data, and prohibits use of collected information for targeted advertising. These safeguards are intended to provide some measure of privacy to the sensitive information collected through DCT apps.

Legal Guidance

Despite numerous initiatives over the last decade, the U.S. lacks a comprehensive national data protection law. U.S. laws on data privacy and security are fragmented, with federal legislation focused on critical sectors such as healthcare and financial services, numerous different state laws including 50+ variations on data breach laws and remedies, and self-regulatory industry standards such as the Payment Card Industry Data Security Standard, and the Network Advertising Initiative.

Sensitive medical information collected through DCT apps largely falls through the cracks. The Health Insurance Protection and Portability Act (HIPAA), for example, is a federal law intended to protect medical information; however, HIPAA only applies to processing of 'protected health information' by healthcare providers and their business associates for specified purposes.

The California Consumer Privacy Act (CCPA), the first and most comprehensive data protection law in the U.S., became effective just months before the pandemic. Despite its breadth, CCPA actually *excludes* healthcare information covered by HIPAA, but *may* extend to other medical information. As a state law, CCPA is limited to for- profit entities, and only protects the personal information of California residents, their households, and devices. Sensitive medical information collected by public health authorities and other regulatory agencies is not protected by the CCPA.

State Attorneys General Take Action

According to state authorities around the country, the proliferation of DCT apps is a mixed blessing. On June 16th the attorneys general of nearly 40 U.S.states and territories sent a letter to the CEOs of Apple and Google praising their "focus on a privacy-centered notification tool," but expressing "strong concerns" about other DCT apps available (or soon to be available) on Google Play and the App Store. According to the state AGs, many of them fail to provide consumer privacy protections comparable to the Apple-Google offering. In fact, certain "free" DCT apps use GPS tracking, include ads, and are not affiliated with public health authorities or legitimate research institutions. Visitors to the app stores may not be equipped to distinguish among the DCT apps, putting their personal information at significant risk.

The state AGs requested that Apple and Google take affirmative steps to mitigate the threat of these DCT apps, including:

1. pre-screening all apps labeled or marketed as related to COVID-19 contact tracing or exposure notification *prior to release on their app stores* to ensure they are affiliated with public health authorities, or a U.S. hospital or university working with such public health authorities, and *removal of any such apps currently offered in the app stores that do not meet these standards*; and
2. removal of *all* COVID-19 related exposure notification and contact tracing apps from the app stores when the national public health emergency has ended, and provide the state AGs with written confirmation of such removal, or an explanation why removal of a particular app would impair the affiliated public health authorities.

Now that the state AGs have apparently designated Apple and Google to monitor their online stores for DCT apps that fail to meet privacy standards established by the Apple-Google platform, their CEOs could be forgiven for regretting their pro-privacy stance. Tech took the lead on privacy and state AGs now want tech to undertake enforcement, all without legislative oversight at any level. As we await a public response from Apple and Google, it's worth noting who the state AGs did *not* publicly request assistance from – the U.S. Congress.

Pending Congressional Legislation

Currently, there are three bills pending in Congress intended to regulate the privacy and security of contact tracing apps and the sensitive medical information they collect. In the last month or so, House Democrats and Senate Republicans announced competing proposals, and the Senate introduced a bipartisan bill referred to as the Exposure Notification Act (the "Act"). Taking into account the complexity of any negotiation and compromise on the partisan bills, passage of the bipartisan bill appears relatively more likely.

The Act incorporates several of the Apple-Google privacy measures such as opt-in consent for participation, affiliation (through operation or development) with public health authorities, and prohibitions on use of the medical information for any commercial purpose, including targeted advertising. Under the Act, the users would also have the right to delete their information, data breaches must be reported to users and the Federal Trade Commission, and individuals that decline to use the app cannot be barred from public places. Further, the Act requires operators to practice the principle of data minimization, which means that only the minimum amount of data necessary to accomplish the purpose of the app may be collected.

None of these bills is perfect or will satisfy all interested parties; however, U.S. consumers, the tech industry, and state authorities would welcome passage of federal legislation on this exceedingly important topic.

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