The Washington Post
Democracy Dies in Darkness

One of the first contact-tracing apps violates its own privacy policy

North and South Dakota’s Care19 coronavirus app sends users’ location data to more than just the government

By **Geoffrey A. Fowler**

May 21, 2020 at 3:45 p.m. CDT

As governments build coronavirus-tracking smartphone technology, who is making sure their apps live up to privacy promises?

A new analysis of one of the first of a handful of U.S. contact-tracing apps, North and South Dakota’s Care19, finds it violates its own privacy policy by sharing citizen location and other personal data with an outside company. The review was published Thursday by privacy software maker Jumbo.

The oversight suggests that state officials and Apple, both of which were responsible for vetting the app before it became available April 7, were asleep at the wheel. Americans are especially wary of location and health data, and privacy violations of any degree will hamper efforts to use smartphones both to trace-contact and to provide exposure notifications.

The states turned to North Dakota app maker ProudCrowd to make Care19 for free. ProudCrowd confirmed to me that some data from its iPhone app goes to Foursquare, a prominent location-data provider for marketers — but says it isn't used for commercial purposes. (The Google Android version of Care19 also uses Foursquare, but does it in a way that obscures the data, ProudCrowd said.) Still, ProudCrowd says it plans to change Care19's privacy policy and will share less data in the future.

"Should this have been vetted? Yes. We are following up on that as we speak," said Vern Dosch, the state of North Dakota's contact-tracing facilitator. "We know that people are very sensitive." Health officials in South Dakota did not immediately reply to requests for comment.

Apple said it was investigating the report and that if it finds an app is out of compliance, it works with the developer to get it into compliance.

Foursquare does “not use the data in any way and it is promptly discarded,” said spokeswoman Jennifer Yu.

Health authorities are moving fast to build coronavirus apps, often with limited technical resources. They’re relying on commercial tracking companies and murky privacy protections — and under those conditions, it’s not clear we should trust them.

The Care19 app is upfront that its main purpose is voluntarily collecting citizen location data. (It’s different from a new set of apps that use Bluetooth technology from Apple and Google to provide anonymous exposure alerts without collecting location data.) Care19 calls itself a “digital diary” to help people remember where they’ve been over the previous 14 days so they can retrace their steps, and the people they’ve been in contact with, should they contract covid-19.

If users do test positive, the app lets them volunteer to share their location data with the state’s Department of Health to assist in its efforts to slow the spread of the virus.

But Care19’s privacy policy says the location data is “private to you” and is “stored securely” on servers belonging to ProudCrowd. Location “will not be shared with anyone including government entities or third parties,” it says.

That’s where the privacy review by Jumbo finds the app falls short. Tracing the flow of data from the app, it found Care19 sends data to Foursquare including a citizen’s location, his advertising identifier (a unique code representing a specific phone) and the unique “citizen code” generated by the app.

Care19’s maker, Tim Brookins of ProudCrowd, told me the app uses a Foursquare service called Pilgrim SDK to convert the location data it collects as latitude and longitude into the names of recognizable places.

“The Care19 application user interface clearly calls out the usage of Foursquare on our ‘Nearby Places’ screen, per the terms of our Foursquare agreement,” Brookins wrote in an email. “We will be working with our state partners to be more explicit in our privacy policy.” (He also said it would clarify privacy policy language about how it shares data to conduct diagnostics.)

Brookins said that in the future, his app would stop sharing the citizen code with Foursquare. “It is important to note that our agreement with Foursquare does not allow them to collect Care19 data or use it in any form, beyond simply determining nearby businesses and returning that to us,” he said.

Foursquare does “not financially benefit from free users like Care19,” said its spokeswoman Yu. “Essentially, any data we might receive is immediately discarded."

Foursquare does have a significant business in marketing tech. Other apps that use the Pilgrim SDK employ it to help them send targeted notifications and put users into marketing audience segments based on where they go, such as “fitness fanatic” and “beauty enthusiast.”

The good news, said Jumbo CEO Pierre Valade, is that Apple and Google have more explicit rules for the new category of virus-tracking apps that use special access to a phone’s Bluetooth signals to help anonymously notify people they may have been exposed to people who have covid-19. The rules for these “exposure” apps say they’re not allowed to collect any location data or the user’s advertising identifier.

Brookins says he's making a second version of the Care19 app that will do exposure notification and comply with Apple and Google's rules.

The bad news is that the Care19 oversight exposes an all-too-common privacy hole in apps: They contain code from hidden, third-party tracking companies. In a study of the data flowing out of my own iPhone, I encountered over 5,400 trackers in a single week. Some of them were even gathering personal information while I was asleep and my phone's screen was turned off.

Third-party software makes it easier for app companies to code quickly. But it also often feeds the personal data economy, used to target us for marketing and political messaging.

And when it comes to highly sensitive contact-tracing apps, the privacy bar should be set even higher. As governments develop these apps, they're going to need the resources to develop their own technology that doesn't rely on commercial surveillance companies — or more help from Apple and Google.

Last week, a group of Democrats in the House and Senate introduced the Public Health Emergency Privacy Act, which includes new provisions for enforcing the use of citizen data in apps to fight the coronavirus.

Sen. Maria Cantwell (D-Wash.), the top Democrat on a key tech-focused committee in Congress, said apps need strong privacy protections in the fight against the coronavirus.

"If it doesn't have a strong privacy framework, it will undermine consumer confidence," Cantwell said.

Tony Romm contributed to this report.

The secret life of your data: What you need to know

Updated March 6, 2020

For all the good we get from technology, it can also take a lot from us. The Washington Post tech columnist Geoffrey A. Fowler examines the personal information streaming out of devices and services we take for granted.

iPhones and Android phones: Hidden trackers in apps share personal information — even while you and your phone are asleep.

Alexa: By default, Amazon keeps a copy of everything Echo smart speakers record.

Credit cards: A half-dozen kinds of companies can grab data about purchases, from your bank to the store where you're shopping.

TVs: Once every few minutes, smart TVs beam out a snapshot of what's on your screen.

Cars: Automakers use hundreds of sensors and an always-on Internet connection to record where you go and how you drive.

Web browsers: Google's Chrome loaded more than 11,000 tracker cookies into our browser — in a single week.

Browser extensions: Add-ons and plug-ins can see and share everything you do on the Web.

Don't sell my data: The California Consumer Privacy Act (CCPA) can help even residents of other states see and delete their data — and tell companies to stop selling it.

Got a question about data privacy? Ask us.

Geoffrey Fowler

Geoffrey A. Fowler is The Washington Post’s technology columnist based in San Francisco. He joined The Post in 2017 after 16 years with the Wall Street Journal writing about consumer technology, Silicon Valley, national affairs and China. Follow