Privacy Considerations For COVID-19 Digital Contact Tracing

Article By
Deepali Doddi
McDermott Will & Emery
Of Digital Interest

Related Practices & Jurisdictions

- Communications, Media & Internet
- Corporate & Business Organizations
- Coronavirus News
- Labor & Employment
- Health Law & Managed Care
- All International

Tuesday, September 29, 2020

Contact tracing is a key tool in the global effort to mitigate the spread of Coronavirus (COVID-19). Digital contact tracing, however, presents significant data privacy risks. Generally, contract tracing refers to an effort by public health officials to identify individuals with whom a patient who has tested positive for an infectious disease has been in close proximity. Public health officials will inform these individuals that they were exposed to a contagious patient and encourage them to monitor their symptoms and quarantine for a period of time.

In response to COVID-19, governments around the world have explored using digital contact tracing, by which smartphone users download an application (app) to enable public health officials to track infected individuals’ contacts. In addition, private sector companies are exploring how digital technologies can be used for contact
tracing on employees as they reenter the workplace.

Types of Government Digital Contact Tracing

From a data privacy perspective, the most intrusive digital contact tracing has involved government surveillance of users’ movements and locations. For instance, the Chinese Government has assigned mandatory, colour-coded quick response (QR) codes to residents based on whether they self-report having COVID-19 symptoms, or coming into contact with confirmed or suspected cases in the last two weeks.

Residents who are assigned red QR codes are required to quarantine for 14 days, while those who receive green QR codes may move freely about their cities, as long as they scan their smartphone apps before gaining entry to public spaces, such as the subway, retail stores, places of employment and restaurants. If a resident is later confirmed to have COVID-19, public health authorities can use the scanned QR code data to identify all individuals who have come into contact with the infected resident.

Other governments have used smartphone geolocation data not only to facilitate contact tracing, but also to enforce quarantine orders. Hong Kong, for example, has required all visitors to self-quarantine for two weeks upon arrival, and to wear an electronic wristband linked to a smartphone app that relays their geographic coordinates to public health officials to alert them of any violations of quarantine.

Other governments have elected to use geolocation data in their digital contact tracing efforts, but have made the sharing of such data with government officials voluntary. New Zealand has encouraged residents to download the NZ COVID Tracer, a smartphone app that they can use to scan government QR code posters to “check in” at sites and create “digital diaries” of their daily movements, which are stored locally on users’ smartphones. If a user checks in at a site visited by an individual with a confirmed or suspected case of COVID-19, the user will receive a notification alert and a call from public health officials. The user may then voluntarily send their entire digital diary to public health officials for contact tracing purposes.

Other, less privacy-intrusive methods of contact tracing do not involve government collection or monitoring of location information at all. Several US states are piloting a digital contact tracing system that relies on Bluetooth technology, whereby app users’ smartphones exchange and record random Bluetooth keys transmitted by beacons when the users are in close proximity to one another. An infected user may voluntarily input a positive diagnosis into the app, which will then use the list of Bluetooth keys that were associated with the infected user to identify and notify others with whom the user’s smartphone had been in proximity.

Similarly, Singapore has created an app and wearable device to collect, encrypt and locally store Bluetooth proximity data on individuals’ devices, rather than in a centralised government database. The app enables users to voluntarily inform public health officials if they test positive for COVID-19. There have been concerns, however, that using Bluetooth technology does not generate results that are as accurate as those derived from precise geolocation data. Some apps that collect neither geolocation nor Bluetooth data are being used by public health officials to supplement manual contact tracing. The US state of Georgia, for instance, is piloting
an app that allows users to voluntarily submit information about their COVID-19 diagnoses and contacts, which government tracers can use as a starting point. DATA

Privacy Implications of Digital Contact Tracing

The data privacy implications of digital contact tracing are significant, as many methods involve the collection of both sensitive health and location information.

Transparency

The success of many digital contact tracing initiatives instituted by western governments depends on users’ willingness to participate. Consumer trust is critical for adoption by a sufficient number of users to render a contact tracing app effective. It is imperative that there is transparency regarding the types of information an app will collect, how long it will store such information, and the third parties who will have access to the information. Government agencies and private entities offering contact tracing apps should ensure that individuals receive adequate notice of their privacy and data security practices.

Centralisation v Decentralisation

Under a centralised approach to contact tracing, all Bluetooth, geolocation and diagnosis information is compiled in a central system. This is generally run by a public health authority but, in some cases, may be shared with or administered by a third-party technology provider.

Under a decentralised approach, however, geolocation or Bluetooth data is stored locally on users’ smartphones, unless the users decide to voluntarily transmit the information to the government agency or private company. The app enables each user’s smartphone to regularly check the locally stored data against a list of infected individuals’ anonymised identifiers to determine whether or not the user’s phone has recently been in proximity with an infected individual’s phone.

A decentralised approach may be more palatable for users from a privacy standpoint, because sensitive personal information is likely less susceptible to a cyber attack, unauthorised access or improper surveillance than if it was stored in a centralised repository. However, a centralised approach allows public health officials to monitor and promptly respond to all incoming information, which may make it a more effective contact tracing tool.

Data Minimisation

“Data minimisation” refers to the core data privacy tenet that an entity should neither collect nor maintain more information about an individual than is necessary to accomplish the purpose for which it is being collected. A contact tracing app that continues to collect users’ geolocation information in the post-pandemic era, for example, would run afoul of this principle.

To comply with it, government agencies and companies should cease collecting app users’ information and delete any stored contact tracing information once it is no
longer needed for COVID-19 mitigation efforts, to comply with legal requirements, or for another appropriate purpose.

**Bluetooth Data Linkage Issues**

Bluetooth-based contact tracing apps typically collect only a random Bluetooth identifier from a COVID-19-positive user who inputs his or her diagnosis. It may, however, be possible for a government agency or private company to link metadata associated with the infected user’s Bluetooth identifier, such as the user’s smartphone IP address, to the user’s identity and location.

**Workplace Surveillance**

Companies seeking to use digital contact tracing in the workplace may encounter barriers in the form of employee surveillance laws. Because contact tracing apps may track an employee’s physical location not only when onsite, but also when the employee is off-duty, the app may be considered a form of surveillance that may be regulated by employment or data protection laws.

**Efforts to Regulate Digital Contact Tracing**

In the United States, federal lawmakers have introduced several bills intended to protect the privacy of COVID-19 personal data. Senate Republicans have proposed the COVID-19 Consumer Data Protection Act, which would impose notice and consent requirements on regulated entities that collect geolocation data, proximity data, and health information related to COVID-19 under certain circumstances. Senate Democrats have proposed a bill to create a Coronavirus Containment Corps, which would require the US Centers for Disease Control and Prevention to collaborate with state and local governments to develop a national contact tracing strategy that ensures privacy protections for COVID-19 patients. At the time of going to press, neither bill has advanced beyond these proposals.

European privacy regulators have also issued guidance on privacy considerations and risks associated with contact tracing. For example, the UK Information Commissioner’s Office published guidance on “data protection expectations” for COVID-19 contact tracing app development, emphasising principles of transparency, data minimisation, and the use of pseudonymised identifiers when possible. Likewise, the French Commission nationale de l’informatique et des libertés issued an emergency opinion on the French Government’s implementation of a national contact tracing app, including recommendations for enhancing users’ privacy protections.

© 2022 McDermott Will & Emery

National Law Review, Volume X, Number 273

digital-contact-tracing