BCLP. Client Intelligent

Insights

US PRIVACY LAW AND CONTACT TRACING APPS: CONSIDERATIONS FOR MITIGATING RISK

Jul 06, 2020

SUMMARY

Contact Tracing Is Crucial: Contact tracing is the systematic identification of infected individuals and their relevant contacts. Along with rapid testing and targeted quarantines, contact tracing is an effective and crucial public health tool during a pandemic.

Digital Contact Tracing Has Privacy Concerns: An app for contact tracing may raise a number of data privacy concerns, including data breaches, the selling of data to third parties, or government surveillance beyond the scope of the pandemic.

Limitations of Contact Tracing Apps: While contact tracing apps could make contact tracing more effective, there are number of limitations, including uptake concerns, over- and under-inclusive data collection, and diagnostic test inaccuracies.

Recommendations: Due to the limited legal privacy protections surrounding tracing apps, user trust will be paramount. We have included several best practices that companies that plan to develop and/or use contact tracing apps may want to consider, such as user-friendly consent, purpose limitations and data deletion requirements, outside audits, and data minimization.

Introduction

Widespread testing, contact tracing, and quarantines are crucial to suppressing any infectious disease outbreak, especially before a vaccine or effective treatment is developed. If we want to effectively manage the current pandemic of SARS-CoV-2, the novel coronavirus responsible for COVID-19, public health authorities must have a way to know who is infected, and who infected persons have been in contact with, in order to quarantine accordingly. While each of these—testing, contact tracing, and quarantine—involve its own set of legal issues, this alert focuses on the data privacy issues raised by *digital* contact tracing.

Importantly, claims that arise out of or relate to COVID-19 testing—potentially including privacy claims associated with subsequent contact tracing—may be subject to liability immunity under the Public Readiness and Emergency Preparedness (PREP) Act. For more information on the PREP Act, see our Alert here. For information on some of the legal issues related to quarantines, see this Congressional Research Services Legal Sidebar.

Digital Contact Tracing

Contact tracing in theory is pretty simple: any person who has come into close contact with a person infected with SARS-CoV-2 for a prolonged period of time (i.e., within 6 feet for at least 15 minutes) is identified, notified of their status, and asked, or required, to quarantine for 14 days. In practice, however, it is a resource-intensive task—often involving a large number of personnel interviewing people for information about where they have been and who they have been in close contact with. Furthermore, given the shortcomings of human memory, there are typically gaps in the data obtained. Some research suggests that a very high percentage of contacts must be identified for contact tracing to reduce the spread of this virus. Effectively identifying such a large portion of a country's population by traditional contact tracing can be an expensive, time-consuming process that can still miss infected persons.

Digital contact tracing, then, may be a crucial supplement to traditional contact tracing. In this bid to make contact tracing faster, cheaper, and more accurate, several countries and companies around the world have developed, or are developing, contact tracing apps that will use a person's smartphone or other cellular device to identify who has potentially been exposed to an infected person. There are currently 80 contact tracing apps worldwide that have been developed to combat the spread of COVID-19. They largely track when two devices are in close contact with each other by using one of two methods—the GPS location of the devices or the devices' Bluetooth signals.

Not surprisingly, the idea of using cellular devices to track our movement and share health data with government authorities raises a number of privacy concerns. Countries and regions around the world are taking varied approaches to handling these privacy concerns.

For example, to ensure a consistent approach across EU Member States, the European Commission released guidance—so it is not legally binding—on April 17, that addresses contact tracing apps. The guidance recommendations include that apps be voluntary, that national health authorities be the data controllers, that individuals should be able to exercise their rights under the General Data Protection Regulation (GDPR) (e.g., rights to access, rectification, and deletion), and that the apps should be deactivated when the pandemic is sufficiently under control.

Singapore launched TraceTogether, a voluntary contact tracing app that uses a phone's Bluetooth signal to determine the distance between two users and the duration of an encounter. Data is stored on a user's phone and is only kept for 21 days. If a user tests positive for the virus, they can provide

the 21 days-worth of data to the Ministry of Health (MOH), allowing the MOH to more effectively contact trace.

While the majority of tracing apps around the world are voluntary, some are not. The most downloaded contact tracing app in the world, for example, is the Aarogya Setu app in India, with more than 50 million downloads—largely because India is the only democracy in the world making the app mandatory for a large portion of its population.

In the US, Google and Apple announced an unprecedented joint development of a contact tracing app. The project is divided into two phases. First, the companies will develop an application programming interface (API) that can be used by public health organizations to develop apps that will be able to carry out contact tracing. Next, Google and Apple plan to create their own software and provide an update for Android and iOS smartphone devices that will allow them to use the software.

From the get-go, the Google/Apple app was designed with privacy in mind. Instead of tracking users' locations via location data in order to track contact, for example, this app is designed to use the device's Bluetooth signal to ping nearby devices. This allows the app to track which other phones it has come into contact with without tracking where that contact occurred. In response to public comments, Google and Apple have since stated that they are increasing security and privacy in the app—by using better encryption, scrambling identifying information, and protecting any potentially identifiable information related to the device. They have also rebranded the app as an "exposure notification" system instead of a contact tracing app. Google and Apple have also promised to dismantle the system when the crisis ends, and the app is voluntary.

Limitations & Risks of Digital Contact Tracing

These apps can be an important supplement to traditional contact tracing but have a number of potential limitations and risks. First, and most importantly, contact tracing apps will only be effective if there is sufficient uptake. This would be a particular challenge in countries like the US that would surely prefer a voluntary app. An Oxford University study has suggested that at least 60 percent of a country's population would need to use an app for it to stop the spread of the virus. A recent survey by the Washington Post-University of Maryland shows that only roughly half of those Americans owning smartphones would be willing to use the Google/Apple tracking app, while stating that they would trust public health agencies or universities with the data. Unsurprisingly, the best predictor of whether someone is willing to use the app is their level of concern about the pandemic. Given these concerns, some have argued that any new federal legislation should mandate digital contact tracing, though, as we note below, this may run into a number of legal challenges, including constitutional issues.

Unfortunately, a lot of people in the US do not even have a device capable of running the app. Approximately 1 in 6 Americans do not own a smartphone, and smartphone ownership is

particularly low among the most at-risk groups—only half of respondents over 65 have a smartphone. Smartphone ownership rates are even lower for respondents over 75. To address this, some commentators have argued that Congress should pass another economic relief or stimulus bill that provides smartphones or smartwatches and mobile service to those in need for as long as data collection is necessary.

Even if there is sufficient uptake, digital contact tracing has additional limitations. For example, the apps may be both over- and under-inclusive because they could account for infected people on the other side of a wall or people that were wearing appropriate protective equipment, but also not account for surface contact or the effects of lingering aerosolized virus. Users might also have a false sense of security because they have not been pinged by the app and subsequently become less cautious. Other reasonable worries include the risks of data breaches, the selling of data to third parties, and government surveillance beyond the scope of the pandemic.

And finally, these apps are going to have limited utility until rapid—and accurate—testing is widely available, which is currently not the case in the US.

Potential Legal Issues & Considerations for Mitigating Risk

There is no overarching federal privacy law that specifically applies to digital contact tracing, though some have been proposed in Congress. Therefore, developers, employers, and public health authorities may be subject to any number of state and/or federal privacy laws. Which laws might apply very much depends on the context, including the jurisdiction, what data is being collected, and how that data is being used and stored. For example, state biometric privacy laws, like Illinois' Biometric Information Privacy Act (BIPA), should be carefully considered if biometric data—like temperature measurement with facial recognition—is collected because they can carry stiff statutory damages for collecting biometric data without informed consent. The California Consumer Privacy Act (CCPA) could require disclosure of this type of data collection and the purpose for the collection, but, like many laws, has carefully defined exceptions, including for medical information or scientific research. Other potential legal claims could be made under traditional privacy torts, and enforcement actions could be brought under the Health Insurance Portability and Accountability Act (HIPAA) if there's a Covered Entity or Business Associate involved. Because state laws commonly require the reporting of certain infectious diseases and subsequent contact tracing under their constitutional police power, states may be able to mandate digital contact tracing. However, federal attempts to do so may run into *Sibelius* problems. There may also be important Fourth Amendment issues to account for, which are discussed in a separate post. Rigorous privacy protections in this context are also crucial for the sake of user trust and to help promote adequate uptake, whether or not an app is mandatory.

Although each context will have to be evaluated carefully, the general considerations to mitigate legal risks will remain the same.

- To the extent apps are voluntary, developers, employers, and public health authorities might consider making apps opt-out instead of opt-in or using other kinds of incentives to promote uptake. Entities could also consider incorporating lessons from survey data on the data privacy preferences of the public when designing and implementing apps.
- Apps should strive for a user-friendly privacy policy that clearly explains what data is being collected and how it is being used and protected. Users could also be required to review the policy prior to the use of the app or watch a short, explanatory video. To ensure that data is collected, used, and protected only as disclosed in the privacy policy, regular audits by an outside entity may be desirable.
- Strong data security protections should be considered, including technical safeguards like encryption and anonymization and other administrative safeguards like access limitations. Agreements with health agencies or other entities that receive the data could be used to ensure adequate privacy and security measures when data is transferred.
- Developers, employers, and public health authorities may want to consider limiting the sale of data and only sharing data with state public health authorities and the Centers for Disease Control and Prevention (CDC) to the greatest extent possible.
- In addition to considering data retention and deletion requirements and purpose limitations, it may be advisable to have a clear exit plan that ensures data is not used for surveillance beyond the scope of the pandemic. For example, there could be a sunset clause in the program that requires it to end after infections drop below a certain rate or a certain percentage of the population has been vaccinated.

Note: You can view other thought leadership, guidance, and helpful information on our dedicated COVID-19 / Coronavirus resources page at https://www.bclplaw.com/en-GB/topics/covid-19/coronavirus-covid-19-resources.html.

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Samual A. Garner

Washington

sam.garner@bclplaw.com
+1 202 508 6039

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be "Attorney Advertising" under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP's principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.

© 2024 Bryan Cave Leighton Paisner LLP.