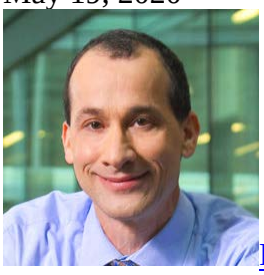
Illusions of consent and COVID-19-tracking apps

May 19, 2020


Paul Schwartz

COVID-19-tracking apps help identify parties with whom a COVID-19-infected person had contact. The apps do so by drawing on information about the location of a person's mobile phone and its proximity to other devices. Experts, including the Bloomberg School of Public Health at John Hopkins University, view this technology as a necessary boost to manual contract tracing by public health officials.

Countries are currently split into those where the government requires the use of these apps and those that do not. Mandatory contact-tracking apps are in use in China, India and Turkey. The rest of the world is following the voluntary route. Nations in this camp include Australia, Austria, Finland, Germany, Ireland, Israel, the Netherlands and the United Kingdom.

In the United States, however, the question is not whether the government is going to require the population to download an app to monitor their movement and contacts. No one is proposing that approach. Rather, the critical issue is how the government and private sector will restrict access to spaces and opportunities based on whether or not one "consents" to the use of an app or other monitoring device.

For example, an employer may block entry to a workplace unless an individual has an app on his phone that uses Bluetooth to track location or copies a QVC code at a building's entrance into an app. The future may be one of "no app, no entry" or even "no app, no job."

The future may be one of "no app, no entry" or even "no app, no job."

In these situations, reliance on consent is illusory. Even though the use of the app is voluntary, in the sense of not being government-imposed, its use is part of a take-it-or-leave-it situation.

In many areas of information privacy law, we've already been down the path of justifying monitoring through the fiction of consent. For example, "notice-and-choice" is frequently used to justify email monitoring at work; employers inform employees in advance of their policy and the use of a workplace email system is then considered to represent consent to the policy. A similar approach is taken by workplaces that require keycards to enter office spaces. In the employee handbook, a company tells folks about how the keycard collects data. It then distributes the keycards and mandates their use and, presto, consent is granted each time an employee swipes the device at an entryway.

Instead of falling back on illusions of consent, the privacy challenges of COVID-19-tracking apps require a federal law. Fortunately, there are now two proposals for such a law before the Senate. Before examining the two bills, however, it makes sense to think through first principles.

How should such a law proceed?

Any regulation of a COVID-19-tracking app should be pragmatic and proportionate. It should reflect that public health during a pandemic is a priority. As the Supreme Court stated in Jacobson v. Massachusetts (1905), "the social compact" requires that "all shall be governed by certain laws for 'the common good,'" including by laws for the protection and safety of the population. Finally, regulation should be attentive to the use of these devices in workplaces because this context will be particularly prone to illusions of consent for COVID-19 data collection.

As for the two competing federal bills, both have pluses and share many areas of agreement. The first bill is the COVID-19 Consumer Data Protection Act, a proposal introduced by five senators led by Sen. Roger Wicker, R-Miss. The second bill is the Public Health Emergency Privacy Act, from Sens. Richard Blumenthal, D-Conn., and Mark Warner, D-Va.

The good news first about both bills. Both agree on the need for data minimization, which means collection of the least amount of information. Further, the proposed statutes mandate data security, which is important as any information collected by these apps will be a target of interest for hackers, domestic and international.

The bills also heighten transparency. They do so by mandating information to the affected party at the point of collection and by requiring public information. For example, the Wicker bill requires "transparency reports to the public under which companies will describe their data collection activities relating to COVID-19." In addition to requiring regulated entities to issue public reports, the Blumenthal-Warner bill calls for the secretary of Health and Human Services to consult with the Federal Trade Commission and Commission on Civil Rights in reporting on the "civil rights impact of the collection, use, and disclosure of health information in response to the COVID-19 public health emergency." These approaches have merit and should be incorporated in a consolidated bill.

Finally, both bills include an exit strategy and enforcement mechanisms. Mandated deletion periods guard against the phenomena, identified by Northeastern University's Woodrow Hartzog, of "surveillance inertia." Regarding enforcement, the Wicker bill would grant the FTC

and state attorneys general enforcement power. The Blumenthal-Warner bill goes further and provides private rights of action.

Even without a crystal ball, one can predict significant controversy around this issue. The need will be to find a sensible compromise that allows the enactment of a COVID-19 privacy law.

Now for one major difference: The Wicker bill contains an exclusion for the workplace. This exception covers "employee screening data," which covers data relating "to the COVID-19 public health emergency" and for use in determining "whether the individual is permitted to enter a physical site of operation of the covered entity." The general idea behind such exclusion is, in my view, sensible. It will allow employees to keep their workplace safe, including by excluding infected employees from the place of employment.

If there is to be a workplace exclusion, however, the law must set strong legal restrictions on the scope of data collection and the substantive uses to be made of personal information. And here the Blumenthal-Warner bill shines. It avoids "illusions of consent" by calling for the collection, use or disclosure of only such data that is "necessary, proportionate, and limited for a good faith public health purpose." It also details a long list of prohibited uses of emergency health data, including for commercial advertising, soliciting or selling services in a discriminatory fashion, or engaging in discrimination in any place of public accommodation.

In addition, a revised bill should have additional strong protections to keep a workplace app from being used for tracking outside of the office or factory. COVID-19-tracking apps should be restricted to the place of employment and to contacts with others in the workplace. Moreover, the law should require that an employer delete all collected data after a set period of time, such as three weeks.

As a final note, the use of COVID-19-tracking apps can only contribute to ending the current emergency as part of a larger governmental response to the pandemic. The paramount needs to begin with a robust system for testing and tracing. There is also an urgent requirement for the creation of quarantine spaces for infected individuals who lack such safe environments. There must also be strong legal protections for people with the virus, including the creation of greater unemployment protections without which there will only be disincentives for individuals to seek out testing.

We are running a marathon and not a sprint, and the current crisis requires a pragmatic and proportionate response that sets legal limits on data collection and the subsequent use of collected data. COVID-19-tracking apps will be here soon, they won't be truly voluntary, and the law should carefully regulate their use as part of a larger public health response.

Photo by Pathum Danthanarayana on Unsplash

https://iapp.org/news/a/illusions-of-consent-and-covid-tracking-apps/