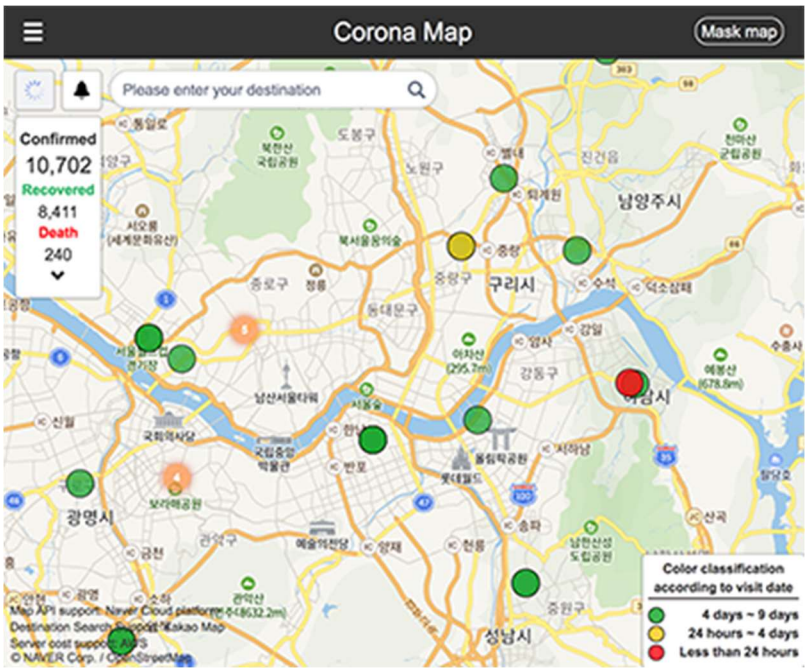
How Virus Surveillance And Civil Liberties Could Collide

By **RJ Vogt** https://www.law360.com/articles/1267269/print?section=access-to-justice

Imagine your phone buzzing with an alert: Someone who passed you at the grocery store has tested positive for COVID-19. Based on location data transmitted through a smart phone app, authorities believe the stranger exposed you to the coronavirus. You might be infected.

The alert directs you to self-quarantine for 14 days to prevent further spread of the deadly disease. In the app, a map of color-coded dots displays the population of your home town. You notice the dot associated with you, previously green, has turned to yellow — now everyone else with the app knows you could be dangerous.



Whether the scenario sounds Orwellian or absolutely necessary could depend on your answer to a rhetorical question Dr. Anthony Fauci, director of the National Institute of Allergy and Infectious Diseases, recently posed during a live Snapchat interview.

"Do you give up a little liberty to get a little protection?" he said.

The answer seems to be yes in at least 23 countries, where dozens of "digital contact tracing" apps have already been downloaded more than 50 million times. Authorities in Australia, India, the United Kingdom and Italy are also deploying drones with video equipment and temperature sensors.

According to experts like Fauci, such widespread public health surveillance is essential to containing the deadly coronavirus that's killed more than 50,000 Americans and infected nearly three million people around the world.

But the devil is in the details for groups like the American Civil Liberties Union and Amnesty International.

For example, in an April 8 report, the ACLU said engineers and tech experts agree that cellphone location data cannot accurately identify contacts within six feet, the generally accepted radius of COVID-19 transmission. The group noted, however, that such data could be accurate enough to place a person near a "bank, bar, mosque, clinic or other privacy-sensitive location."

"Location data contains an enormously invasive and personal set of information about each of us, with the potential to reveal such things as people's social, sexual, religious and political associations," the ACLU report states. "The potential for invasions of privacy, abuse and stigmatization is enormous."

Michael Kleinman, director of Amnesty International's Silicon Valley initiative, shared a similar sentiment during an April 2 workshop on surveillance and human rights.

"There is an understandable desire to marshal all tools that are at our disposal to help confront the pandemic," he said. "Yet the country's efforts to contain the virus must not be used as an excuse to create a greatly expanded and more intrusive digital surveillance system."

Because U.S. health agencies and big technology companies are still developing the public-private partnerships necessary to enable digital contact tracing, it remains to be seen whether app-based monitoring or drone usage will be challenged in court as a violation of Fourth Amendment rights to be free from unlawful search and seizure.

But considering the rash of constitutional litigation already filed by churches and other groups over social distancing orders, legal experts say it's only a matter of time before public health surveillance is tested in court.

There will be judicial review, but the response will depend on the nature of the surveillance.

"I think, definitely, there will be cases," said Eric Posner, a law professor at the University of Chicago. "There will be judicial review, but the response will depend on the nature of the surveillance."

He noted the precedent set by Jacobson vs. Massachusetts, a 1905 case in which the U.S. Supreme Court upheld a state's authority to enforce compulsory smallpox vaccination laws. In a 7-2 majority opinion, Justice John Marshall Harlan wrote that liberty is not "an absolute right in each person to be, in all times and in all circumstances, wholly free from restraint."

"Vaccinating someone against their will is pretty invasive," Posner noted. "To violate the Fourth Amendment during a pandemic, you'd need to do something that's even more extreme than that."

Traditionally, public health surveillance hasn't triggered data privacy debate. Previous contact tracing efforts relied on manually interviewing infected persons about their movements and then notifying those who may have crossed their paths.

But because COVID-19 spreads rapidly through unknowing asymptomatic carriers, many scientists believe that harnessing big data and 21st-century technologies is the only way to control contagion.

In the words of a widely cited March 31 Science article by four Oxford University researchers, "viral spread is too fast to be contained by manual contact tracing, but could be controlled if this process was faster, more efficient and happened at scale."

"A contact-tracing app which builds a memory of proximity contacts and immediately notifies contacts of positive cases can achieve epidemic control if used by enough people," they added.

That type of system is already in place in South Korea, where the government publishes online the movements people made before being diagnosed with the virus. Surveillance via GPS phone tracking, records from credit card purchases and store security camera footage has helped authorities keep infections to a fraction of the levels seen in the U.S.

Although the detailed reporting of people's movements has led to several human rights complaints — Choi Young-ae, chair of the National Human Rights Commission of Korea, has warned that the "excessive disclosure of private information" could cause people with symptoms to avoid testing — public outrage has been nearly nonexistent.

All the measures are authorized under a law passed in 2009 to respond to the country's MERS outbreak, and the widespread surveillance has enabled far more economic activity than in the U.S., where surveillance has been comparatively minimal.

That could soon change, however.

On April 10, American tech giants Apple and Google announced a joint effort to enable government contact-tracing via the Bluetooth technology on their devices. In their announcements, the companies emphasized that "user privacy and security" would be central to the project, which would have an opt-in component and could roll out its initial stages in May.

Posner said such surveillance, though certainly intrusive, may be preferable to the stay-at-home orders that most Americans have experienced over the past month.

"While it would be a restriction on liberties, surveillance might allow a relaxation of the more obtrusive restrictions currently in place," he said.

But for Mason Marks, a Gonzaga University law professor, the assurances of Big Tech do little to assuage fears of overreach.

"Historically, we have seen Big Tech firms abusing and misusing the data they collect for purposes other than those officially stated by them," he said, noting Facebook's Cambridge

Analytica scandal as one example. "Moreover, Big Tech is likely to find more uses and to derive more inferences once new analytical tools are available in the future."

I don't see a world in which we can deal with this without a government being more intrusive.

Last week, Marks and Ido Kilovaty, a law professor at the University of Tulsa, published an op-ed in The Hill calling on federal and state lawmakers to enact a "right to digital self defense" ensuring Americans can freely use anonymity, privacy and cybersecurity tools to shield themselves from data collection.

They noted that public-private partnerships, like the one Apple and Google are reportedly working on, circumvent protections in the Bill of Rights because the tech companies conduct the surveillance — not the government itself.

"If Big Tech moves forward with their network of surveillance, and in the absence of state action, the Fourth Amendment might not apply to the unreasonable uses of such surveillance," the pair wrote in an email to Law360.

So far, White House transparency about what surveillance measures the government is working on has been limited.

After multiple media outlets reported that Jared Kushner, a White House senior adviser and President Donald Trump's son-in-law, had contacted a range of health and technology companies about creating a national coronavirus surveillance system, three lawmakers expressed privacy concerns in an April 10 letter.

"This growing health pandemic further exacerbates increasing concerns about the role large tech firms are starting to play in our health care sector," wrote U.S. Sens. Mark R. Warner, D-Va., and Richard Blumenthal, D-Conn., along with U.S. Rep. Anna Eshoo, D-Calif. "These partnerships have bolstered the platforms' ability to exploit consumer data and leverage their hold on data into nascent markets such as health analytics."

The legislators asked eight questions in the letter, seeking, among other things, information on what companies Kushner contacted, whether the administration would commit to stopping the data collection when the emergency ends, and what measures the administration was taking to prevent discriminatory outcomes on marginalized groups.

According to a spokesperson for Blumenthal, Kushner has not responded. But clear answers will be hard to come by in the absence of concrete proposals, according Alan Rozenshtein, a law professor at the University of Minnesota who previously advised the National Security Division of the U.S. Department of Justice.

But Rozenshtein noted that the response to the Sept. 11, 2001, terrorist attacks could be indicative of what lies ahead for Americans.

He said measures like robust contact tracing programs could raise similar constitutional concerns as the National Security Agency's bulk collection of telephone metadata via the USA Patriot Act. Nevertheless, he noted that judges have tended to back executive authority, especially in times of crisis.

"I don't think courts will stand in the way," he added. "Pandemics are key drivers of

government expansion — I don’t see a world in which we can deal with this without a government being more intrusive.”

https://www.law360.com/articles/1267269/print?section=access-to-justice