# Your Cell Phone Is a Spy!

By Judge Herbert B. Dixon Jr. (Ret.)

Tracking and surveillance are no longer the stuff of old espionage movies—the little black box covertly hidden underneath a car, a bug placed in a room, or an agent spying from the rooftop across the street. The most targeted surveillance subjects in the United States now voluntarily provide volumes of information that would amaze the clandestine agents of yesteryear. I am referring to that ever-present device that you rarely leave home without—your cell phone—an electronic gadget that constantly yields digital location data about your daily movements and travels.

Three years ago, I asked the question, "Is Your Internet Device Spying on You?"[1] Now, instead of asking a question, I am telling you, "Your cell phone is a spy!" It is a tracking device that logs information about your locations and movements throughout the day and reports that information to third parties. Many of us are aware of this spotlight on our daily travels, but we have traded this loss of privacy for the convenience of our ever-increasing reliance on mobile devices. What are the implications? The answers may amaze you.

An investigation of cell site location data that resulted in a series of *New York Times* articles, including "How to Track President Trump," has placed some of these implications into stark relief. The article reports how the *Times* obtained a random sample dataset consisting of over 50 billion location pings occurring in 2016 and 2017 from over 12 million people in Washington, New York, San Francisco, Los Angeles, and other major cities in the United States.[2]

## Pings, Cell Site Data, and Location Data Companies

As discussed in this column, I am using the term "ping" to include any of several ways that a cell phone provides electronic clues or descriptions of its location. This location information is often known as cell site location information or global positioning system (GPS) data. When a phone is in standby mode ready to make or receive a call, it initiates several searches a minute seeking the strongest network signal from nearby cell towers, which is often the closest tower. In this situation, the phone identifies its approximate location by connecting with a particular cell tower. Additionally, the GPS feature of a cell phone allows tracking within several feet of its precise location. Lastly, as typically referred to in the telecommunications industry, a network may "ping" a cell phone to reveal its location as part of standard network protocol. One or more entities, including the cell carrier, the phone itself, or a location data company, maintain a time-stamped log for each of these contacts.

Depending on the number of apps installed, a cell phone may send data regarding its location thousands of times per day. Indeed, some phone apps will share as many as 200 individually time-stamped location data points within a 12-hour interval.[3] These data are sent in real time to multiple companies, each of which can track the phone in real time or retrace the phone's path by analyzing the logged historical data. According to the *Times*, every minute of every day, everywhere on the planet, dozens of companies . . . largely unregulated, little scrutinized . . . are logging the movements of tens of millions of people with mobile phones and storing the information in massive data files.

Location data are collected by companies along with millions of other data points, commonly packaged and sold as marketing analysis to advertisers, financial institutions, real estate investors, and other third parties. Location data are particularly lucrative to advertisers, who use it to determine the places people frequent and the times they go to these locations. Although companies routinely package location data and commercially sell those data to other companies, additional dissemination may occur through unauthorized leaks, such as the dataset received by the *Times*, or hacking efforts by malevolent actors to steal the historical information from location data companies and cell phone carriers.

The data provided to the *Times* did not come from a "telecom or giant tech company" or "governmental surveillance operation." The data came from a location data company that collects digital information from mobile phone apps.[4]

## Analysis of the Dataset Received by the *Times*

The data provided to the *Times* included location, date, and unique identifier information for the device, but no information identifying any individual's association with a device. This is often described as anonymized data. However, deanonymizing the anonymized data was a straightforward task for the researchers. The location pings associated with each device revealed work and life patterns. This enabled the researchers to determine the location of a user's site of employment, the user's home, and other places the user frequents. Once the address of a home was located, public records for the home were accessed to provide the name of the person and often the name of his or her spouse or other persons occupying the property.[5]

It did not take long for researchers to deanonymize the data. They were able to track federal employees in almost every major government building in Washington, D.C. This included congressional advisors, department of defense officials, and Supreme Court judicial staff. The observations also included thousands of pings inside the Pentagon, on military bases, in F.B.I. headquarters, and in Secret Service facilities across the country. The researchers were even able to track a secret service agent assigned to President Trump. By proxy, the researchers were able to track the location of the president himself, capturing movements to within a few feet of accuracy on a day when the president traveled between Mar-a-Lago and nearby golf clubs, which also included a golf outing with the prime minister of Japan.

## Phone Tracking in Government Facilities

Addressing the risks associated with location tracking has proven difficult for government institutions. Policies limiting employee use of location-sharing apps are difficult to enforce, particularly as they relate to personal devices. Further, compliance with such rules is complicated by the fact that users often cannot detect which apps are actually tracking them. With cell phones being so ubiquitous and increasingly necessary, government employers find that, to an extent, they must acquiesce to their employees' use of those devices. Even when cell phone use is prohibited within government buildings, risks still exist. The Central Intelligence Agency, the National Security Agency, and other intelligence agencies prohibit most personal phones within their facilities. These agencies also advise employees to turn off their personal devices before they arrive at their work location. However, researchers still located thousands of location pings in parking lots outside these buildings, with additional pings creating trails leading back to the homes of these employees and visitors.

## Risks Posed to Courts, Judges, and Attorneys

Many of the risks present at government facilities pose similar threats to the courts. Every place judges visit could be tracked. Sensitive location information released publicly for the purpose of embarrassing or impugning the impartiality of a judge or court official could serve to undermine public confidence in the judiciary. Additionally, concerns regarding the security of the courts and the personal safety of judges are implicated. The researchers were able to track dozens of phones within multiple Washington, D.C., courthouses. One person whose movements researchers traced had a role in the technology division, which controls servers containing data for the Supreme Court.[6] Similar tactics could be used to undermine and embarrass prosecutor and public defender offices, prominent law firms, government officials, and officers at major corporations.

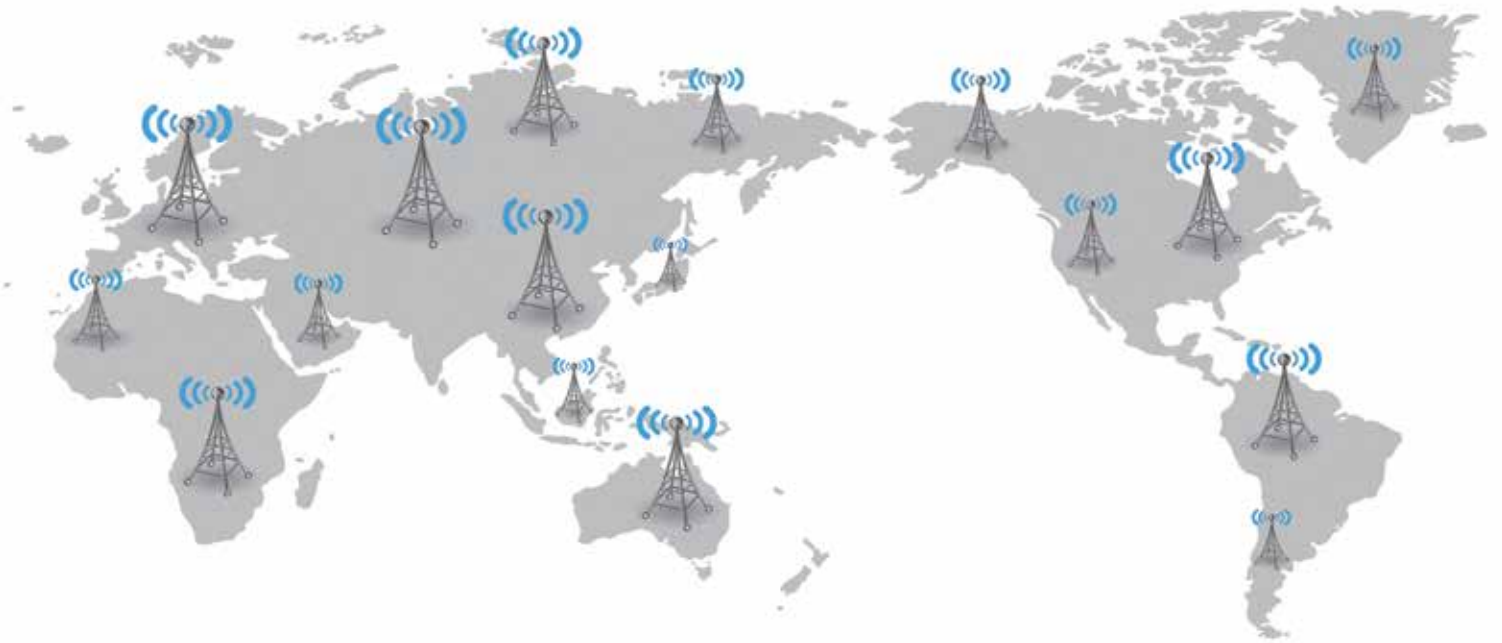
## Cell Phones in the Courthouse

The courts across the United States have adopted a variety of policies regarding cell phones, with many permitting them within courthouses. While phone use is generally prohibited within courtrooms, courthouse hallways are commonly filled with litigants on their devices. Some courts have banned the general public from bringing phones into the courthouse. However, these prohibitions have been increasingly met with pushback from the public and legal community who assert that such bans are overly burdensome for litigants, particularly pro se litigants who may rely on connectivity to aid in their cases,[7] and jurors who want to conduct personal business while they are not in jury selection, trial, or deliberations. Moreover, courts that prohibit the public and visitors from bringing phones into the courthouse often make exceptions for staff. Hence, even these courts are not signal-free.

## A Few Specific Observations After Reviewing the Location Data

In one case, researchers noticed the recorded movements of a Microsoft engineer when he visited the campus of a Microsoft competitor, Amazon. Further information obtained the following month from employment announcements within the tech industry revealed the engineer started a new job at Amazon as a manager for an Amazon drone delivery service.[8] Another set of pings noticed by the researchers was someone who spent weekdays at the Pentagon and visited a mental health and substance abuse facility multiple times.[9] Researchers also found cell phones traveling to a Church of Scientology storefront and a late-night stop at a massage parlor. This travel and location

**Judge Herbert B. Dixon Jr.** retired from the Superior Court of the District of Columbia after 30 years of service. He is a former chair of both the National Conference of State Trial Judges and the ABA Standing Committee on the American Judicial System and a former member of the Techshow Planning Board. You can reach him at Jhbdixon@gmail.com. Follow Judge Dixon on Twitter @Jhbdixon.



information is recorded in a database and often tied directly to a home address, viewable by anyone with access to the data.[10]

## Protecting Your Phone from Being Tracked Is Not Easy

The primary vulnerability allowing our phones to be turned into tracking devices is found within the phone's apps. Many of the apps we use collect and share our data with advertisers or other third parties. This includes not only those apps that require our location information for functionality, such as mapping apps, but may include apps that we would not expect to utilize location data, such as a coupon saving app.

The one-time permission requests and privacy disclosures we see when we download apps commonly go unread or are not fully understood before we accept them. When installing a new app, we almost always click "Accept" or "Agree" in response to the End User License Agreement (EULA) (our contract with the software provider) because we know from experience the app will not install on our device if we decline.

Even reading the fine print might not guarantee that your cell phone app will not transmit more information than you agreed to share. Security researchers have discovered many apps that share data beyond what users have consented to under the permission requests and privacy policies. For example, researchers found over 1,000 apps that shared data even after permission had been revoked or denied by the user. In one case, the popular weather app AccuWeather was sending location data even after users had turned location sharing off.[11] Privacy advocates have expressed concerns that more apps in the future will contain tracking technology in order to improve business data collection methods, the result of which the advocates believe will increase the threats posed.

## Beneficial Uses of Phone Tracking Can Cause Concern

Researchers can use cell phone location data to provide insights for transportation studies and government planners. The City Council of Portland, Oregon, approved a traffic and transit study to monitor millions of cell phones. Unicef announced a plan to use similar data to study epidemics, natural disasters, and demographics.[12]

The ongoing coronavirus pandemic has placed some of these benefits in the public eye. Private technology companies have used cell phone location data to create heat maps demonstrating the potential impact that disregard for social distancing and travel guidelines could have on the spread of COVID-19. One of these maps showed cell phones active on a Florida beach during spring break, as well as their subsequent movements throughout the country as the owners of these devices returned to school or home. Notwithstanding the insight this use of location data can provide, critics have pointed out that this technology poses the same risks associated with other forms of location tracking. Although user data are anonymized, users' identities can nonetheless be determined by following their movements back to their homes and other places.[13]

Apple and Google are jointly developing technology utilizing cell phone data in response to the pandemic for contact tracing. The planned software is not strictly location tracking, as it does not collect individual location pings or follow a phone's movements. Instead, whenever cell phone users with the enabled technology come into close proximity with one other, their phones collect a randomized identifier number associated with the other person. These identifier numbers change approximately every 15 minutes. Information from these person-to-person contacts are collected and stored on individual phones instead of a centralized database.

In the event someone is diagnosed with COVID-19, that person or his or her doctor can upload the identifier information

to a central system set up by a health authority, whereby anyone documented to have been in contact with the infected person will be notified. Although contact tracing appears to be more protective of users' information than forms of location tracking, critics have noted privacy concerns, including hacking. On the other side of the debate, some have argued that Apple and Google's concessions to privacy concerns will make the technology less effective than more rigid versions proposed or already deployed in other countries. For example, the ability to opt out of contact tracing will result in lower utilization.[14]

And finally, many readers know about the use of location pings in aid of law enforcement and witness investigations and to help parents keep track of their children's whereabouts. However, with each of these uses, debates continue concerning the benefits and conveniences offered versus the resulting loss of privacy.

## Final Thoughts

In *Carpenter v. United States*,[15] the Supreme Court invalidated the warrantless acquisition of stored cell site location data, a result that should have been a clarion call to the public. The cell phone has now achieved the protected status of a private residence or body appendage because it stores so much information about the owner as to deserve constitutional protection requiring the government to obtain your consent or a search warrant based on probable cause. As the *Times* stated, the private sector does not need a search warrant to request your data, and nothing prevents companies from tracking the precise movements of hundreds of millions of Americans and selling copies of that dataset to anyone who can pay the price.[16] Remember, if your cell phone is turned on, someone, somewhere is collecting information about you. ■

*Judge Dixon wishes to thank James L. Anderson, Esquire, Superior Court of D.C. Senior Judges' Law Clerk, for his assistance researching the topic of cell phone tracking technology and preparing this article.*

## Endnotes

1. Herbert B. Dixon Jr., *Is Your Internet Device Spying on You?*, 56 Judges' J., no. 2, Spring 2017, at 36, https://bit.ly/2VBmVFq.
2. Stuart A. Thompson & Charlie Warzel, *The Privacy Project: Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 19, 2019), https://nyti.ms/3geMYu4.
3. Alfred Ng, *Your Phone Talks About You Behind Your Back. These Researchers Are Listening In*, CNET (Feb. 13, 2020), https://cnet.co/3ik4xKW.
4. Thompson & Warzel, *supra* note 2.
5. Stuart A. Thompson & Charlie Warzel, *The Privacy Project: How to Track President Trump*, N.Y. Times (Dec. 20, 2019), https://nyti.ms/2NIFO59.
6. Thompson & Warzel, *supra* note 5.
7. Amanda Robert, *ABA Asks Courthouses to Reconsider Cellphone Bans*, ABA J. (Nov. 1, 2019), https://bit.ly/3dUb8s1.
8. Thompson & Warzel, *supra* note 2.
9. Thompson & Warzel, *supra* note 5.
10. Charlie Warzel & Suart A. Thompson, *The Privacy Project: Where Even the Children Are Being Tracked*, N.Y. Times (Dec. 21, 2019), https://nyti.ms/2ZpVTSx.
11. Ng, *supra* note 3.
12. Thompson & Warzel, *supra* note 2.
13. Jason Murdock, *Mobile Phone Location Data of Florida Beachgoers During Spring Break Tracked to Show Potential Coronavirus Spread*, Newsweek (Mar. 27, 2020), https://bit.ly/3inLUpt.
14. Bill Duberstein, *How Apple and Google Are Turning Your Cell Phone into a COVID-19 Tracker*, Motley Fool (Apr. 12, 2020), https://bit.ly/2BqCDwc.
15. 138 S. Ct. 2206, 201 L. Ed. 2d 507 (2018).
16. The Editorial Board, *Total Surveillance Is Not What America Signed Up For*, N.Y. Times (Dec. 21, 2019), https://nyti.ms/2BW6PPX.