Published on *American Council on Science and Health* (https://www.acsh.org)

Tracking and Tracing in the Time of Covid: Public Good or Unreasonable Search and Seizure?

By Chuck Dinerstein, MD, MBA — September 15, 2020

Geofencing is a virtual fence in the real world. When combined with our homing beacon -- the smartphone that identifies us everywhere we go -- it becomes a tool with extraordinary powers, for good and evil. Several recent court cases, which likely have escaped your attention, may give you more than a moment's pause in this era of the coronavirus.

Image courtesy of Ezequiel Octaviano on Pixabay [1]

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

For those of us that need a moment, that is the 4th Amendment to our constitution – the one discussing unreasonable searches. I want to share three scenarios involving that Amendment beginning with the most common form of search and seizure, advertising, in this case, marketers who search for you and seize your attention.

Case 1 - Geofencing for Dollars

My predecessor, Dr. Wells, wrote [2] often about patient privacy and geofencing, spurred on by its most widespread form, providing targeted marketing information.

"Our … geo fencing technology allows law firms to use this legal marketing target people based on their physical activities. Whether it's a particular event or a physical building you want geo fenced (i.e., hospital, car dealership, etc..), this can be a powerful form of lawyer marketing to serve ads to individuals based on their physical location."

Your visit to the Emergency Room may well result in a plethora of ads for "slip and fall" attorneys suddenly appearing in your social media feeds. A profitable market [1] in connecting a consumer who doesn't even know their needs with the persons most likely to fulfill them. And while a transient pain or something to ignore, after all the ads will move on to other salient interests and geographies, who really cares? Does it matter?

Case 2 - What about geofencing that helps us catch bad guys?

Consider the theft of valuable pharmaceuticals. Law enforcement asked the courts for a geofencing warrant – asking for all the phone numbers in the vicinity of the robbery during three forty-five minute periods. The government requested that Google, in this case, provides them with anonymized location data, which they, in turn, would sift through finding numbers of interest and then asking Google for the accounts. In early July, the courts ruled that the warrant request violated 4th Amendment rights – those of search and seizure, probable cause. The Court found the request "overly broad," it was, after all, a geofenced urban area with lots of phones, and nothing was holding the police from asking for all the accounts, no sifting at all.

The government modified their request, just the numbers, no account information. This amended warrant was also denied based on a Supreme Court decision involving the real world. In that case, the Court found that a warrant to search a bar and bartender did not give them leave to search all of the bar's patrons.

Case 3 - What about geofencing to protect our health?

In the time of COVID, track and trace can be seen as an essential public health measure. If we can identify the vectors, they can be isolated, and the burden of COVID-19 on our health and economy lessened. Mobile phone geolocation information, a necessary component of geofencing, has been used in research to demonstrate how mobile or locked down the public has become and was probably the most realistic of data in the Sturgis Motorcycle Rally [3] saga. For the most part, Western track and trace programs do not require disclosure of personal information. But it is that more private information that is the most helpful epidemiologically. In some ways, track and trace

is no different than the dilemma we face with most digital apps, being anonymous or the convenience of cookies and other digital baggage that informs the app and its owner of who we are, who we know, and what we may be doing.

The track and trace programs rolled out in South Korea, and Hong Kong do make use of personal data. These programs can tell you if you have been in contact with a possibly infected individual because it coordinates public health information with your geolocation data. From a public health perspective, this makes the programs better at identifying the at-risk; kinda like how the government wants to sift through those phone numbers.

"This is particularly important because contact tracing requires surveillance not just of infected individuals but of all the individuals the infected person might have come into contact with. This means that the government will need to collect information on individuals it has little individualized suspicion to think have contracted the virus." – Alan Rosenshtein

We already have established law requiring the reporting of disease, especially infectious disease, to the government. Track and trace for a rapidly spreading disease such as COVID-19 are not feasible as a manual process. It has to scale to short time frames and large populations, and that makes cellphone apps the most effective means at our disposal. As described [4] by Alan Rozenshtein, an Associate Professor of Law at the University of Minnesota Law School, the Fourth Amendment has a special interest exemption. But, from a legal point of view, the exemption can be ambiguous. It allows us to set up drunk driving checkpoints and to require all employees to be drug tested. But the same exemption does not allow for checkpoints for drug interception or for randomly requiring random employees to be drug tested. Of course, in times of emergency, our rulings tend to consider the aggregate need over that of the individual.

The Expectation of Privacy

In some ways, all of these concerns boil down, from a legal point of view, to whether we expect privacy, in this instance, the use of our cell phones. The fourth Amendment applies solely to the government, but when it comes to our privacy, we need to consider the digital players. Google and Apple have announced a collaboration where health information can be shared on their respective mobile software platforms with public health apps downloaded by end-users, us. They also plan to create a track and trace ability into their platform, so that any developer can use these tools, of course, with your consent made explicit somewhere in the bowels of the EULA. That you do not recognize the acronym EULA, End User Licensing Agreement, is perhaps all you need to know about how well your privacy is protected and used. For those of you already hip to EULAs and who claim to read them in detail, consider this interesting factoid [5]. "In 2017, 22,000 people who signed up for free public Wi-Fi inadvertently agreed to 1,000 hours of community service — including cleaning toilets and "relieving sewer blockages."

We have already allowed marketeers to invade the privacy of our locations. The Courts are upholding our 4thAmendment rights, tempering the requests of law enforcement to pursue criminal behavior. Where do we put our rights and responsibilities when it comes to public health. How will the battle over masks and social distancing play out when it comes to track, trace, and the 4th

Amendment?

[1] According to at least one source [6], the word lawyer in an advertisement is the fourth most profitable AdWord or "keyword" for Google. Each click costs the attorney $54.86. Feel free to click away.

Sources: New Federal Court Rulings Find Geofence Warrants Unconstitutional Electronic [7] Frontier Foundation.

Disease Surveillance and the Fourth Amendment [4] Lawfare

Links
[1] https://pixabay.com/photos/legal-right-justice-law-of-nature-5293009/
[2] https://www.acsh.org/news/2019/02/25/patient-privacy-relic-everyone-outside-exam-room-13834
[3] https://www.acsh.org/news/2020/09/10/sturgis-effect-15018
[4] https://www.lawfareblog.com/disease-surveillance-and-fourth-amendment
[5] https://www.npr.org/2019/03/08/701417140/when-not-reading-the-fine-print-can-cost-your-soul
[6] https://medium.com/marketing-and-entrepreneurship/here-are-the-top-10-most-expensive-keywords-on-google-aaf3773479eb
[7] https://www.eff.org/deeplinks/2020/08/new-federal-court-rulings-find-geofence-warrants-unconstitutional-0