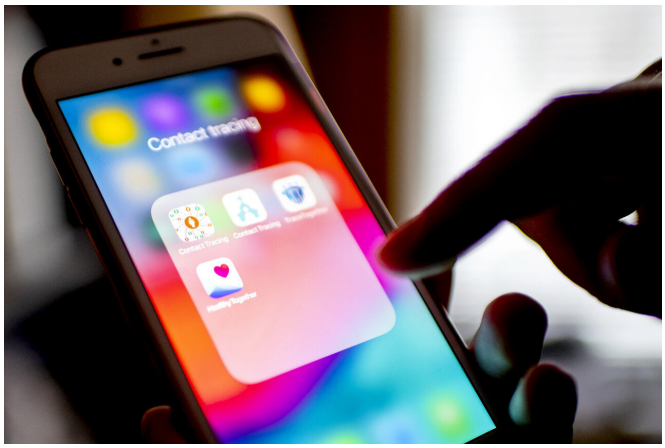
Will contact-tracing apps infringe on data privacy? Germany may soon find out.

1 May 2020, by Andrew Curry



Contact-tracing apps, which would make use of ubiquitous smartphones to monitor and manage the disease, are high on the list of measures government officials are considering to mitigate the spread of SARS-CoV-2, the virus that causes COVID-19. Credit: Ruby Wallau/Northeastern University

To help societies around the world control the spread of COVID-19 and get schools and businesses up and running, health officials are considering a range of technological solutions. Contact-tracing apps, which would make use of ubiquitous smartphones to monitor and manage the disease, are high on the list here as Germany begins to lift isolation orders this week.

With pressure and expectations high, government officials and privacy advocates spent the weekend battling over how such an app will work and how it will protect personal information.

On Friday, officials announced they were backing a system that would store contacts on a central server accessible to public health officials over a competing approach developed by Google and Apple. "This belief that data would be better guarded by Apple and Google, that it is better protected by American corporations than by government servers in Germany—I just don't get it sometimes," German Health Minister Jens Spahn said in an interview with the TV channel ZDF on Friday.

The discussions in Berlin are part of a wider European effort to roll out apps to help automate tracking of new COVID-19 cases. After weeks of testing, the German government announced late last week its preferred app could be ready to unveil within a week or two. Meanwhile, Austria's Red Cross recently rolled out its own "Stop Corona" app, and Britain, Germany, France, and the Netherlands are among the other European countries racing to develop their own apps.

"It's absolutely a way to leverage the technology in phones in a way that will benefit public health," says Northeastern University law professor Woodrow Hartzog, who specializes in privacy and data protection law.

But privacy activists warn that the apps—and the personal information they collect—could be abused. Addressing such concerns, Hartzog says, is critical to making contact-tracing apps a success. "If we don't do it right, we risk dampening people's willingness to engage," he says. "The pandemic's not going to last forever, but the data that's collected from the pandemic might. Until they feel protected, people are going to be reluctant to participate and share—and rightfully so."

Such apps have already been used in some regions in Asia to control outbreaks there. In Hong Kong and South Korea, for example, authorities have used cell phone GPS location data to track people and digitally enforce quarantine orders. When someone tests positive for SARS-CoV-2, the virus that causes COVID-19, stored location data can be used to reach out to anyone they might have infected and ask them to quarantine.

Hartzog argues that Europe is starting in a strong position: Privacy and data protection are treated as human rights in Europe, where regulations restricting the way businesses collect and store personal data have been in place for years. Perhaps the best-known may be the General Data Protection Regulation, or GDPR, which lays out how businesses all across the 27-nation European Union are supposed to treat personal information and puts a premium on personal privacy and user control.

Rather than tracking physical location using GPS, the European approach would rely on Bluetooth connections between mobile devices. When two phones sense each others' Bluetooth signals—as you sat on a bus or squeezed by someone in the supermarket aisle, for example—the contact would be logged by an app that mobile phone users could voluntarily download and install.

If someone using the app later tested positive for SARS-CoV-2, the app could automatically notify anyone who had been near that person in the past few weeks and urge them to self-quarantine.

But to succeed, the apps will require people to voluntarily share personal information, including a rough approximation of their whereabouts and their health status. Not unlike vaccines, apps need to be used by at least half of a country's total population to be effective, according to a recent study published by a team of researchers at Oxford University. That means app developers and public health officials have to convince a wary European public that the apps won't violate their privacy. "None of this works unless we trust the rules and the tools," says Hartzog.

Activists are already voicing objections: On Monday, more than 300 researchers from 26 countries published a letter criticizing the approach supported by the German government, which would store contact tracing data on a central server rather than on individual phones. "We are concerned that some 'solutions' to the crisis may, via mission creep, result in systems which would allow unprecedented surveillance of society at large," the letter says.

Privacy advocates in Germany are backing the approach behind the Google-Apple partnership, which would store logs of Bluetooth contacts on individual phones rather than central servers.

Whichever platform Germany picks in the end, its robust, heavily regulated approach to privacy and data protection may nonetheless work to its advantage. In Germany, traditionally a country where people are particularly sensitive about data privacy, data protection has been on the table from the outset—in an interview in early April, Spahn said any app would have to conform to existing data protection regulations. "We need to be as perfect as possible when it comes to data security and protection," he told the ARD TV channel.

Recent polls show more than half of the country would be willing to use a tracking app if it meant lifting social distancing restrictions. In the U.K., a Financial Times poll suggests almost two-thirds of adults supported the idea. "Germany and everyone else in Europe are in a better position not just because the GDPR is the most robust framework in the world but because privacy and data protection are treated as human rights," Hartzog says.

Would enough people volunteer to use such an app in the U.S., home to both Silicon Valley and the world's highest number of COVID-19 cases? Hartzog has his doubts: Americans, he says, are likely to be hesitant to sign up unless laws are put in place to ensure the tools they are being asked to use and companies and government agencies requesting their data remain trustworthy.

According to Hartzog, U.S. law too often relies on informed consent to justify data collection and use. That's the thinking behind the "agree" buttons you've probably clicked by the dozens while making your way across the internet—each one backed by small print giving companies the right to use your data however they see fit once you consent to their terms.

"My fear is that app developers will over-rely on the concept of informed consent to enable these tools," Hartzog says. "Consent at scale to justify data practices is a farce: I study these things for a living, and I can't press 'I agree' fast enough."

Particularly in the midst of a pandemic, agreeing to use a contact-tracing app hardly constitutes the gold standard for consent. "It's not really a meaningful choice, especially in these times when people are so scared and desperate and want to help," Hartzog says. "The standard notice-and-choice approach to protecting people's privacy is only going to make people more vulnerable and will be self-defeating. It won't encourage trust. People will be—rightfully—skeptical of sharing."

That's why as contact-tracing apps are rushed to phones across the world it's important to make sure privacy is baked into both the apps and the laws behind them.

"The key is going to be not only making sure the specifics of these apps are serving both privacy and the public," he says, "but also ensuring there are adequate rules in place to protect people who are being asked to trust both technology companies and the government with their data, freedom and well-being."

Provided by Northeastern University