Cell Phones, Social Media, and the Capitol Insurrection

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

Last year in an article about an investigation by the *New York Times* of cell site location data received from an unnamed source, I wrote "[I]f your cell phone is turned on, someone, somewhere, is collecting information about you."[1] The information proved to be a treasure trove of data about the cell phone users captured in that sweep. The reporters were able to de-anonymize so-called anonymous cell phone information and discover the movements of Pentagon officials, a Supreme Court employee, business executives, and everyday citizens. In certain instances, the cell phone data revealed visits to drug treatment centers, strip clubs, abortion clinics, and places of worship.

Little did I know that, less than a year later, I would be writing about events in Washington, D.C., where the usual suspects were still collecting cell phone user information, and cell phone users were themselves creating a wealth of additional information for law enforcement investigators to discover witnesses and participants in the insurrection event at the U.S. Capitol.

On January 6, 2021, thousands of individuals converged on the U.S. Capitol in Washington, D.C., the meeting place of the U.S. Congress. Many in the assembling crowd came to express their disagreement with the results of the 2020 presidential election. Security at the Capitol was unable to contain the advancing crowd. The siege resulted in deaths, injuries, property damage, and a nationwide law enforcement hunt for suspects and witnesses. News organizations, law enforcement agencies, and others have referred to this event as the U.S. Capitol Insurrection.

Following the events at the Capitol, the *New York Times* received a dataset that included approximately 100,000 pings for thousands of cell phones. The pings led to Washington, D.C., from surrounding and far-away states, many of which were tracked to a rally at which the president spoke and to the Capitol during the insurrection.[2] As with the previous dataset I wrote about last year, this set contained no names or phone numbers. However, the data included a new piece of information—a unique user ID for each cell phone, called a mobile advertising identifier. This ID allows data collectors to track individual cell phone users across the internet. Although this ID does not include anyone's name, it was instrumental in the *Times* reporters' investigative efforts to identify specific individuals. The reporters cross-referenced the unique mobile advertising identifiers with other databases, which facilitated the reporters' ability to find names, addresses, phone numbers, and social media accounts, including Facebook, Twitter, Instagram, TikTok, and Parler.

A mobile advertising identifier by itself is anonymous information. As an extra precaution to guard against the misuse of a cell phone owner's data, major cell phone providers have policies that limit sharing

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.

or selling user data. Additionally, users theoretically can reset or disable the identifiers within the settings of their cell phones. Unfortunately, a poorly kept industry secret is that some app developers have evaded detection of their sometimes casual observance of these rules by either disguising their actions within the app or sharing the data from the developer's server and not from the user's app. The *New York Times* reporters concluded that the idea of cell phone data being anonymous is a farce, particularly noting that several companies offer tools to any interested party to match user data with mobile advertising identifiers.

When users share data through an installed app, the developers collect the data and sell it to third parties. In turn, these parties supply marketers with information about where you live, work, and shop. A November 2017 study analyzed 300 Android apps and detected trackers in over 75 percent of the apps. A March 2018 study of 160,000 free Android apps found that more than 55 percent of the apps tried to extract user location, and 30 percent accessed the device's contact list. A 2015 analysis of 110 popular free mobile apps revealed that 47 percent of iOS apps shared geo-coordinates and other location data with third parties. These services generally operate in the background without any indication to the cell phone user.[3] In other words, you should assume your device is always tracking your movements and location through its installed apps and geolocation system. Meanwhile, once collected, the sets of data are virtually untraceable as they pass from data brokers to marketers to others; and each recipient likely has the tools to match cell phone data with the assigned mobile advertising identifier across multiple databases.

Following the Location Data

As a part of their data analysis, the *Times* reporters created a time-lapse animation to show cell phone pings as they moved to the Capitol on January 6, 2021, from a rally at which President Donald Trump spoke before a gathered crowd. The animation demonstrated that about 40 percent of the phones near the rally stage during the speeches later traveled to locations in and around the Capitol. In tying the "anonymous" ping information and unique mobile advertising identifiers to names, addresses, social networks, and phone numbers, reporters identified a significant number of individuals, including three members of one family.

The *Times* reporters' analysis of the location data revealed that many folks at the rally or the Capitol traveled along major highways from South Carolina, Florida, Ohio, and Kentucky, stopping along the way at gas stations, restaurants, and motels, dotting the route with digital breadcrumbs. The *Times* reporters matched more than 2,000 devices in the dataset with email addresses, birthdays, ethnicities, ages, social media accounts, and more.

Here is the way the *Times* reporters identified one individual. One phone was traced from inside the Capitol to a home in Kentucky. In addition, an email was matched to the phone's unique identifier. This information led to a Facebook page that displayed photos of the same person standing on the steps of the Capitol with a Facebook post stating, ". . . Yes we got inside. One girl was shot by the D.C. cops as she was knocking on the glass. She probably will die. We stopped the voting in the house." When contacted by the reporters, this person said he never entered the Capitol, and the "we got inside" meant "we the people." Recognizing the possibility that the person may have been either inside or outside the Capitol, the reporters noted that some data can be imprecise and that a few feet may be the difference between an onlooker and a participant who committed a crime.

Broadcasting Personal Activities on Social Media

In addition to the preserved digital breadcrumbs along the path traveled by cell phone users, the *Times* reporters and law enforcement officers have the benefit of pictures that users posted to social media along with descriptive text messages and videos tied to those same devices. In addition, family and friends of some individuals displayed in social media posts notified investigators about incriminating posts. Although the *Times* reporters did not discuss any law enforcement warrant requests for location data, they noted that some military agencies had acquired similar datasets the same way the information is obtained by marketing and advertising interests—by purchasing the information from data sellers.

At the time this article was submitted for publication, law enforcement authorities had arrested over 300 individuals on suspicion of their involvement in criminal activity at the Capitol. Additionally, even without law enforcement involvement, employers have taken action against some employees implicated in the Capitol insurrection based on the publicity generated by social media posts.

As publicity of the Capitol insurrection increased, some individuals who posted selfies of their presence for the occasion began deleting their posts. Regretfully, their effort to reclaim anonymity was doomed. Others had already duplicated and widely distributed the images and videos.

Cell Site Information Leads to More Evidence

A user's cell phone information may lead to other evidence of their presence at the Capitol. While awaiting its next call, a cell phone maintains its readiness to make or receive a call by "pinging" its readiness to a nearby cell tower. When making or receiving a call, a cell phone connects with a nearby cell tower. A record is created of each ping and call, and the location datasets find their way to multiple information storage sites. It is preserved in the location pings, cell site records, and cell phone app data sharing between marketers and data sellers.

In some cases, the cell site location data may be insufficient to determine if a cell phone was inside the Capitol. In those cases, law enforcement investigators may benefit from security cameras around and throughout the Capitol complex. After investigators obtain cell site data indicating that a person was near or possibly in the Capitol, surveillance videos and social media postings vastly increased the investigative opportunities to identify unknown persons and determine their various locations during the events at the Capitol.

In addition to surveillance video and social media postings, law enforcement investigators visited D.C. residents living near the Capitol. The investigators said they had everyone's phone number that pinged off the cell phone towers near the Capitol and could show the resident their location on a Google map. The investigators advised the residents they were not suspected of any wrongdoing and requested any pictures and videos the residents had taken during the hours of the insurrection.[4]

Use of Other Technologies

The myriad technology used by law enforcement investigators to identify persons present and participating in the Capitol insurrection includes facial recognition technology. Facial recognition systems work by matching a face in a video or photo with a face in a database that includes state driver's license records and criminal files. Law enforcement agencies also turn to private companies to access large databases of identified faces, including social media posts.

Sometimes, investigative efforts suffer from grainy or distant surveillance video footage captured on street surveillance, gas station, and convenience store cameras. In the Capitol insurrection case, investigators have been blessed with high-resolution photographs and videos captured by cell phones at numerous angles and the network of security cameras within and around the Capitol complex. This type of image quality enhances the effectiveness of facial recognition technology. While this technology has experienced continuing improvement, it has suffered setbacks identifying persons wearing masks. In addition, a previous article by this author noted problems associated with categorizing and identifying Black women.[5] However, as reported in one news article,

> The countless hours of video—much of it taken by the rioters themselves and uploaded to social media—also offers an ideal data set for facial recognition. Many scenes were captured from multiple angles, with good lighting, over several minutes. Few people wore masks. While facial recognition technology often struggles to reliably identify people with dark skin, the large majority of the Trump supporters who entered the Capitol on Wednesday appeared to be white.[6]

In other instances, there was no need for investigators to resort to facial recognition technology. For example, they successfully traced one person because he was wearing his company ID badge. Another person wore clothing with the name and mascot of a high school sports team in his locality. Indeed, other individuals wore clothing that clearly identified their employer by name, logo, and business telephone number.

Unregulated Accumulation and Transfer of Data

There is very little practical regulation of the data received by the *Times* reporters. The same goes for the enhancement of those data when the mobile advertising identifier is matched with other databases, allowing the addition of names, addresses, phone numbers, email addresses, social media accounts, online pictures, and more. The nearly continuous feeding of information from your cell phone apps to data collectors is purchased and sold by hedge funds, financial institutions, marketers, and other data brokers. Once the collected data find their way into this ecosystem, according to the *Times* reporters, they may be bought and sold in perpetuity.[7]

Final Thoughts

This discussion about the Capitol insurrection was not merely to explore the use of technology to identify participants in the horrific events of that day. A subtext of this discussion concerns the extent to which members of our society carry around tracking devices and make frequent worldwide broadcasts on social media platforms about their daily activities, no matter how benign or risqué. While using technology to identify and hold accountable any individual who commits a violent crime is a concept highly supported by many, others recoil at the extent to which everyday citizens voluntarily yield some part of their personal privacy for the benefits and conveniences offered by today's technologies. This discussion is about the intersection of those principles. We voluntarily share many details about our everyday activities on social media, and we consent to data sharing for the convenience of GPS route guidance, shopping, maintaining of social contact, and enjoyment of other online activities. While some in our society may have a reticence about giving up their privacy, others revel in knowing as much as possible about their friends' and relatives' daily activities.

I end with this query: What is the outer limit of our willingness to trade personal privacy for the benefits and conveniences offered by new technologies? ■

Endnotes

1. Herbert B. Dixon Jr., *Your Cell Phone Is a Spy!*, 59 Judges' J., no. 3, Summer 2020, at 34, https://bit.ly/3b0G4Ja.

2. Charlie Warzel & Stuart A. Thompson, *They Stormed the Capitol. Their Apps Tracked Them.*, N.Y. Times (Feb. 5, 2021), https://nyti.ms/3kxECRv.

3. Nicole Nguyen, *A Lot of Apps Sell Your Data. Here's What You Can Do About It*, BuzzFeed News (May 1, 2018), https://bit.ly/3b40IIw.

4. Bruce Leshan, *DC Residents Get Visits from FBI as Agents Track Cell Phones That Pinged near the Capitol*, WUSA9 (Jan. 19, 2021), https://bit.ly/3kF5i32.

5. Herbert B. Dixon Jr., *Artificial Intelligence: Benefits and Unknown Risks*, 60 Judges' J., no. 1, Winter 2021, at 42, https://bit.ly/3kuVgRY.

6. Craig Timberg, Drew Harwell & Spencer S. Hsu, *Police Let Most Capitol Rioters Walk Away. But Cellphone Data and Videos Could Now Lead to More Arrests.*, Wash. Post (Jan. 8, 2021), https://wapo.st/2NQD1KP.

7. Bijan Stephen, *Go Read This* New York Times *Investigation of the Location Tracking Data of the Capitol Rioters*, The Verge (Feb. 5, 2021), https://bit.ly/3dRJVKp.