Bloomberg Law

Professional Perspective

Minimizing Pandemic Impact Through Location Data

Joel Schwarz, The Schwarz Group, LLC

Minimizing Pandemic Impact Through Location Data

Contributed by Joel Schwarz, The Schwarz Group, LLC

Ever since social distancing and contact tracing entered our daily lexicon, stories about the sharing of consumer location data have dominated the headlines. The most common reasons cited for needing this data have been:

- Assessing virus hotspots and the spread of the virus (relatedly, over a period of time this data can also be used to monitor reduction of hotspots, and slowing of the virus spread)
- Measuring compliance by communities with social distancing and/or stay at home orders
- Engaging in contact tracing to identify who an individual diagnosed with Covid-19 has been in contact with in the previous 14 days

Of course, there are additional uses for location data in the fight against Covid-19 not mentioned above, such as assessing the impact of stay-at-home orders on a local economy, but the above uses are certainly the most oft-cited in conjunction with pandemic-related needs.

Conspicuously absent from the discussion have been details about what data is being shared, and under what legal authorities. Based upon what's been reported publicly, there's enough information to make some educated guesses as to sources of the data involved, from which we can then assess the legal authorities that govern the sharing of this data.

Cell Phones

According to a Pew Research poll, as of February 2019, 81% of Americans owned a smartphone. Most of these phones incorporate functionalities that track location, movement, proximity, and orientation in one form or another. This data is then captured by the manufacturer of the phone's operating system, whether that's Google's Android, Apple's iOS, Huawei's Harmony O/S or something else. So long as a phone's location button is toggled on, this data is captured and reported back to the manufacturer at varying frequencies throughout the day.

GPS, Wi-Fi, and Bluetooth

GPS is by far the most accurate location information commercially available on a phone. And as one might expect, any phone that has a built-in GPS receiver—which is most phones today—is able to generate this information.

Wi-Fi can also be used to track location, although the information is generally not as precise as GPS. This location data then sits with the provider of the Wi-Fi service, whether it's a city-wide Wi-Fi network, or a local Wi-Fi hotspot, such as those offered by Starbucks, KFC, and probably hundreds if not thousands of other locations throughout a city. Interestingly, once you sign up with one hotspot, the terms of service usually allow the provider to continue tracking you when you pass other branded hotspots. And because there are only a limited number of hotspot providers, there's a finite universe of entities gobbling up this location data.

Bluetooth is more localized, useful for connecting to other devices in close proximity to a phone. While Bluetooth doesn't necessarily capture a user's precise location, it's become the technology of choice for contact tracing apps, including the API developed collaboratively between Google and Apple. This data is then stored locally on the phone, in a location designated by the App provider, or both.

Wireless Telecom Providers

Any time a cell phone is on and cellular service is active, it almost continually searches for cell towers to maintain connectivity. This creates a record identifying the cell phone's location, known as cell site location information, which is stored by the telecom provider (i.e., Verizon, Sprint, T-Mobile, etc.), the precision of which varies based upon cell tower coverage in the area. In a rural area, a single cell tower might cover miles of territory, while in a highly dense city area, a cell tower may cover a few city blocks.

Third-Party Apps and Providers

Because most if not all apps request access to location, app manufacturers also have access to location data. Users of course have the option of sharing location information one time, only while the app is in use, or all the time, the choice of which determines the richness of the location information collected.

Many apps today also share this information with third-party analytics companies to analyze data points relating to use, as well as with advertising companies (e.g., Doubleclick) and social media sites (e.g., Facebook and LinkedIn) to monetize the traffic.

To understand how apps and third-party analytic companies can use this information to aid with combatting the pandemic, consider the mapping by data visualization group Tectonix. Specifically, they demonstrated the potential impact of ignoring social distancing by analyzing "secondary locations of anonymized mobile devices [collected through apps] that were active at a single Ft. Lauderdale beach during spring break," and then visualized how those individuals could potentially spread the virus as they traveled home across the U.S.

Wearable Fitness and Health Devices

Finally, many people today own a smart watch, a Fitbit, or use some type of wearable fitness or health device as part of an exercise and fitness regimen (wearables). Each wearable tracks location information and is potentially shared with the manufacturer.

Consider when San Francisco-based Strava updated its global heat map of user activity—collected from wearables—enabling the visualization of people engaging in running and cycling around the world. This included U.S. military forward operating bases in Afghanistan, Syria, and elsewhere, putting military operational security at risk.

Legal Authorities for Location Data Sharing

Having identified the most likely potential sources of location information used to address pandemic-related needs, the next question is, what laws allow for sharing of this information with the government and the private sector?

To answer, two categories should be examined: data shared with the government, and data shared with anyone not affiliated with the government. This piece will focus exclusively on federal law.

Sharing Data With the Government

Why differentiate between sharing with the government and the private sector? Because many of our laws are designed to protect against overreach by the government, not private parties. Likewise, the Fourth Amendment guarantees a right to privacy, but only against unreasonably invasive searches by the government.

Interestingly, none of the location data discussed above is actually protected by the Fourth Amendment. That's because people lose their reasonable expectation of privacy (REP) when they disclose information to a third-party. This is known as the third-party doctrine (although, as noted below, there are cracks emerging in the absolutism with which the third-party doctrine has traditionally been applied).

As a result of the third-party doctrine, courts have found no REP in a phone number dialed, because the act of dialing the number conveys the number to the phone company, a third party. *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). The same holds true for data transmitted through a wireless cell provider, although the Supreme Court has noted that the third-party doctrine doesn't automatically vitiate Fourth Amendment protection, given the unique nature of cell site location information. *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

In 1986 Congress passed the Electronic Communications Privacy Act, which included protection for stored content and non-content of communications, pursuant to a law known as the Stored Communications Act. Under the SCA, the government can compel providers to produce information about a subscriber of a communication service, including location information. However, it's questionable whether the government could actually use the SCA to compel providers to produce location data for pandemic-related purposes, because in order to compel there needs to be a belief that criminal conduct is involved, which is unlikely given the stated purpose.

The SCA does, however, allow voluntary sharing of non-content location data with the government in several circumstances, one of which is applicable to the pandemic. Specifically, pursuant to 18 U.S.C.§2702(c)(4), a provider may disclose information pertaining to a customer of the service, including location information. "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency..."

Sources of Information Covered by the SCA

Importantly, the SCA only applies to "Electronic Communications Services" (ECS), meaning services that enable a user to send and receive communications with others. For example, when Airbnb challenged a subpoena served on them by the government, the court differentiated between platforms that provide "user-to-user messaging," which are covered by the SCA, and platforms that merely allow users to interact with the platform itself, which are not covered by the SCA. *In Re Application of the U.S.A. for an Order Pursuant to 18 U.S.C. §2705(b)*, 289 F. Supp. 3d 201 (Dist. D.C. 2018). The court ruled that Airbnb was indeed covered by the SCA because of "Airbnb's user-to-user electronic messaging system."

Applying this prerequisite to the companies holding the location data discussed above, it becomes clear that not all of them are covered by the SCA:

- Wireless carriers that provide cell phone service are ECSs, as would be the entities that provide Wi-Fi network connectivity.
- It would also appear that the location information captured by phone manufacturers, such as Apple's iOS and Google's Android, are also covered by the SCA.
- Conversely, only some of the app providers that hold location records appear to be covered by the SCA. Apps that allow users to communicate with others, such as Instagram, Facebook, and WhatsApp, are covered. On the other hand, apps such as health trackers and temperature apps may not be covered by the SCA, because they don't allow users to communicate with others, just the platform or manufacturer.
- Relatedly, the third-party analytics providers and advertising companies that receive data shared by apps are clearly not covered by the SCA, because they're not designed to provide communications services to users. Their relationship is exclusively with the app provider.
- Social media sites, on the other hand, to the extent they allow interaction with other users, are probably covered by the SCA. Indeed, even posting information through mechanisms such as a Facebook wall, for a group of other users to view, has been determined to fall within the purview of the SCA. *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659 (Dist. NJ 2013).
- Whether the SCA covers location information captured by wearables will vary by the device itself. Some devices, such as the Kinsa Thermometer, appear to only allow communication with the app or the device manufacturer, not with other users. Other devices, such as an Apple watch, fall into a gray area, providing communication services like voice and email, but only when paired with an iPhone. Interestingly, the Fitbit watch seems to have evolved over time, and now allows users to share their health and training stats with friends - even sending messages of support and encouragement to others – potentially moving the Fitbit into the zone of an ECS, although this is by no means definitive yet (nor has this been tested in court).

SCA Exemption Impact on Tracking Devices

A further consideration relates to Congress's exclusion of tracking devices from coverage under the SCA. A tracking device is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. §§2510(12)(c), 3117. This then begs the question as to whether the SCA's tracking device exclusion applies to this location data.

While not definitively resolved for all the aforementioned data sources, there are two reasons to believe that the tracking device exclusion wouldn't affect the SCA's coverage of this data.

First, the focus of the tracking device exclusion is on devices specifically designed and installed for tracking purposes, such as those placed on a vehicle or a person to track movements. *In re Search of a Cellular, Telephone ___, Cellular, Number ___*, 2019 BL 501734 (Dist. UT 2019). Yet none of the devices used to generate this location data are designed as tracking devices. Cell phones are designed for communication, and to the extent wearables are covered by the SCA, they're generally designed for a particular health or fitness medical purpose, not for tracking movements. Likewise, it's a stretch to argue that an app designed for sharing information or speaking with others is a tracking device. At best, the tracking component of these devices is an ancillary byproduct of the device's main purpose.

Second, to the extent there's been litigation surrounding the tracking device exclusion—most commonly with regard to cell site location records—the cases have focused on prospective collection, the premise being that when the government seeks access to prospective cell site information this effectively converts a cell phone into a tracking device. *In re Smartphone Geolocation Data Application*, 977 F. Supp. 2d 129, 148 (E.D.N.Y. 2013). For purposes of Covid-19, however, the focus is not on prospective location information, but rather on historical location data already captured by the companies. The same holds true for the data collected by Wi-Fi providers, cell phone manufacturers, apps, third-party analytic companies, advertisers, social media sites, and wearables; all the location information disclosed is presumably historical data, previously captured by the device in the ordinary course of operation.

SCA Privacy Protection for Data Shared with Private Sector

But what about SCA-covered location data that's shared with other private sector entities?

Pursuant to 18 U.S.C. §§2702(c)(6), providers are allowed to voluntarily share SCA-covered data with other private sector entities without restriction, so long as the data is limited to transactional data, like location data, and doesn't include content. Potential limitations on such sharing, however, may stem from requirements outside of the SCA, such as the Terms of Service (TOS) and Privacy Policy published by the company that collected the location data. Further limitations may spring from state-specific privacy statutes, such as the California Consumer Privacy Act.

This also holds true for data shared with the government or private sector that's not covered by the SCA; the TOS and Privacy Policy control whether and what privacy protections are incumbent on the data.

Many privacy policies explicitly include exceptions for disclosure without consent when shared with the government for emergent purposes, such as public health. Even Apple's privacy notice—Apple's privacy commitment being legendary—reserves broad discretion to disclose information about a person "if we determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate." To the extent Apple and Google are sharing location information in their possession for pandemic-related purposes, however, they're apparently sharing this in non-identifiable forms, either anonymized, aggregated, or both.

Voluntary Sharing Under the Communications Act of 1934

In addition to SCA-imposed limits on disclosure of location information, and a company's TOS and Privacy Policy, limitations can also come from industry-specific statutes. Take, for example, the Communications Act of 1934, which governs location data held by wireless carriers. In February 2020 the FCC proposed cumulative fines of over $200 million against the 4 largest wireless carriers, T-Mobile, ATT, Verizon and Sprint, for selling customer location information to aggregators, who in turn, resold that information to third-party location-based service providers, without adequately adhering to the privacy requirements of the Communications Act.

Pursuant to §222(a) of the Communications Act, telecommunications carriers have a duty to "protect the confidentiality of proprietary information" of customers, which includes location information. Other than under a few narrow exceptions (none of which include selling to third-party aggregators), "express prior authorization of the customer" is needed for disclosure of location information, a requirement the FCC found these companies had failed to abide by.

Although the Communications Act allows a carrier to release customer location information without consent for 911, emergency dispatch, public safety, hospital emergency, and similar purposes, this exception is narrowly tailored to responding to an individual customer's need, not en masse, as is envisioned to address the needs generated by the pandemic.

One alternative for disclosing location information without customer consent under the Communications Act is when the data is released as "aggregate information," defined as "collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed." 47 U.S.C. §§222(c)(3), (h)(2). In short, under the Communications Act, wireless carriers appear to have two options for disclosing customer location information for pandemic-related purposes: express consent of individual customers, or in aggregate form.

Voluntary Sharing Under HIPAA

Another industry-specific privacy statute that might come into play with regard to pandemic-related data sharing comes from the Health Insurance Portability and Accountability Act of 1996.

Specifically, the HIPAA Privacy Rule sets standards for the use and disclosure of individuals' health information, called Protected Health Information, by organizations known as covered entities. Notably, PHI includes geographical identifiers as well as device identifiers, both of which would be encompassed within an individual's location information.

Under HIPAA, "covered entities" are health plans, health care clearinghouses, and health care providers that perform "certain financial and administrative transactions... such as electronic billing and fund transfers." Given this definition, unless the fitness or health-related app or wearable is owned by, or operated on behalf of, a health-care provider, health insurance company, or health-care clearinghouse, it's unlikely that the location data it generates is subject to HIPAA.

While some apps or wearables may fit this definition, such as an app issued by Blue Cross Blue Shield to monitor heart rate for insurance coverage purposes, the vast majority of fitness and health apps and wearables today are used by individuals on their own volition, and not in conjunction with a health-care entity.

As such, the assumption is that fitness and health-related apps and wearables are generally not covered by HIPAA, and thus not subject to the Privacy Rule. This means that the TOS and Privacy Notice of the manufacturer likely dictate the conditions under which location information can be disclosed.

To the extent a device or App is subject to HIPAA, HIPAA does permit disclosure of PHI without consent when releasing information for the "conduct of public health surveillance," as well as to public health authorities for purposes of controlling a disease. 45 C.F.R. §164.512(b)(1). The HIPAA Privacy Rule also allows disclosure, without restriction, when the data released is de-identified in such a way that it "provides no reasonable basis to identify an individual." 45 C.F.R. §§ 164.502(d)(2), 164.514(a).

Conclusion

Given the heightened privacy sensitivities surrounding sharing of location information today, there are two things that can, and should, be done to minimize the impact. One is already being done, namely sharing in aggregated de-identified form, to reduce the potential for being able to trace back to an individual. The other is transparency about what data is being shared, who is sharing it with whom, under what provisions, and for how long.

Transparency equals trust and accountability, and it's here where there is room for improvement. This is especially true now, during the pandemic, when little information is known about sharing of location information, other than the news stories discussing the concept at a high level – leaving people to speculate, generate conspiracy theories and worst-case scenarios. And it's here where this article, extrapolating about the most likely data sources, and setting forth the legal authorities under which that data might be shared, that we hopefully begin that conversation.