

Contact Tracing: Privacy Implications and Practical Considerations

Almost as soon as COVID-19 began ravaging the world, countries turned their hopes to mobile apps as a weapon to fight against it. Contact tracing was quickly recognized as a potential tool to monitor, and possibly contain, the spread of the virus. The ubiquitous presence of cell phones and their capacity to record and transmit data offered a perfect application to track the risk of potential transmissions of the novel coronavirus. However, the potentially intrusive nature of cell phone tracing raised a myriad of privacy concerns.

Background

The tech industry rapidly developed COVID-19 apps and technologies as early as March 2020. Within weeks products hit the market. The quick turnaround time, however came at a cost. Many products became available without fully assessing possible unintended consequences. First to market trumped adequate time for fulsome review. One of the overriding concerns surrounding the new technology is its actual effectiveness. The technology only functions properly if test results are promptly available and it is deployed nearly as ubiquitous as cell phones themselves (click [here](#)). However, achieving a widespread user base and delays in test results have proven to be a significant challenge – particularly in the United States.

Compounding the challenge, the United States in particular has not adopted a singular approach to containing COVID-19, and that hurdle extends to the manner in which different jurisdictions utilize these mobile tracing apps. The lack of a uniform federal standard has resulted in a patchwork of technological approaches, with various states utilizing GPS-based apps, Bluetooth proximity apps, a combination of the two, or no apps at all. Most importantly, any use of tracking apps is voluntary. Users may choose to share their information, or not, which inherently limits the efficacy of any contract-tracing application.

Five states have implemented GPS tracking apps, (with one already subsequently abandoning the program) (click [here](#) and [here](#)). Three of the others have not seen any

Related Capabilities

- Privacy & Social Media
- Technology
- Labor & Employment

meaningful results; one — Rhode Island — has had limited success. Meanwhile, as many as eighteen states have acknowledged that they are not currently developing or planning to develop a contact-tracing app.

On the flip side, centralized contact tracing is not without its own concerns. The centralized model gathers data and reports it to a remote server, often controlled by public health authorities, which then generates matches to potential contacts (click [here](#)). This approach was initially embraced by France, Italy and the U.K., amongst other countries although some have since switched to a decentralized approach citing to privacy concerns. Norway's Smittestopp app was criticized as a mass government surveillance tool since it provided a central server with near-live tracking of the users' location by consistently uploading the GPS coordinates (click [here](#)). Norway has since abandoned the centralized approach. India's approach also has the potential for continued surveillance following the pandemic, as it includes Bluetooth tracking, but it also assigns risk levels to users, offers telemedicine and diagnostic services all in one location. The app, which is "voluntary," is actually required by government employees and some private employers and landlords have mandated its use (click [here](#)). Coupled with the lack of transparency regarding the developers of the application it is unclear how the data may be used in the future.

Current Status

In general, Americans have been hesitant to download contact tracing especially if the apps track their location. For example, Apple and Google's joint API has the capacity to support apps on nearly a hundred percent of cell phones *in the world*. Yet only a handful of states have plans to build apps based on the Apple-Google API. *None of them* have actually released an app yet.

It remains unclear whether the general public is willing to trade privacy for public interest through the use of these kinds of applications. Intentionally or not, contact tracing apps provide significant data about how the infected individual might be identified and have the capacity to gather a great deal of additional personal data. When an individual is diagnosed with COVID-19, public health officials may be able to retrace their steps in order to notify exposed persons. In theory, this should not require the disclosure of the individual potentially infected. But it does not require a stretch of the imagination to project how that person might be identified.

Public health officials have always played an important role in exposure notification for communicable disease, but some of the apps, especially early iterations, do not appear to carefully balance the rewards and risks. For example, South Dakota's contact-tracing app was apparently inadvertently sending personal identifying information to Google and Foursquare, despite claiming not to share any such data (click [here](#)).

Given that we are still experiencing the first wave of coronavirus, and a vaccine is at best months away from market, the pressure to track the spread will continue, especially as society attempts to find safe ways to reopen. We can expect to see continued refinement in the use of both voluntary and mandatory schemes, with several initiatives in contact

tracing being discussed at institutions of higher-education as they attempt to reopen. The challenge of striking the proper balance between the need for contact tracing information for the public good, versus the privacy compromises invariably associated with these apps, will continue to offer a fascinating social experiment. How should the public's 'need to know' their exposure to past and current infected individuals be weighed against an individual's interest in maintaining personal privacy about their own health conditions? We will continue to assess, and advise, on important developments in this space.