Coronavirus Response To Test Limits Of Location Privacy

By Ben Kochman

Law360 (March 31, 2020, 10:53 PM EDT) -- U.S. authorities may be able to use location data culled from smartphones to track people amid the coronavirus pandemic without breaching privacy laws, but they should explain how they are masking that data and taking steps to avoid targeting individuals, attorneys told Law360.

Privacy lawyers agreed that it might be legal for federal, state or local governments to use "anonymized" cellphone location data to determine, for example, whether people are flouting shelter-in-place orders by gathering in public places. But U.S. authorities will enter murky legal ground if they attempt to track the locations of individuals who have tested positive for the coronavirus, in a process known as contact tracing.

Governments should also take steps to explain what identifying pieces of information they have stripped from location data in order to ensure that it is fact anonymized, and cannot later be traced back to an individual by combining it with other data, attorneys said.

"The government's use of truly anonymized data to find people engaged in behavior that risks public health in a public place is not going to present any kind of constitutional issue," said Jed Davis, a veteran privacy attorney and former federal prosecutor. "The hard question is: Is it truly anonymized, and even if it is, what is the government doing, if anything, to trace people into private spaces?"

The U.S. government's approach to handling cellphone location data amid the pandemic was not yet clear Tuesday, and officials at the Centers for Disease Control and Prevention did not return a request for comment. But other governments across the world have been not shy in demanding that telecommunications firms or other companies with access to location data pass on that information to public health authorities.

The Israeli government, for example, approved emergency legislation earlier this month that will allow authorities to locate those who have tested positive for the virus

and to enforce two-week quarantines by monitoring geolocation data, Prime Minister Benjamin Netanyahu said in a Facebook post.

In Poland, citizens returning from trips abroad after March 15 were given a choice of either receiving unexpected visits from the police or downloading a smartphone app called Home Quarantine, which Agence France-Presse reported uses geolocation and facial recognition data to ensure compliance, even requiring users to send the government "selfies."

The Chinese government, meanwhile, has tapped into an existing geolocation surveillance apparatus to enforce coronavirus-related quarantines, requiring citizens to use an app that tells them whether they need to isolate themselves, according to media reports.

The U.S. does have several laws that address location data privacy, even without a comprehensive federal law that explicitly addresses location privacy. Using location data to track specific people in the U.S. during the pandemic may violate the Fourth Amendment's ban on unreasonable searches and seizures, said Jennifer Daskal, faculty director of the tech, law and security program at American University's Washington College of Law.

"There should be a clear line between population-level analysis and individualized tracking, which raises much greater privacy and civil liberties concerns," Daskal said.

So far, authorities appear to be focused on potentially harvesting location data in a de-identified, aggregated form in order to track the spread of the virus. The Washington Post has reported that the U.S. government is discussing such a plan with tech giants like Google and Facebook, while The Wall Street Journal reported that the CDC and local governments are already using anonymized data harvested by the mobile advertising industry in a bid to help authorities understand how U.S. residents might be spreading the disease.

Attorneys who spoke with Law360 agreed that it would be far easier for the government to justify sweeping up geolocation data if it can make the case that it is being used in anonymized, aggregate ways. The Fourth Amendment, plus federal statutes like the Electronic Communications Privacy Act and state laws like Utah's

Electronic Device Location Amendments, limit the circumstances in which private companies can turn over location data to the government, with particular attention given to "personally identifiable" data.

"If it comes to individualized location tracking, that will be a hard mountain to climb," said Sherrese Smith, vice chair of the data privacy and cybersecurity practice at Paul Hastings LLP. "I think the inclination is to hold off trying to give that information to anyone."

Scott Lashway, co-leader of the privacy and data security group at Manatt Phelps & Phillips LLP, said companies will still need to make sure there is a valid legal basis for providing any location data requested by the government.

"I don't think this changes their obligations, though this might be on a larger scale than what they usually deal with," Lashway said.

Telecommunications companies may be particularly cautious in handing over location data to the government, given that the Federal Communications Commission in February proposed $200 million fines for the top four mobile carriers for allegedly mishandling customers' location data.

There are also questions about whether what is being called anonymized data is truly anonymous. Computer scientists have for decades reported that "clever adversaries can often reidentify or deanonymize the people hidden in an anonymized database" by using outside sources of information, Georgetown University Law Center professor Paul Ohm wrote in a 2009 paper on what he called the "surprising failure of anonymization."

Governments claiming to be processing geolocation data anonymously might be wise to explain what precise steps they have taken to do so. The Health Insurance Portability and Accountability Act, for example, requires 18 different identifiers to be removed for a piece of information to be deemed not "personally identifiable," including names, Social Security numbers and IP addresses, or for handlers of the data to provide an "expert" opinion that the data has been properly de-identified.

"Companies in the privacy space always say that we can anonymize the data, but

the question is, how exactly are they doing that?" said Ryan Logan of Hunton Andrews Kurth LLP, who advises companies on HIPAA issues. "It needs to be spelled out in a clear and conspicuous way that the average person can understand."

Government health care facilities can be required to pass on the names of people who have tested positive for the coronavirus to public health authorities due to a HIPAA exemption for emergencies, Logan said. But it's unclear whether U.S. authorities would attempt to use location data to do contact tracing of individuals, given how widely the disease has already spread and the reported lack of widespread testing for the virus around the country.

Civil liberties advocates say they are on high alert for any attempts by the U.S. government to pass legislation broadening its legal authority to monitor citizens during the crisis, with some drawing comparisons to domestic surveillance programs that Congress authorized in the Patriot Act shortly after the 9/11 attacks.

Those powers, including a massive bulk collection program for domestic telephone metadata, were curtailed in the 2015 USA Freedom Act, but lawmakers have continued to extend them at the request of U.S. intelligence agencies, including most recently in March.

"Hopefully, we can focus on pieces of data that we know actually serve people and help in these situations," said Michelle Richardson, director of privacy and data at the nonprofit Center for Democracy and Technology.

"Now is not the time to do big data grabs and experiment over time," Richardson added. "Because if we are sincerely looking at how mass data collection has happened in the U.S. in the past, it is likely to be not all that effective, and ripe for abuse."

--Editing by Breda Lund and Brian Baresch.