Contact Tracing Shouldn't Upend 4th Amendment Protections

By **Lara Yeretsian** (June 8, 2020)

Lara Yeretsian

As the country slowly reopens following the initial onslaught of COVID-19, public health officials are urging that states and counties implement rigorous contact tracing to forestall future outbreaks.

Contact tracing works by identifying where people who have tested positive for the virus have traveled and with whom they've interacted.

The intent of these programs, which have shown positive results in other countries, is to alter the trajectory of the pandemic. It's an unobjectionable undertaking, but it could end up becoming a criminal justice nightmare.

Contact tracing requires that the information of more than one person is collected. A subject who has opted to participate in the program allows his or her geolocation and proximity data to be tracked. That person's friends, colleagues and acquaintances may now show up on the government's radar screen, whether they've agreed to be tracked or not, and without any forewarning.

Without probable cause for a search warrant, law enforcement could, absent legal restrictions, use geolocation data to build a case for probable cause against a criminal suspect. Proximity data could provide police with new tools for tracking cohorts against whom there isn't reasonable suspicion, simply by using other parties' location information.

It's not unlike DNA that has been submitted to a genealogical site for purposes of uncovering one's ancestry. The person submitting a DNA sample does not agree to its use by law enforcement to track down and arrest relatives who may have committed unsolved crimes. The implications of extending the same legal sophistry to law enforcement's use of COVID-19 data to go after criminal suspects should be troubling to everybody who cares about our system of justice.

At the end of April, U.S. Sens. Roger Wicker, R-Miss., John Thune, R-S.D., Jerry Moran, R-Kan., and Marsha Blackburn, R-Tenn., introduced the COVID-19 Consumer Data Protection Act, whose intent is to "provide all Americans with more transparency, choice, and control over the collection and use of their personal health, geolocation, and proximity data."

The act would require covered companies to obtain express consent from individuals to collect, process or transfer their personal health, geolocation or proximity information for the purposes of tracking the spread of COVID-19. Companies would have to tell consumers how their data will be handled, to whom it will be transferred, and how long it will be retained. They would also be required to delete or deidentify all personally identifiable information when it is no longer being used for the COVID-19 public health emergency.

Covered companies — those subject to Federal Trade Commission jurisdiction, as well as not-for-profit entities and common carriers — would be obligated to disclose to consumers at the point of collection how their data will be handled, to whom it will be transferred, and for how long it will be retained.

They would be required to publish transparency reports every 30 days describing their data

collection activities related to COVID-19 and to delete or deidentify all personally identifiable information when it is no longer being used for the COVID-19 public health emergency.

Companies would also be required to have an effective opt-out mechanism for individuals to revoke their consent for the collection, processing and transfer of personal information, and they would need to adhere to prescribed data minimization and data security requirements for all personally identifiable information they collected.

Information that is aggregated, deidentified or publicly available is not considered covered data under the proposed law. Significantly, the bill would provide no private right of action, authorizing state attorneys general to enforce its provisions.

The act defines "precise location data" and "proximity data" as a person's past or present physical location. There are important public safety benefits to tracking the location of individuals who have received a positive COVID-19 diagnosis, as well as the identity and location of others with whom they've come into contact.

It's critical to understand who has been exposed to a COVID-19 carrier so that those people can be notified and can take immediate precautionary steps to prevent further exposures.

At the same time, however, the specter of Big Brother arises when we talk about tracking people's exact whereabouts. Without clear legal boundaries, geolocation and proximity data could become weapons in law enforcement's arsenal, used to track down people suspected of crimes in direct contravention of more than two centuries of protections against unreasonable search and seizure. Once the data is collected, how do we ensure that it isn't used for a different purpose?

The text of the CCDPA doesn't answer the question. Section 3(a) provides as follows:

During the COVID–19 public health emergency, it shall be unlawful for a covered entity to collect, process, or transfer the covered data of an individual for a purpose described in subsection (b) unless. ... (3) the covered entity publicly commits not to collect, process, or transfer such covered data for a purpose other than the purpose described in subsection (b) to which the individual consented unless — (A) such collection, processing, or transfer is necessary to comply with the provisions of this Act *or other applicable laws*. (emphasis added)

Subsection (i) opens the door to collection and use of third-party data:

Notwithstanding subsection (a), a covered entity may collect, process, or transfer the covered data of an individual or group of individuals for a purpose described in subsection (b) during the COVID–19 public health emergency without obtaining the affirmative express consent of the individual if such collection, processing, or transfer is necessary to allow the covered entity to comply with a Federal, State, or local legal obligation.

It isn't enough that the proposed CCDPA requires companies to notify consumers about how their data will be used and with whom it will be shared. The law must explicitly prohibit the transmission of location data to law enforcement, and it must include a private right of action.

Relying on attorneys general to monitor and assess penalties for alternative uses of the information — especially to give a leg up to law enforcement in prosecuting suspected criminals — is unrealistic.

Location data could give police another mechanism for pursuing suspects, despite laws against unreasonable search and seizure. Just as with other violations of Fourth Amendment rights, evidence gathered as a result of geolocation or proximity tracing must be thrown out of court as unlawfully obtained.

Unless a suspect's relationships and location are public knowledge or are obtained through a valid search warrant, evidence obtained as a direct result of contact tracing data must be deemed inadmissible.

When society stops protecting the rights of criminal suspects, it stops protecting all of our rights.

Lara Yeretsian is a Los Angeles criminal defense attorney and principal of Yeretsian Law.