SQUIRE PATTON BOGGS

# Insight: Battling COVID-19—Are Privacy Considerations Collateral Damage?

April 16, 2020



The federal government is planning partnerships with social media and telecommunications providers to use geo-tracking information on social distancing to help prevent the spread of Covid-19. Squire Patton Boggs' Shalin Sood looks at the privacy issues inherent with this and asks how this information might be used in a post-Covid-19 world.

In an attempt to halt the spread of Covid-19 and enforce social-distancing practices, the U.S. government is reaching out to various companies in the private sector, including social media companies and telecommunications providers, to use app-enabled geolocation features, facial recognition solutions, and other technology.

The government hopes this information will provide a better understanding of how the virus is spreading globally and whether individuals are practicing appropriate social distancing measures. Unsurprisingly, a variety of privacy considerations have arisen as a result of this information-sharing between the public and private sector.

The Centers for Disease Control and Prevention is working with Palantir and Google, among others, to model the spread of the virus using data scraped from public social media. A task force has also been developed that is working in conjunction with the government, and includes several companies from the technology sector.

Data analytics company Palantir is working with the CDC to track Covid-19 through the use of data mapping and integration. The CDC previously worked with Palantir during the 2010 cholera outbreak in Haiti to monitor communications within the populace and track the spread of the disease.

Similarly, the facial-recognition firm Clearview AI may potentially collaborate with state authorities to use facial-recognition technology to track infected individuals. Clearview reportedly developed its facial recognition algorithm using approximately 3 billion images scraped without permission from various websites. The company hopes to contribute to a greater understanding of "contact tracing," the term given to the practice of identifying individuals with whom infected individuals may have been in contact.

## Cell Phone Information

The government is also in active talks with technology companies about using location data gleaned from cell phones to track the proliferation of the virus and to track whether Americans are adhering to social distancing protocols.

As currently developed, the plan would involve the technology companies sending collected anonymous and aggregated geolocation and facial recognition data from their apps to the federal government as a means to map the presence of the virus.

At this time, Google has indicated that the plan would not involve sharing an individual's movement or individual location. The data could be used to demonstrate the impact of social distancing and spread of Covid-19, similar to the way Google is able to show store traffic or traffic patterns.

The assumption is that the spikes in aggregated geolocation data could help the government track Covid-19, while detecting, disrupting, and discouraging gatherings that could result in a dramatic transmission of the virus between infected and non-infected populations.

As a part of the $2 trillion stimulus bill that President Trump recently signed into law, the CDC will receive $500 million for public health data surveillance and modernizing analytics infrastructure.

While it is not clear what the surveillance system will look like, the CDC must report on the development of the system within the next month. Based on previous reports, ostensibly the CDC will be aggregating anonymized data from its partnerships with the aforementioned technology companies and smartphone applications to track and monitor movement patterns.

The use of this data seemingly pushes the bounds of U.S. privacy laws. The data likely is not being used in a manner that has been clearly communicated to users and many obvious questions have yet to be answered:

- What information is being shared with the task force?
- How is the information being kept secure?
- What conditions are being placed on the use of this data?
- What are the processes and procedures in place for destroying the data (or returning it) once it is no longer useful to the task force?
- Will the data be used for additional purposes beyond tracking Covid-19 (e.g., for law enforcement purposes)?
- Some state governments have issued stay-at-home orders: will this data be used by state governments and law enforcement to enforce these orders?

## Consumer Protections Must Be Considered

Although the information is being shared for altruistic purposes (i.e., the tracking of Covid-19), opponents of the data sharing practice argue there needs to be more clarity in how the data is being shared and there must be an emphasis on consumer protection. How technology companies and the federal government address these concerns remains to be seen.

These data sharing practices come on the heels of more draconian data sharing practices around the world, including extensive surveillance practices in Singapore involving tracking where infected individuals have been and the Iranian state-developed app for individuals to check their symptoms but which also includes a geo-tracking feature.

Ultimately, we are facing a global crisis that has created catastrophic consequences. In utilizing cutting-edge technology to track and fight the pandemic, we should understand that there remains a careful balance between public health and privacy considerations.

In determining how the technology will developed and deployed, we should not only consider how the technology will be used to battle Covid-19, we should also carefully consider how it will be used in the future, in a post-Covid-19 world.

*This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.*

## Contact

**Shalin Sood**
Associate, Washington DC
T +1 202 457 6183
E shalin.sood@squirepb.com