A HOOVER INSTITUTION ESSAY

Modern-Day General Warrants and the Challenge of Protecting Third-Party Privacy Rights in Mass, Suspicionless Searches of Consumer Databases

JENNIFER LYNCH

Aegis Series Paper No. 2104

Today, more than ever, law enforcement has access to massive amounts of consumer data that allow police to essentially pluck a suspect out of thin air. Internet service providers and third parties collect and aggregate precise location data generated by our devices and their apps, making it possible for law enforcement to easily determine everyone who was in a given area during a given time period. Similarly, search engines compile and store our internet searches in a way that allows law enforcement to learn everyone who searched for specific keywords like an address or the word "bomb." In addition, DNA is now amassed in consumer genetic genealogy databases that make it possible for law enforcement to identify almost any unknown person from their DNA, even if the unknown person never chose to add their own DNA to the database.

Modern law enforcement officials very frequently conduct "suspicionless searches"—searches that are not based on individualized suspicion—on these computer databases. These searches can include the private information of millions of people unconnected to a crime on the mere possibility the police will find one person who is. Law enforcement justifies these searches by arguing that people voluntarily provide their information to third parties and agree to contracts that allow those third parties to share consumers' data with others. They also argue that the individual data points exposed through these searches are, standing alone, not all that revealing or are de-identified. Therefore, they argue, the Fourth Amendment should not restrict access to the data.

For the most part, courts are only addressing the privacy and civil liberties issues posed by these searches piecemeal through the criminal justice system. But by looking only at the data used to identify an individual defendant, society as a whole is missing a much larger looming problem: as we and our devices generate more and more data that is shared with

third parties, law enforcement now has relatively easy and inexpensive access to data that can identify and track *all* of us. Consumers would be surprised to know that their data is so readily accessible to law enforcement. However, as discussed below, it is almost impossible to opt out.

There are currently few explicit legislative or judicial checks on these kinds of searches. That has left it up to third-party data collectors to push back. In some cases, this happens, to a certain extent. For example, in response to warrants for mass location data, it appears Google has shaped search protocols to try to protect accounts.[1] However, in other cases, disclosure may be subject to the whims of the data collector. Genetic genealogy company GEDmatch allowed law enforcement access to its clients' DNA data for investigations that its founder personally felt were worthy,[2] while a similar company, FamilyTreeDNA, has welcomed law enforcement with open arms.[3] And location data brokers appear ready and willing to sell aggregated data to anyone able to buy it on the open market, including the government.[4]

This article describes the problem of suspicionless searches of consumer databases, explains the threat that these searches pose to privacy interests, argues that the legal arguments put forth by law enforcement in defense of these practices are flawed, and suggests what should be done about the problem both in courts and in the legislature. The article focuses on three versions of these suspicionless searches: reverse location warrants issued to specific internet service providers (also known as "geofence warrants"); searches of de-identified location data generated by applications on a user's device and aggregated by third-party data brokers; and forensic searches of consumer genetic genealogy databases. It will discuss the privacy implications posed by a lack of restrictions on access to the data and the challenges to developing and enforcing new restrictions. The article argues that these searches should be addressed on two fronts at once. First, for reasons I explain, suspicionless searches should be challenged as unconstitutional general warrants in the courts. And second, states and the federal government should pass laws explicitly limiting or banning police from using these technologies.

The Data, the Searches, and the Accompanying Privacy Concerns

The federal government and law enforcement have a long history of unrestrained access to large collections of data about or that can be linked to individuals. Much of this data in the past came directly from databases of public records collected by the government, such as driver, vehicle, and property records, as well as from law enforcement databases like arrest records. In general, these databases were not integrated with one another, and searching for information on an individual could be time-consuming. This created resource constraints and practical limitations on how many individuals could be investigated at any one time.

Over the past few decades, however, data aggregation by private vendors such as Palantir and Thompson Reuters and direct access to private consumer data has made database searches cheaper, easier to conduct, and quicker to produce results. In addition, the search results can offer insights—such as patterns of behavior and relationships among seemingly unconnected people—that individual law enforcement officers might not be able to identify on their own. All of this has increased the privacy ramifications of law enforcement database searches.

Courts are only now starting to address these privacy concerns. In 2018 the Supreme Court in *Carpenter v. United States*, for example, held that the Fourth Amendment required a warrant for access to historical cell site location information (CSLI) held by phone companies. The three types of data discussed in this article—geofence data, aggregated app-generated location data, and genetic genealogy data—implicate privacy rights in several key ways that are similar to CSLI. First, they allow police access to "a category of information otherwise [and previously] unknowable"—data from people who were not under suspicion at the time the data was collected.[5] Second, the technologies circumvent traditional constraints on police surveillance power and make searches "remarkably easy, cheap, and efficient compared to traditional investigative tools."[6] Finally, the data searched can be highly revealing. Location "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[7] And DNA can tell us where in the world our ancestors came from, who we are related to, our physical characteristics, and whether we are likely to get a host of genetically determined diseases. In the future, as researchers learn more about genetics, our DNA will likely reveal even more.

But these three types of data are also different from the CSLI at issue in *Carpenter* in three key ways: (1) consumers have tacitly or knowingly consented to share their data with third parties to a greater extent than CSLI (which is merely collected as a by-product of using a cell phone); (2) law enforcement does not need to start with an individual suspect or device when searching through the data; and (3) as a result of that, each search reveals or can reveal significant amounts of private and sensitive information, not just about a single individual under investigation, but also about lots of people who have no connection whatsoever to the crime. As discussed further below, these differences could require courts and legislatures to take a different approach in restricting police searches through the data.

Geofence Data

Geofence or reverse location searches allow law enforcement to identify all devices that were in a given area during a given time period in the past. Of the three types of searches

discussed in this paper, geofence searches are the only searches where law enforcement has consistently sought a warrant. However, geofence warrants are unlike typical warrants for electronic information because they do not name a specific person, device, or account. Instead, they require a provider to search its entire reserve of user location data to identify all users that fit within the geolocation and time parameters defined by the police.

So far, all geofence warrants at issue in criminal cases have involved Google, which has a particularly robust collection of location data. As Google has explained in a Virginia case, it collects location data from users of its Android devices as well as from Apple devices that use Google apps, and it stores that data in a database called "Location History" or "Sensorvault."[8] The location data draws on a variety of sensors, including GPS and Bluetooth, as well as methods for locating a device in relation to nearby cell towers and Wi-Fi networks.[9] As a result, individual location data points held by Google are often highly precise, determining where a user was at a given date and time, sometimes to within twenty meters or less.[10] Google's Location History database contains information about hundreds of millions of devices around the world, going back almost a decade.[11] Although Google emphasizes that users must opt in to Location History, opting in may be virtually automatic, especially on a mobile device running the Android operating system. Further, if users do opt in, figuring out how to later opt *out* is confusing; internal Google emails revealed even the company's own engineers were not sure how to do it.[12]

Law enforcement has used a three-step process to learn the identities of device holders (in most cases, a single warrant authorizes all three steps, so officers never need to go back before a judge). In the first step, the officer specifies the geographic area and time period of interest, using GPS coordinates to designate a "geofence" around the area. In response, Google searches its entire database of user location information—tens of millions of accounts—to extract the subset of data responsive to the warrant,[13] giving police de-identified information on all devices within the area. This step may reveal hundreds or thousands of devices, depending on the size and location of the geofence, the time of day, population density, and the length of time requested. At the next step, officers narrow the scope of their request to fewer devices and ask Google to release more, and more detailed, data for those devices, including data on where devices traveled outside the original requested geographic area and time period. This data, which still involves multiple devices, can reveal detailed travel patterns. In the final step, police review that travel data to see if they think any devices appear relevant to the crime, and then they ask for identifying information for those devices. The information Google turns over at this point includes the subscriber's name, email address, IMEI and phone numbers, service subscription, recovery SMS phone number, and recovery email address.

Reports indicate that law enforcement frequently receives large sets of data in response to geofence warrants. In one case, the Bureau of Alcohol, Tobacco, Firearms and Explosives was investigating a series of arsons in Milwaukee and served Google with two warrants that sought data for all Google customers within areas covering 3 hectares (roughly 7.5 football fields) during a total of nine hours.[14] In response, Google provided the government with identifying information for nearly 1,500 devices. Even in cases with more limited search windows, geofence warrants routinely produce information belonging to tens or even hundreds of devices.[15] This means that most of the information Google provides to law enforcement in response to a geofence warrant is for people who have no connection to the crime under investigation.

The use of geofence warrants is relatively new, reportedly dating to 2016, but they have quickly become a popular surveillance tool for the police. Google recently released a supplemental transparency report that discloses for the first time that Google received approximately 20,000 geofence warrants between 2018 and 2020. Geofence requests now constitute more than a quarter of the total number of all warrants Google received.[16] The vast majority of geofence warrant requests (95.6 percent) came from state and local police agencies, with nearly 20 percent of those coming solely from agencies in California.[17] Further, many states have ramped up their use of geofence warrants exponentially over the last couple years—in 2018, California issued 209 geofence warrant requests, but in 2020, it issued 1,909.[18] The use of geofence warrants has become widespread enough that a magistrate judge from the Northern District of Illinois recently chided the government publicly: "The government's undisciplined and overuse of this investigative technique in run-of-the-mill cases that present no urgency or imminent danger poses concerns to our collective sense of privacy and trust in law enforcement officials."[19]

Even though the use of geofence warrants is relatively new, they have already ensnared innocent individuals. In one case in Gainesville, Florida, police sought detailed information about a man in connection with a burglary after seeing his travel history in the first step of a geofence warrant.[20] However, the man's travel history was generated through an exercise tracking app he used to log months of bike rides, including a loop ride that happened to take him past the site of the burglary several times. In Ventura County, California, police arrested a man for attempted kidnapping after a geofence warrant identified him as being in the park at the same time as the alleged crime occurred—a park he visited regularly. The police eventually dropped the case, apparently due to the lack of hard evidence, but not until after they held the man in custody and published his name in an article about the investigation in the local paper.[21] While misidentifications like these could happen in traditional police investigations, they may be more likely to occur and may have more serious ramifications in the geofence context because the only link between an individual

and the crime is that the individual happened to be in the area around the time the crime occurred. This can force a suspect into the position of having to prove their innocence—that they were in the area for an unrelated purpose—rather than the police having to prove their guilt, and it increases the risk of both confirmation bias and implicit bias.

Geofence warrants have also been used to identify people in mass gatherings, including some who were likely engaged in First Amendment–protected political protests. Police requested geofence warrants to identify individuals involved in the January 6 riot at the US Capitol, in Minneapolis around the time of the protests following the police killing of George Floyd, and in the protests in Kenosha, Wisconsin following the police shooting of Jacob Blake.[22]

Aggregated App-Generated Location Data

Aggregated app-generated location data is similar to location data produced in response to a geofence warrant in that it can be used to identify people in a specific location during a specific time period. However, unlike the geofence data discussed above, which so far comes from one source, app-generated data may come from almost any application on a user's phone. App developers frequently collect users' location data as a by-product of using an app. They divorce the data from users' names and device identifiers and sell it to third-party data brokers. Those data brokers then aggregate it with millions of other users' location data and sell it to anyone who will pay for it, including other data brokers, insurers, marketers, and increasingly law enforcement. Because officers can purchase the data, law enforcement has been accessing aggregated app-generated location data without any judicial oversight at all.

Researchers are still trying to piece together exactly where this data comes from (which apps, which data brokers), how law enforcement accesses and searches the data, and which agencies are using it. There are still many questions. What researchers do know is that several federal agencies, including the IRS, Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), the Secret Service, and the US military, have all purchased access to this location data.[23] Agency contracts seem to provide law enforcement with access to "advertising identifier data, or 'AdID,' which typically includes information about where a person is located, what device they're using, what language they use, which websites they're visiting, and which websites they buy things from."[24] Although this data is not linked to a person's name and is arguably de-identified, re-identification is not difficult, given the granularity and volume of data available.[25] The *New York Times* obtained access to similar location data in 2018 and noted it "reveals people's travels in startling detail, accurate to within a few yards and in some cases updated more than 14,000 times a day."[26] The *Times* was able to identify several individuals from the dataset for its story. A Norwegian reporter used GDPR rules to obtain his own location data from a data broker

called Ventel and received 75,406 data points, collected over a period of months.[27] From this, he was easily able to plot his unique route from home to work (as well as to myriad other locations). Federal agencies have acknowledged their ability to reidentify individual users from location data, in combination with other information, suggesting they are purchasing access to the data for this purpose.[28]

Not only does this threaten individuals' privacy interests, but it could also allow for targeting based on First Amendment–protected freedoms including religion, speech, and association. For example, a handful of apps from which the military received data were targeted specifically at Muslims.[29] Further, as with geofence warrants, access to location data from individuals who were in the same place at the same time could allow police to identify political protestors and to establish relationships among people at other gatherings. Even the US military has recognized that access to this data poses a security risk; it has issued specific guidance to service members, and the NSA has recommended military and intelligence personnel disable location tracking entirely.[30]

While some specific location data-sharing apps have been identified, it may be impossible for users to truly know with whom their data is being shared and whether their data is going to the government. According to *Motherboard*, even some app developers "were not aware who their users' location data ends up with."[31] One investigation found that data passed through at least three separate entities after leaving the app and before reaching its end purchaser.[32] Even if users do learn of specific apps' data-sharing practices, it also may be difficult to impossible for users to opt out of data sharing and continue to use the apps they want, especially if data-sharing and location tracking are built into the functionality of the app.

Forensic Genetic Genealogy Searches

The police are also accessing mass consumer databases of genetic information to try to identify suspects. These searches, called forensic genetic genealogy searches (FGGS), are similar to searches of both app-generated location data and geofence data in that they allow the police to access vast troves of personal and sensitive consumer information. However, the information searched does not reveal where people have traveled in the past; instead, it can identify dozens or even hundreds of people unrelated to a crime but genetically related to a forensic DNA sample, and it has the potential to reveal large segments of people's genetic makeup. As with aggregated app-generated location data searches, the police are not seeking warrants to access this data.

Genetic genealogy sites are run by private companies and offer to help people find long-lost relatives, learn more about their families and ancestors, and identify their own traits and

health predispositions. Consumers provide extensive genetic data, either as a biological sample or in electronic format, which results in a genetic genealogy profile that is made up of more than half a million single nucleotide polymorphisms (SNPs). The sites' powerful search and algorithmic functions can identify familial relationships and estimate how close or distant those relationships may be (e.g., a direct connection, like a parent, or a very distant connection, like a fifth cousin).

There are two main types of consumer genetic databases—closed databases like Ancestry and 23andMe, where the company controls and can limit direct access to users' data and can limit search results, and open databases like GEDmatch, FamilyTreeDNA, and MyHeritage, that offer much broader access and allow users to search their own genetic data against genetic information submitted by all other site users. Open databases make it easier for consumers to search through and find other users, but they also make it easier for law enforcement to do the same. As a result, these sites are increasingly being used by law enforcement around the country to try to identify suspects in cold cases. Just like consumers, officers take advantage of the genetics companies' powerful algorithms to try to identify familial relationships, but that relationship is between existing site users and an unknown forensic DNA sample. This technique has been gaining interest after one site, GEDmatch, was used to find the "Golden State Killer," a man responsible for a series of brutal rapes and murders that plagued California in the 1970s and 1980s.[33] By 2018, FGGS had been used in at least two hundred investigations.[34]

Traditional searches through government-run DNA databases like CODIS are designed to identify an unknown DNA profile by matching it exactly to one that already exists in the database, so search results will be one or zero.[35] However, with FGGS, police do not believe the perpetrator's own DNA is in the database. Instead, they are hoping to match the unknown DNA to biological relatives who may lead them to the perpetrator. For this reason, initial search results could include hundreds of people, depending on how many genetic relatives a person has and how much or how little law enforcement decides to constrain a search.[36]

The data held in genetic genealogy websites is highly revealing. Where a DNA profile stored in a law enforcement database like CODIS typically contains only thirteen to twenty short-tandem repeat (STR) DNA markers, which are specifically chosen from noncoding (and thus less revealing) segments of DNA,[37] the SNPs in a genetic genealogy profile span the entirety of the human genome. Genetic genealogy profiles not only can reveal family members and distant ancestors, but they can also reveal a person's propensity for various diseases like breast cancer or Alzheimer's and can predict traits like addiction and drug response. Companies are even able to use genetic data to extrapolate other information about a

person like what that person looks like today or in the past. FGG search results can also be combined with other data from public records and social media to create a full picture of a person's life. And unlike a social security or driver's license number, DNA can never be changed. As with app-generated location data, the US military is concerned about the privacy implications of sharing data with genetic genealogy databases. In 2019, the military warned personnel against using at-home DNA tests, noting that the tests "could expose personal and genetic information, and potentially create unintended security consequences and increased risk to the joint force and mission."[38]

Although sites like GEDmatch state that they do not disclose a person's raw DNA to other users, they do allow users to see where, along each chromosome, uploaded genetic data may be similar to that of another user. Using that information, researchers at the University of Washington were able to learn enough to identify people's genetic traits and predispositions.[39] Also, when users perform a one-to-many search on GEDmatch, "each 'match' includes the individual's name or alias . . . email address . . . and any [family tree or inherited genetic segments] they have chosen to share."[40]

Even if we do not personally choose to disclose our own DNA to a consumer service, it is impossible to prevent biological relatives from revealing our genetic data, simply because we share genetic data with people we do not even know. Research shows 60 percent of white Americans can already be identified from a genetic genealogy database representing just 0.5 percent of the US population.[41] This same research shows that once just 2 percent of the US population has uploaded DNA, 90 percent of white Americans would be identifiable. Because of this, these sites are well on the way to creating a de facto national DNA database.

Like geofence searches, FGG searches have also already implicated innocent people who happen to have DNA markers similar to the forensic sample. For example, an earlier search in the Golden State Killer case identified a different person as the likely perpetrator.[42] In 2014, a similar search in an Idaho cold case led police to suspect an innocent man.[43]

Genetic genealogy searches can also easily be misused. As technology has become more advanced and the costs of sequencing have decreased significantly, it has become much easier to collect a DNA sample and extract a useable profile, even without a person's knowledge or consent. Where once, a useful forensic sample could only be obtained from blood, semen, or other bodily fluids, today, forensic investigators can detect, collect, and analyze trace amounts of DNA from objects merely touched by a person. This means that law enforcement can secretly collect an object used by an individual, such as a straw or beer can, extract DNA from that object, upload the profile to a genetic genealogy database, and use it to identify not just that individual but also that individual's close and distant

family members. Courts have generally been unwilling to find a Fourth Amendment protectable interest in discarded or abandoned property, even if that "property" is discarded inadvertently and unavoidably, like DNA.[44] This means there are currently no meaningful checks to prevent law enforcement from abusing this technique and using it just to generate leads or, in questionable investigations, to identify protestors or map entire families or communities.[45]

Challenges to Challenging Suspicionless Search Techniques

Despite the privacy concerns raised by these technologies, there are several reasons why it may be difficult to challenge the database searches discussed in this article through the courts. For one, it has been difficult to determine just how widely used these search techniques are. There are no meaningful reporting requirements, and law enforcement does not always seek a warrant. If these search techniques are revealed at all, it is through individual criminal investigations where defendants may have incentives not to challenge the search. Second, even if defendants *do* challenge the search, the rights of the millions of other consumers in the database may not be addressed at all. The Supreme Court has held Fourth Amendment rights are personal, so defendants cannot assert the privacy rights of others.[46] Finally, these records are in the hands of third parties, and, in many cases, consumers explicitly or tacitly consented to sharing the data. Although every justice on the Supreme Court in *Carpenter* recognized an expectation of privacy in at least some records shared with third parties,[47] the Court explicitly did not overrule the key "third party doctrine" cases: *Smith v. Maryland*[48] and *United States v. Miller*.[49] This means there is still an open question as to how the Fourth Amendment applies to various kinds of consumer data. Each of these challenges will be discussed further in this section.

Do We Know about the Search in the First Place? (The "Stingray Problem")

One frequent difficulty in challenging new law enforcement search techniques is that we don't know what we don't know—we still may not know how, when, and how frequently law enforcement is using a technology and accessing data. This problem is reminiscent of law enforcement attempts a few years ago to conceal their use of cell site simulators (CSS), known colloquially as Stingrays.[50] For years, there was no oversight of Stingray use because law enforcement agencies did whatever they could to hide their use of the devices from defendants, prosecutors, and even the courts. Police used vague terms to describe Stingrays (if they mentioned them at all), such as referring to the use of a Stingray as "receiv[ing] information from a confidential source regarding the location of the suspect,"[51] and they employed parallel construction[52] to make it seem like they used other means to identify and locate the defendant. Prosecutors even withdrew evidence and dropped prosecutions to avoid having to reveal their "source."[53] Much of this secrecy was required in nondisclosure

agreements between the FBI and state and local agencies that were drafted at the behest of private contractors.[54]

As with Stingrays, we still don't know how widespread the use of these newer suspicionless search technologies actually is and how some of these technologies truly operate. This is especially true of aggregated app-generated location data. Despite a flurry of media attention following initial stories in *Motherboard* and the *Wall Street Journal*,[55] we still don't know where exactly the data comes from, how easy it is to reidentify a specific person from the data, how widespread its use is, which agencies are using it, and whether and how it has been used in specific criminal or immigration investigations. This could be due in part to data brokers' contract terms—*Protocol* found that one company, Locate X, included a term stating its data may not be "cited in any court/investigation-related document"[56]—or law enforcement could be using parallel construction. In December 2020, after DHS failed to respond to Senate questions, the DHS Inspector General launched an investigation, which may turn up some answers.[57] The Department of Treasury Inspector General investigated the IRS Criminal Investigations unit's use of the technology, which it described in a letter to Senators Ron Wyden and Elizabeth Warren, but it didn't provide many details, perhaps because IRS did not maintain logs of use or access.[58]

There are similar challenges to learning more about geofence and genetic genealogy searches, including how and where they are being used. Although Google has now released some data on the numbers of warrants it has received, and several geofence warrants have been unsealed, there is still a lot to learn. Further, although the police seem eager to discuss their use of genetic genealogy technology in solving some cold cases, there is some evidence that police have purposefully hidden information about FGG searches from the defense.[59] Also, the lack of any countrywide reporting requirements for police use of either of these techniques means there is no easy way to track how often and where they are being used and how frequently they ensnare innocent people. Department of Justice rules from 2019 require federal agencies to track their FGG searches on an annual basis, but DOJ has yet to release any of this reporting to the public.[60]

Even if police do not explicitly hide information about their use of suspicionless search technologies, it still may be difficult to learn the full scope of that use. When police request a warrant or some other court process (which they don't currently do for FGGS or searches through app-generated location data), that process is opaque and non-adversarial. Warrants are almost always sealed before cases are brought and frequently remain sealed afterward. And even if they are unsealed, warrants are difficult to track across jurisdictions, due to a lack of standard naming conventions within PACER, the online federal court record database, and a lack of easily searchable online court records in many state jurisdictions.

And if police never find anything useful for their investigation from one of these searches, the public may never learn about it; without a successful investigation, prosecutors won't bring a case, so there may not be a forum in which the search is proactively disclosed.

Does the Defendant Have an Objectively Reasonable Expectation of Privacy in the Data?

A second obstacle to challenging or placing limits on these searches via the courts is establishing, once a person has been charged, that they have a reasonable expectation of privacy in the data or that a search protected by the Fourth Amendment has occurred. This analysis, based on Justice Harlan's concurring opinion in *Katz v. United States*, requires a determination that a person has "an actual (subjective) expectation of privacy" in the place searched that society would objectively view as reasonable.[61] However, the reasonable expectation of privacy test is challenging to implement in the technological world of today where, based on a strict application of the *Katz* test, the more we understand about how our data is collected and shared, the less we can claim we have an "objectively reasonable" expectation that our data will remain private. As the Seventh Circuit recently concluded, "The up-shot: the *Katz* test as currently interpreted may eventually afford the government ever-wider latitude over the most sophisticated, intrusive, and all-knowing technologies with lessening constitutional constraints."[62] As discussed below, this failing in the *Katz* test could doom its ability to protect privacy interests impacted by each of the suspicionless search technologies discussed in this article.

What if the defendant did not contribute their own data? (FGGS) Although most people would recognize that genetic genealogy databases contain individuals' most sensitive and private data, it could be difficult to challenge FGG searches through the criminal justice process because the individual charged with the crime did not upload their own genetic data. Instead, investigators rely on data uploaded by that person's relatives to generate leads in an investigation. If the individual who uploaded the data is not the person who will ultimately stand trial (or, put the other way, if the defendant on trial did not upload their own genetic data), courts may resist finding the defendant had a protectable privacy interest in the data. The Supreme Court has held that Fourth Amendment rights are personal; defendants cannot assert them for someone else, even if the defendant is the target of the search.[63] This means a defendant cannot easily challenge a search where all the data came from other people.

One possible way around this problem would be to argue that the defendant *does* have a personal privacy interest in the data because some of the defendant's own genetic code is in the database; the genetic data that the defendant shares with their biological relatives is what led the police to the defendant in the first place, even though that genetic code was uploaded by someone else. The Supreme Court recognized in *Carpenter* that we can still

have a privacy interest in data shared with another party, even if that data is outside our own control.[64] So, like CSLI, theoretically the Fourth Amendment should protect genetic genealogy data, even when it is shared involuntarily with a relative who has chosen to upload it to a consumer website accessible to the police. However, this argument has not yet been tested in court.[65]

How much information is enough to show a protectable privacy interest? (De-identified data, limited data points, and the "mosaic theory") *Carpenter* recognized a privacy interest in location data that is aggregated and collected over time, finding it can reflect a wealth of detail about "a person's . . . 'familial, political, professional, religious, and sexual associations.'"[66] In doing so, *Carpenter* built off the opinions of five justices in *United States v. Jones*, who recognized "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[67] This identification of a privacy interest in aggregated data that, collectively, reveals more about a person than the individual data points ever could, is frequently referred to as the "mosaic theory" of privacy.[68] The difficulty with the mosaic theory is that it is unclear how much data is needed to create a protectable privacy interest. Neither *Jones* nor *Carpenter* answered the question of how much data is enough; nor has the Court addressed the question of whether the Fourth Amendment protects privacy interests in sensitive non-locational data or de-identified data. Lower courts are still struggling with these questions today, and this could create challenges as courts grapple with the Fourth Amendment's application to searches of the three types of data discussed in this article. For example, the government has argued that geofence searches do not violate the Fourth Amendment if the geographic search area is small, and the time period of the search is short. Similarly, the government argues that access to genetic genealogy data does not raise a privacy interest because the government only uses a small amount of data and uses it merely to identify someone.

A recent case from the Fourth Circuit Court of Appeals, *Leaders of a Beautiful Struggle v. Baltimore Police Department*, demonstrates the various ways courts are approaching these questions.[69] In the case, the court addressed a police surveillance program in Baltimore, Maryland, called "Aerial Investigative Research" (AIR), by which multiple airplanes flew continuously over the city for twelve hours each day photographing about 90 percent of the city at any given time. This allowed analysts to track the public movements of people and vehicles in the hours leading up to and following a crime.[70] When the case came before a panel of the court, the panel held that the program did not violate a reasonable expectation of privacy because it was "merely a tool used to track short-term movements in public, where the expectation of privacy is lessened," and, standing alone, the program did not allow the police to identify individuals.[71] The court did not engage with plaintiffs' and *amici*'s claims that the program's data could easily be combined (and was being combined)

with other data from security cameras and license plate readers to identify individuals and vehicles.

However, when the *en banc* court reviewed the case, a majority of judges held the plaintiffs had a clear, Fourth Amendment–protected privacy interest impacted by the program.[72] The *en banc* court found *Carpenter* "appl[ied] squarely to the case" because the program tracked "'every movement' of every person outside in Baltimore," provided a "'detailed, encyclopedic'" record of where those people came and went, and allowed law enforcement to "'travel back in time' to observe a target's movements."[73] Even if the program collected data in "shorter snippets of several hours or less," that was "enough to yield 'a wealth of detail' greater than the sum of the individual trips."[74] The court also addressed the fact that individuals were not directly identifiable from the footage alone. Unlike the panel, the *en banc* court held that this was not the end of the analysis. The court held the police could use "any number of context clues [such as where people start and end their day] to distinguish individuals and deduce identity."[75] They could also cross-reference footage against other available surveillance data. For example, if police lost a vehicle during the time AIR cameras were not recording, they could turn to automated license plate readers to relocate the car.[76] This was fully in line with *Carpenter*, where the Supreme Court noted "'the Government could, *in combination with other information, deduce* a detailed log of Carpenter's movements.'"[77] The court refused to let "inference insulate a search."[78]

Leaders of a Beautiful Struggle may indicate a greater willingness of courts to engage with the types of suspicionless searches discussed in this article. However, the outcome of that engagement is far from clear, given other recent cases. For example, in *United States v. Moalin*,[79] the Ninth Circuit questioned the constitutionality of the NSA's mass telephony metadata program but stopped short of holding it unconstitutional.[80] In *Commonwealth v. McCarthy*,[81] the Massachusetts Supreme Judicial Court recognized the potential privacy implications of automated license plate reader (ALPR) data collection but did not find a search of the ALPR database violated the state constitution.[82] It noted that ALPRs placed near sensitive locations can "reveal . . . an individual's life and associations" and "allow the police to reconstruct people's past movements without knowing in advance who police are looking for, thus granting police access to 'a category of information otherwise [and previously] unknowable.'"[83] The court also noted that, "[w]ith enough cameras in enough locations, the historic location data from an ALPR system in Massachusetts would invade a reasonable expectation of privacy and would constitute a search for constitutional purposes."[84] However, the court held that it couldn't assess how privacy invasive the technology was in the case because the defendant had not introduced enough evidence of widespread ALPR collection by the government; all the court had in front of it was that the

police had gathered data from cameras on two bridges over a limited period of time, and that wasn't enough.[85]

Similarly, in *United States v. Hammond*,[86] the Seventh Circuit held that real-time cell phone tracking wasn't a search because the data collected covered a "matter of hours" rather than one hundred twenty-seven days at issue in *Carpenter* and "crucially . . . [did] not provide a 'window into [the] person's life, revealing . . . his familial, political, professional, religious, and sexual associations' to the same, intrusive degree [as in *Carpenter*.]"[87] In *United States v. Tuggle*,[88] a panel of the Seventh Circuit held that eighteen months of pole camera surveillance of the front of a person's home did not violate the Fourth Amendment, in part because, while "the stationary cameras placed around [the defendant's] house captured an important sliver of [his] life . . . , they did not paint the type of exhaustive picture of his every movement that the Supreme Court has frowned upon."[89]

Similarly, in *Sanchez v. Los Angeles Department of Transportation*,[90] the district court held the City of Los Angeles's collection of mass, citywide shared mobility device (scooter and bike rental) data did not implicate the Fourth Amendment.[91] Although the city is collecting real-time location data on the start and endpoints of all shared bike and scooter rides and the path of all rides on a twenty-four-hour delay, the court refused to recognize a privacy interest in the data because it is de-identified. The court said, "[o]bviously, a person does not have a reasonable expectation of privacy over information that cannot even be connected to her."[92]

Outside the context of location, courts have also contended with the question of how much data is enough. For example, in *Maryland v. King*, the Supreme Court addressed the collection of DNA from all people in Maryland arrested for felony offenses.[93] Mr. King argued that DNA can reveal sensitive and private information about people and therefore the government's collection of DNA from individuals presumed innocent violated the Fourth Amendment. However, the Court refused to engage with that argument, holding that, even though the government had access to *all* of the arrestee's genetic information contained in the DNA sample it collected, that was irrelevant to the analysis because the government only relied on the CODIS core loci, which were from noncoding regions that did not reveal genetic traits.[94] However, a more recent Supreme Court case could indicate a newer willingness to accept as part of the analysis the government's mere *ability* to access more data, not just the smaller portion of data it may rely on to prove its case. In *Birchfield v. North Dakota*,[95] the Court held that the Fourth Amendment did not allow the warrantless collection of a blood sample from an allegedly intoxicated driver because "blood tests are significantly more intrusive [than breath tests]."[96] It didn't matter to the Court that the sample was used merely to test for blood alcohol content because:

> [A] blood test, unlike a breath test, places in the hands of law enforcement authorities a sample that can be preserved and from which it is possible to extract information beyond a simple BAC reading. Even if the law enforcement agency is precluded from testing the blood for any purpose other than to measure BAC, the potential remains and may result in anxiety for the person tested.[97]

In each of these cases, the government had access to significant quantities of data (or at least had the ability to access it). However, in *McCarthy*, *Hammond*, *Tuggle*, and *King*, the courts were unconvinced that the quantity of data was sufficient to create a protectable privacy interest, and in *Sanchez* and the *Leaders of a Beautiful Struggle* panel opinion, the judges did not accept that people have any expectation of privacy in de-identified data at all. The shortsighted analysis exemplified by these cases could make it difficult to challenge the mass, suspicionless searches discussed in this article, as each, to a certain extent involves de-identified data or the use of limited amounts of data. However, *Birchfield* and the *en banc Leaders of a Beautiful Struggle* opinion may begin to provide a road map for a path forward.

What if consumers knowingly disclose their data to third-party companies? (Third-party doctrine, terms of service, consent, and law enforcement access to data on the open market) Courts may also have difficulty finding a protectable privacy interest in the types of data addressed in this article because all consumer data is shared with third parties; the police don't need to go directly to the consumer to get it. Also complicating matters—the police are able to purchase access to aggregated app-generated location data and to access genetic genealogy data without restrictions, just like other, non-law enforcement users.[98] The majority opinion in *Carpenter* explicitly did not overrule the third-party doctrine, and law enforcement continues to argue that defendants lack a reasonable expectation of privacy in data in the hands of third parties.[99]

In *Carpenter*, the Supreme Court carved out an exception to the third-party doctrine for certain consumer location data held by phone companies, explaining that cell phone location information "is not truly 'shared' as one normally understands the term," particularly because a phone "logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up."[100] However, the Court also emphasized that its holding was "a narrow one,"[101] and it remains to be seen how narrow or broad a carve-out the Court actually created. Justice Kennedy noted in his dissent that the majority's "reinterpretation of *Miller* and *Smith* will have dramatic consequences for law enforcement, courts, and society as a whole."[102] But so far, lower courts seem unwilling to push the limits of *Carpenter* on data shared with third parties. In cases with facts somewhat similar to *Carpenter*, such as cases involving location data, some lower courts have found the third-party doctrine does not apply. For example, in *United States v. Diggs*,[103] the

government argued the defendant could not show an expectation of privacy in GPS location data generated by the car he was driving because the data was collected by the car company pursuant to an agreement his wife signed when she bought the car, and the company voluntarily disclosed it to the police.[104] The court disagreed, holding "[t]he GPS data at issue here fits squarely within the scope of the reasonable expectation of privacy identified by the *Jones* concurrences and reaffirmed in *Carpenter*."[105] Similarly, some courts have also applied *Carpenter* to real-time cell phone location data.[106]

However, where facts diverge from *Carpenter*, even slightly, courts have been quick to hold the third-party doctrine still applies. In *Sanchez v. Los Angeles Department of Transportation*,[107] the court distinguished the compelled collection of de-identified rental scooter location data from CSLI, refusing to find a protectable privacy interest and holding "[w]hen someone chooses to use a rental scooter service for transportation, she assumes the risk that a technology company will be tracking her location for so long as she rides a scooter belonging to that company."[108] In cases involving facts outside the context of location data, courts have been even more resistant to weakening the third-party doctrine. In *United States v. Trader*,[109] the Eleventh Circuit held *Carpenter* does not apply to subscriber information like email addresses and internet protocol addresses, holding these are business records disclosed during ordinary use of the internet and fall within the third-party doctrine.[110] In cryptocurrency cases, courts have held *Carpenter* does not extend to data associated with cryptocurrency purchases because the "nature of the information on the Bitcoin blockchain and the voluntariness of the exposure weigh heavily against finding a privacy interest in an individual's information."[111]

And, although courts have yet to address the issue, federal and local agencies have taken the position that the Fourth Amendment also does not preclude access to data available on the open market because consumers have explicitly or implicitly chosen to share that data with others by "agreeing" to a company's terms of service. Similarly, agencies have argued that they are not required to seek any court process before accessing genetic genealogy data because consumers have chosen to share this data with third-party companies and to make it available without restrictions to other site users.[112]

However, courts might, in the future, be convinced to further limit the third-party doctrine and cabin the scope of data-sharing agreements between consumers and companies, given the sheer volume and sensitivity of data available on individuals and the ubiquity of these non-negotiated agreements. As noted above, in *Carpenter*, every Justice suggested that the Fourth Amendment protects the content of at least some records stored with third parties. The Ninth Circuit in *Moalin* seemed poised to find the NSA's bulk telephony metadata collection program unconstitutional based on the sheer quantity of data and the

government's ability to analyze it.[113] And in *United States v. Byrd*,[114] the Court rejected the argument that Fourth Amendment rights can be determined by private form contracts.[115] The Court held that drivers have a reasonable expectation of privacy in a rental car even when they are driving that car in violation of the rental agreement.[116] Car-rental agreements, wrote the Court, are filled with "long lists of restrictions" that have nothing to do with a driver's reasonable expectation of privacy in the rental car; what matters more is if the driver otherwise has "lawful possession of and control over the car."[117] Given *Byrd*, one could argue similarly that technology companies' terms of service should not impact whether someone otherwise has a reasonable expectation of privacy in data shared with third parties.[118]

How to Address These Challenges

Carpenter laid out a much-discussed multifactor approach to determining a Fourth Amendment protectable privacy interest in data shared with third parties and collected in mass databases. This approach considers "intimacy, comprehensiveness, expense, retrospectivity, and voluntariness."[119] It is possible to apply *Carpenter* to other types of data, but these qualities do not map cleanly to protect the data discussed in this article. For example, few would argue that our genetic data does not hold the "privacies of life,"[120] and researchers have shown that within a few years it will be possible to identify almost all white Americans through consumer genetic databases. Therefore, genetic data seems to meet *Carpenter*'s intimacy and comprehensiveness factors. Further, access to many genetic genealogy databases is inexpensive or free, and genetic sequencing costs have dropped dramatically over the last twenty years. These databases also allow for retrospective searches—the data has already been collected so law enforcement does not need to go out and seek genetic data to build its own database for each new criminal investigation. So genetic data also seems to meet *Carpenter*'s expense and retrospectivity factors.

However, voluntariness could create a barrier to a clear application of *Carpenter* to consumer genetic data. First, consumers willingly and knowingly upload and share their genetic data, in some cases explicitly opting in to sharing it with law enforcement. And, unlike with CSLI, there is less of an argument that people need to do so to live in the modern world. Second, almost the flip side to this same coin, the suspect did not upload their own genetic data to a genetic genealogy database, so the disclosure of segments of their shared genetic code was not voluntary. But because of that, they may also have a hard time arguing they have a privacy interest in the data at all.[121]

Similarly, geofence and app-generated location data searches meet some of the *Carpenter* factors but not others. Like cell site location information, they allow the police to "travel back in time to retrace a person's whereabouts."[122] However, the government has argued that

access to aggregated app-generated location data does not implicate the Fourth Amendment because users voluntarily share data with third parties by using apps that are not necessary to modern life. And, they argue, the data is not necessarily intimate because it is (theoretically, at least) anonymized. Similar arguments have been applied to geofence data, which is the one type of data discussed in this article for which law enforcement already gets a warrant. For geofence data, law enforcement argues that it is only seeking a limited slice of data that users voluntarily share with Google, and therefore the data is neither comprehensive nor intimate.[123]

Given these challenges with applying *Carpenter* to law enforcement access to the types of data discussed in this article, these searches require a different approach. This article proposes two: judicial and legislative. If the searches are challenged in court, courts should treat them as general searches that violate the Fourth Amendment. However, as these searches may never reach a court, legislatures should pass strict and clear limits on law enforcement access to the data or ban access entirely.

These Searches Are Unconstitutional General Warrants in Violation of the Fourth Amendment

Stepping back from *Carpenter*, it is important again to highlight the main characteristic of these searches: they do not require individualized suspicion. For each of these searches, law enforcement lacks predicate facts to link any individual person to the crime under investigation. Instead, these are dragnet searches through the data of everyone in a database. The fact that the searches start without a specific suspect makes them similar to the general warrants with which all Fourth Amendment scholars are familiar.

The Fourth Amendment was drafted to preclude general warrants. In the American colonies, British agents used general warrants, also known as "writs of assistance," to conduct broad searches for smuggled goods that were limited only by the agents' own discretion.[124] Colonists' opposition to these searches was "one of the driving forces behind the Revolution itself."[125] In addition to the American colonists' own experiences, two important English cases involving general warrants—*Wilkes v. Wood*[126] and *Entick v. Carrington*[127]—directly inspired the Fourth Amendment. In *Wilkes*, Lord Halifax issued a general warrant authorizing the seizure of papers from people suspected of libel without specifying which houses or businesses to search and without naming anyone charged.[128] Officers arrested nearly fifty people, ransacking their houses and seizing their papers in the process.

In *Entick*, the King's agents were authorized to search for the author and anyone related to a publication deemed seditious, as well as to seize Entick's books and papers. However,

the warrant did not specify where to search or provide any foundation to believe evidence of criminal conduct would be found at any particular location. At the agents' discretion, they raided, searched through, and carted away papers from many homes and businesses, including Entick's. In *Wilkes*, the court held "this was 'a ridiculous warrant against the whole English nation'" and awarded damages.[129] In *Entick*, the court declared the warrant unlawful. After both cases, "the House of Commons passed two resolutions condemning general warrants, the first limiting its condemnation to their use in cases of libel, and the second condemning their use generally."[130]

These cases were so important and abhorrent to the founders that several state constitutions from the original thirteen colonies outlaw general warrants explicitly, while the remainder outlaw them by description, requiring particularity, specificity, or including some other language indicating the need for individualized suspicion.[131] The Fourth Amendment was drafted against this backdrop. Its text "reflect[s] the determination of those who wrote the Bill of Rights that the people of this new Nation should forever 'be secure in their persons, houses, papers, and effects' from intrusion and seizure by officers acting under the unbridled authority of a general warrant."[132] As Justice Scalia noted in his dissent in *Maryland v. King*, "No matter the degree of invasiveness, suspicionless searches are *never* allowed if their principal end is ordinary crime-solving."[133]

Mass, suspicionless searches of consumer data have direct parallels to the general warrants that inspired the Fourth Amendment. Whether conducted with a warrant (as with geofence searches) or without (as with searches of aggregated app-generated location data and genetic genealogy data), mass suspicionless searches through consumer data could be described as digital analogues to arrest warrants that authorize officers to search every house in a town simply on the chance that someone connected with a crime might be located inside one. The searches fail the Fourth Amendment's requirements, which state that a search should be particularized, supported by probable cause, and generally be conducted pursuant to a warrant. The searches lack particularity because they do not identify any specific person or profile to be searched. They are overbroad because they encompass intensely private data from potentially millions of people. And these searches cannot be supported by probable cause because there are no facts indicating that any particular consumer in the database was in any way personally connected to the crime. The mere possibility that the perpetrator may have been sharing their own location data at the time of the crime or may share some genetic data with the genetic genealogy site users should not be sufficient to support probable cause to search through *all* users' data.[134]

Several recent court opinions have agreed with this approach. For example, in *Leaders of a Beautiful Struggle*, the *en banc* Fourth Circuit held, the AIR "program is like a 21st century

general search, enabling the police to collect all movements, both innocent and suspected, without any burden to 'articulate an adequate reason to search for specific items related to specific crimes.'"[135] Similarly, several magistrate judges—who, by virtue of their role, are the first to review most warrant applications—recently blocked several geofence warrants, likening them to general warrants and holding they lacked probable cause and were overbroad.[136] As one judge noted, even if the government had established probable cause that a single cell phone user within a geofenced area might have committed a crime, that was insufficient to establish probable cause to believe *all* devices in the area were connected to the crime as well. Narrowing the time period and geographic scope of the request would not cure this deficiency. As the court stated:

> the geographic scope of [the] request in a congested urban area encompassing individuals' residences, businesses, and healthcare providers is not "narrowly tailored" when the vast majority of cellular telephones likely to be identified in this geofence will have nothing whatsoever to do with the offenses under investigation.[137]

Similar to *Ybarra v. Illinois*,[138] the government was seeking unlimited discretion to search *all* users' devices in a given area—including users who merely walked along the sidewalk next to a business or lived in the residences above it—based on nothing more than their proximity to a suspected crime.[139]

Like the original general warrants and writs of assistance, these searches leave to law enforcement's discretion "the decision as to which persons" to pursue.[140] By starting with a broad search that seeks information from *all* accounts, they give the police unrestricted license to search each of these accounts and then, without clear limiting criteria or further judicial oversight, to conduct a more detailed search of a subset of those accounts. With a proper search warrant, "[n]othing is left to the discretion of the officer."[141] That is not the case with these database searches.

These searches are also arguably broader than colonial-era general warrants, because they are not necessarily limited by physical geography or officer manpower.[142] As Google notes, because it does not retain location data in discrete groups labeled by date, time, or particular geographic areas, reverse location warrants require it to search through *all* of its users' data—tens of millions of user accounts—just to extract the subset of location information responsive to a warrant.[143] Similarly, when officers search a genetic genealogy site, they search the entire database of millions of site users' genetic data. Searches like this were not conceivable, much less possible, at the nation's founding. These searches therefore "give[] police access to a category of information otherwise unknowable."[144]

The breadth of the searches discussed in this article, coupled with the absence of specific information about the accounts or devices to be searched, should render them invalid under the Fourth Amendment. However, a general search argument only helps if a defendant can get into court in the first place (and if the defendant happens to have a decent lawyer and gets a sympathetic judge). Given the challenges discussed above—including the dearth of information about how and how frequently these searches are used, the standing problems with challenging FGG searches, and how slow the courts are to act—a judicial remedy cannot be the only solution; legislatures should consider restricting these searches by statute as well.

Legislative Approaches

Recently, there have been several attempts at the state and federal levels to ban or restrict suspicionless searches of consumer data. This section will briefly discuss three bills, including a New York bill that would prohibit all geofence searches,[145] a federal bill that would limit government searches of aggregated app-generated consumer location data,[146] and a Maryland bill, recently passed into law, that places strict limits on genetic genealogy searches.[147]

New York's proposed legislation would ban reverse location searches. New York's bill, Assembly Bill A84A,[148] goes the furthest of the three bills and would ban police use of reverse location searches entirely. The bill defines reverse location data broadly as:

> records or information pertaining to electronic devices or their users or owners, whose scope extends to an unknown number of electronic devices present in a given geographic area at a given time as measured via global positioning system coordinates, cell tower connectivity, Wi-Fi data and/or any other form of location detection.[149]

The bill would prohibit the government from accessing reverse location data in any way, including by court order, asking a company to provide the data voluntarily, purchasing the data, or obtaining the data from another government entity not covered by the law (such as a federal agency). And it includes both a suppression remedy and a private right of action.[150] If enacted, this bill would ban law enforcement from sending geofence warrants directly to Google and also from purchasing app-generated location data from third-party data brokers.

Given the analysis above, comparing the suspicionless searches discussed in this article to general warrants, some would argue that any legislation should ban all such searches entirely, as New York's would do. However, others would argue that some restrictions are better than the status quo, which is almost no restrictions at all. Legislation that bans a law enforcement technique or technology can be controversial and can face strong opposition from police associations and lobbying organizations, especially if police are already using the technology.

So far, several cities around the country have successfully enacted bans on police use of face recognition,[151] but full bans have not yet been enacted at the federal level and have had limited success at the state level.[152] It is possible that states and local legislatures will have success enacting bans on reverse location searches, like the bill introduced in New York. However, face recognition bans have had the full, multiyear support of national civil rights and privacy organizations like the Electronic Frontier Foundation and ACLU, as well as local and community organizations like ACLU's affiliates,[153] Oakland Privacy,[154] Restore the Fourth Minnesota,[155] and many others. It remains to be seen whether bans on suspicionless searches, like New York's bill, will garner the same strong and sustained support. A similar ban, previously introduced in Utah, has since been watered down and now would require a warrant for reverse location searches.[156]

The federal "Fourth Amendment is Not For Sale Act" would prohibit police purchase of location data. The federal "Fourth Amendment is Not For Sale Act," introduced by Senator Ron Wyden, takes a different approach to the problem of reverse location searches.[157] The bill would amend sections of the Electronic Communications Privacy Act (ECPA) and the Foreign Intelligence Surveillance Act (FISA) to prohibit federal law enforcement and intelligence agencies from purchasing location data (and other types of data) on people in the United States and Americans abroad. Unlike New York's bill, it would not ban the *use* of this data; it would merely require law enforcement to first obtain a court order, just as they would for similar types of data already covered by ECPA.

The federal bill is still relatively broad in the types of data to which it applies, however. It would apply regardless of whether the government obtained the data from an entity that collected it directly from the consumer (such as an app developer or a company like Google) or from an entity that obtained the data indirectly (such as a data broker like Ventel), and it would apply even if the entity obtained the data in violation of terms of service or in a way that is "inconsistent with the privacy policy," such as through scraping or hacking.[158] It would require law enforcement to get a court order, consistent with existing ECPA rules, to compel data brokers to disclose data, and it would mandate that courts must "apply the most stringent [federal statutory or constitutional] standard[s]" to law enforcement requests for data.[159] The bill requires the Attorney General to develop minimization procedures that would limit the acquisition and retention of data and prohibit the dissemination of data that was acquired in violation of the statute. It would also mandate that the government could not use any data acquired in violation of the act as evidence in any proceeding and similarly could not use evidence derived from data acquired in violation of the act.

By merely amending ECPA and FISA to extend existing protections to cover similar data obtained in new ways, the Fourth Amendment is Not For Sale Act does not seem like it

would be controversial or difficult to enact into law. So far, the bill has bipartisan support and twenty cosponsors in the Senate,[160] and a companion bill has been introduced in the House.[161] However, while this strong support is promising, it is unclear whether the bill will be enacted into law. Attempts to amend ECPA in the past—even bills with overwhelming Congressional support—have failed to make it out of Senate committee.[162]

Maryland's new law limits FGG searches. Maryland *has* passed a law restricting suspicionless searches, however. In May 2021, the state enacted a law that places strict limits on police use of FGGS. This new law could be a model for similar legislation in other states.

The bill began as a ban on FGGS in 2019 but was unsuccessful.[163] When the state senator sponsoring the bill reconfigured it to, instead, allow FGGS but require a warrant, and worked with diverse stakeholders to get consensus support behind the bill (including support, or at least non-opposition, from law enforcement), it passed both legislative houses with little opposition. It is now the strongest law on FGGS in the country.[164]

The new Maryland law is very broad and covers much more than FGGS. It requires judicial authorization for FGGS and places strict limits on when and under what conditions law enforcement officers may conduct FGGS. For example, in Maryland, now, FGGS may only be used in cases of rape, murder, felony sexual offenses, and criminal acts that present "a substantial and ongoing threat to public safety or national security."[165] Before officers can pursue FGGS, they must certify to the court that they have already tried searching existing, state-run criminal DNA databases like CODIS, that they have pursued other reasonable investigative leads, and that those searches have failed to identify anyone. And FGGS may only be used with consumer databases that have provided explicit notice to users about law enforcement searches and sought consent from those users. These meaningful restrictions ensure that FGGS does not become the default first search conducted by law enforcement and limits its use to crimes that society has already determined are the most serious.

Maryland's law regulates other aspects of genetic investigations as well. For example, it places strict limits on and requires judicial oversight for the covert collection of DNA samples from both potential suspects and their genetic relatives. This is an important protection because officers frequently and secretly collect and search DNA from free people in criminal investigations involving FGGS, and courts have yet to hold the Fourth Amendment prohibits these searches.[166] The new Maryland law also mandates informed consent in writing before officers can collect DNA samples from third parties and precludes covert collection from a third party who has refused to provide a sample. It requires destruction of DNA samples and data when an investigation ends. It also requires licensing for labs that conduct DNA sequencing used for FGGS and for individuals who perform genetic

genealogy. It creates criminal penalties for violating the statute and a private right of action with liquidated damages so that people can enforce the law through the courts. It requires the governor's office to report annually and publicly on law enforcement use of FGGS and covert collection. Finally, it states explicitly that criminal defendants may use the technique as well to support their defense (but places similar restrictions on a defendant's use).

Maryland's law and its process for getting the law enacted—working behind the scenes to get support from diverse stakeholders before introducing the bill—could serve as a model for other states trying to place limits on each of the suspicionless database searches discussed in this article.[167] Until courts have a chance to address these searches, statutory protections like the legislation discussed above are an important way to reinforce our constitutional rights.

Conclusion

As the Supreme Court in *Carpenter* found with CSLI, law enforcement's position on mass, suspicionless searches of consumer data "fails to contend with the seismic shifts in digital technology" that make possible the tracking and identification of not just individual defendants but of everyone else as well, "not for a short period but for years and years."[168] Search warrants "are fundamentally offensive to the underlying principles of the Fourth Amendment when they are so bountiful and expansive in their language that they constitute a virtual, all-encompassing dragnet" of information "to be seized at the discretion of the State."[169] Searches through the data discussed in this article—where the only information the police have is that a crime has occurred—are no less a "dragnet." They provide unprecedented access to the kinds of private and sensitive information about individuals and communities that the Court highlighted in *Carpenter*, and they will inevitably implicate innocent people. Given all this, both judicial *and* legislative constraints, like those discussed in this article, are necessary to prevent the sort of "general, exploratory rummaging" the Fourth Amendment was intended to forestall.[170]

NOTES

Many thanks to Corynne McSherry, Jennifer Granick, and Jack Goldsmith for their helpful feedback on this paper.

1 *See* Br. of Amicus Curiae Google LLC in Supp. of Neither Party Concerning Def.'s Mot. to Suppress Evid. From a "Geofence" General Warrant at 12, United States v. Chatrie, No. 19-cr-00130 (E.D. Va. Dec. 23, 2019), ECF No. 73 [hereinafter "Google Amicus"].

2 *See* Peter Aldhous, *The Arrest of a Teen on an Assault Charge Has Sparked New Privacy Fears about DNA Sleuthing*, Buzzfeed (May 14, 2019, 10:15 PM), https://www.buzzfeednews.com/article/peteraldhous/genetic-genealogy-parabon-gedmatch-assault.

3 *See* Amy Dockser Marcus, Customers Handed Over Their DNA. *The Company Let the FBI Take a Look.*, Wall St. J. (Aug. 22, 2019, 12:26 PM), https://www.wsj.com/articles/customers-handed-over-their-dna-the-company-let-the-fbi-take-a-look-11566491162.

4 *See, e.g.*, Joseph Cox, *How an ICE Contractor Tracks Phones Around the World*, Vice (Dec. 3, 2020, 6:35 AM), https://www.vice.com/en/article/epdpdm/ice-dhs-fbi-location-data-venntel-apps.

5 *See* Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

6 *Id.*

7 *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400, 415 [2012] [Sotomayor, J., concurring]).

8 *See* Google Amicus, *supra* note 1, at 1–2; Jennifer Lynch, *Google's Sensorvault Can Tell Police Where You've Been*, Elec. Frontier Found. (April 18, 2019), https://www.eff.org/deeplinks/2019/04/googles-sensorvault-can-tell-police-where-youve-been.

9 *See* Google Amicus, *supra* note 1, at 77.

10 *See id.*; Decl. of Marlo McGriff at ¶ 12, United States v. Chatrie, No. 19-cr-00130 (E.D. Va. Mar. 11, 2020), ECF No. 96-1, https://www.eff.org/document/us-v-chatrie-google-declaration-geofence-warrant [hereinafter "Google Decl."].

11 *See* Jennifer Valentino-DeVries, *Tracking Phones*, *Google Is a Dragnet for the Police*, N.Y. Times (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html.

12 *See* Alfred Ng, *Google Court Docs Raise Concerns on Geofence Warrants, Location Tracking*, c|net (Aug. 26, 2020, 3:27 PM), https://www.cnet.com/news/google-court-docs-raise-concerns-on-geofence-warrants-location-tracking.

13 *See* Google Amicus, *supra* note 1, at 12–13; Google Decl., *supra* note 10, at ¶ 13.

14 *See* Thomas Brewster, Google Hands Feds 1,500 Phone Locations in Unprecedented "Geofence" Search, Forbes (Dec. 11, 2019, 7:45 AM), https://www.forbes.com/sites/thomasbrewster/2019/12/11/google-gives-feds-1500-leads-to-arsonist-smartphones-in-unprecedented-geofence-search.

15 *See, e.g.*, Defendant Okello Chatrie's Motion to Suppress Evidence from a "Geofence" General Warrant at 6, United States v. Chatrie, No. 19-cr-00130 (E.D. Va. Oct. 29, 2019), ECF No. 29 (warrant produced identifiers belonging to 19 devices).

16 Google, Supplemental Information on Geofence Warrants in the United States 1 (2021), https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf.

17 *Id.* at 2.

18 *Id.* (follow "Download supplemental data as a CSV" hyperlink).

19 Mem. Op and Order, In the Matter of the Search of: Info. Stored at Premises Controlled by Google, No. 1:20-mc-00297 (N.D. Ill. July 8, 2020), ECF No. 7, https://www.eff.org/document/re-search-information-stored-premises-controlled-google-no-20-m-297-de-4-nd-ill-july-8-2020 [hereinafter July 8 Mem. Op. and Order].

20 Jon Schuppe, *Google Tracked His Bike Ride Past a Burglarized Home. That Made Him a Suspect*, NBC News (Mar. 7, 2020, 6:22 AM), https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761.

21 *See* Alex Wilson, *Charges Dropped in Attempted Kidnapping*, Camarillo Acorn (Apr. 23, 2021), https://www.thecamarilloacorn.com/articles/charges-dropped-in-attempted-kidnapping-arrest. I consulted with the defense attorney on this case.

22 Drew Harwell & Craig Timberg, *How America's Surveillance Networks Helped the FBI Catch the Capitol Mob*, Wash. Post (April 2, 2021), https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests

-technology-fbi-privacy; Zach Whittaker, *Minneapolis Police Tapped Google to Identify George Floyd Protesters*, TechCrunch (Feb. 6, 2021), https://techcrunch.com/2021/02/06/minneapolis-protests-geofence-warrant; Russell Brandom, *How Police Laid Down a Geofence Dragnet for Kenosha Protestors*, The Verge (Aug 30, 2021), https://www.theverge.com/22644965/kenosha-protests-geofence-warrants-atf-android-data-police-jacob-blake.

23 *See* Joseph Cox, Secret Service Bought Phone Location Data from Apps, Contract Confirms, Vice (Aug. 17, 2020, 9:00 AM), https://www.vice.com/en/article/jgxk3g/secret-service-phone-location-data-babel-street; Charles Levinson, *Through Apps, Not Warrants, "Locate X" Allows Federal Law Enforcement to Track Phones*, Protocol (March 5, 2020), https://www.protocol.com/government-buying-location-data.

24 Hamed Aleaziz & Carlone Haskins, *DHS Authorities Are Buying Moment-by-Moment Geolocation Cellphone Data to Track People*, Buzzfeed (Oct. 30, 2020, 6:19 PM), https://www.buzzfeednews.com/article/hamedaleaziz/ice-dhs-cell-phone-data-tracking-geolocation.

25 *See* Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, 3 Nature Sci. Reps., no. 1376, 2013 at 1 (2013), http://www.nature.com/articles/srep01376.

26 Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. Times (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

27 *See* Martin Gundersen, *My Phone Was Spying on Me, so I Tracked Down the Surveillants*, NRKbeta (Dec. 3, 2020), https://nrkbeta.no/2020/12/03/my-phone-was-spying-on-me-so-i-tracked-down-the-surveillants.

28 Aleaziz & Haskins, *supra* note 24.

29 *See, e.g.*, Joseph Cox, *How the US Military Buys Location Data from Ordinary Apps*, Vice (Nov. 16, 2020, 10:35 AM), https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.

30 *See* Byron Tau, *The Ease of Tracking Mobile Phones of US Soldiers in Hot Spots*, Wall St. J. (Apr. 26, 2021, 5:30 ET), https://www.wsj.com/articles/the-ease-of-tracking-mobile-phones-of-u-s-soldiers-in-hot-spots-11619429402.

31 *See* Cox, *supra* note 29.

32 *See* Gundersen, *supra* note 27.

33 *See* Thomas Fuller, *How a Genealogy Site Led to the Front Door of the Golden State Killer Suspect*, N.Y. Times (Apr. 26, 2018), https://www.nytimes.com/2018/04/26/us/golden-state-killer.html.

34 *See* Megan Molteni, *The Future of Crime-Fighting Is Family Tree Forensics*, Wired (Dec. 26, 2018, 8:00 AM), https://www.wired.com/story/the-future-of-crime-fighting-is-family-tree-forensics.

35 Some states allow familial searches through the state-run DNA database, but that is not the database's main purpose, and those states have clear restrictions on using government-run databases for such a search. *See, e.g.*, Cal. Dep't of the Att'y Gen., Memorandum of Understanding: DOJ Familial Searching Protocol, https://oag.ca.gov/sites/all/files/agweb/pdfs/bfs/fsc-mou-06072019.pdf (describing California's familial search requirements). Other states, like Maryland, prohibit familial searches entirely. *See* Tim Prudente, *Maryland to Limit Police Use of Genealogy Websites*, Wash. Post (June 7, 2021, 7:33 PM), https://www.washingtonpost.com/local/legal-issues/maryland-limit-police-genealogy-websites/2021/06/07/179b5a3c-c7a2-11eb-a11b-6c6191ccd599_story.html.

36 Law enforcement may choose to make an initial search as broad as possible to include distant relatives such as third and fourth cousins, but such a search could include significantly more people. Also, because DNA recombination is random, the more distant a genetic relationship is, the more difficult it is to identify without additional information. *See, e.g.*, 23andMe, *The Method behind the Relative Finder Tool*, 23andMeBlog (Apr. 19, 2012), https://blog.23andme.com/ancestry-reports/method-behind-relative-finder (noting that the average person has about 940 fourth cousins); Ellen Greytak et al., *Genetic Genealogy for Cold Case and Active*

Investigations, Forensic Sci. Int'l, March 2019 at 103, https://www.researchgate.net/publication/332047092_Genetic_genealogy_for_cold_case_and_active_investigations.

37 This means the DNA does not directly code for genetic traits and is not currently known to be linked to race, gender, or health.

38 Heather Murphy & Mihir Zaveri, *Pentagon Warns Military Personnel Against At-Home DNA Tests*, N.Y. Times (Dec. 24, 2019), https://www.nytimes.com/2019/12/24/us/military-dna-tests.html; *see also* Andrea Roth,*"Spit and Acquit": Prosecutors as Surveillance Entrepreneurs*, 107 Calif. L. Rev. 405, 413 (2019) (Genetic genealogy data could easily be misused for "intrusive purposes, such as blackmail and invidious research.").

39 *See* Sarah McQuate, *Popular Third-Party Genetic Genealogy Site is Vulnerable to Compromised Data, Impersonations*, UW News (Oct. 29, 2019), https://www.washington.edu/news/2019/10/29/genetic-genealogy-site-vulnerable-compromised-data-impersonations.

40 Greytak et al, *supra* note 37.

41 Jocelyn Kaiser, *We Will Find You: DNA Search Used to Nab Golden State Killer Can Home in on About 60% of White Americans*, Science (Oct. 11, 2018, 2:00 PM), https://www.sciencemag.org/news/2018/10/we-will-find-you-dna-search-used-nab-golden-state-killer-can-home-about-60-white.

42 *See* Tom Barnes, *Golden State Killer: Police Using Genealogy Website Wrongly Identified Innocent Man in Nursing Home as Suspect*, Independent (Apr. 28, 2018, 12:51 PM), https://www.independent.co.uk/news/world/americas/golden-state-killer-2018-case-solved-identity-genetic-genealogy-websites-dna-joseph-james-deangelo-a8326946.html.

43 *See* Jennifer Lynch, *How Private DNA Data Led Idaho Cops on a Wild Goose Chase and Linked an Innocent Man to a 20-Year-Old Murder Case*, Elec. Frontier Found. (May 1, 2015), https://www.eff.org/deeplinks/2015/05/how-private-dna-data-led-idaho-cops-wild-goose-chase-and-linked-innocent-man-20.

44 *See, e.g.*, Raynor v. State, 99 A.3d 753 (2014).

45 A few years ago, law enforcement collected cigarettes left behind from the Dakota Access Pipeline protests and used the DNA from the cigarettes to identify protestors, though not through FGGS. *DNA from Cigarette Leads to Dakota Access Arrest 3 Years on*, AP (Sept. 6, 2019), https://apnews.com/abb444c2e6f14ca49a675e82d4b0d520; *see also* Comments of the Electronic Frontier Foundation Regarding Notice of Proposed Rulemaking on the Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 85 Fed. Reg. 56338 (Oct. 13, 2020), https://www.eff.org/document/eff-comments-dhs-proposed-rule-collection-and-use-biometrics-october-2020 (opposing federal agency proposal to collect DNA from US citizens and their immigrant family members, which would have allowed the agency to identify and map families and, eventually over time, whole communities).

46 *See* Rakas v. Illinois, 439 U.S. 128, 133–34 (1978).

47 *See* Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018) ("If the third-party doctrine does not apply to the 'modern-day equivalents of an individual's own "papers" or "effects,"' then the clear implication is that the documents should receive full Fourth Amendment protection."); *id.* at 2230 (Kennedy, J., dissenting) (stating that case law permitting warrantless access to records "may not apply when the Government obtains the modern-day equivalents of an individual's own 'papers' or 'effects,' even when those papers or effects are held by a third party."); *id.* at 2262 (Gorsuch, J., dissenting) ("Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers. *Smith* and *Miller* teach that the police can review all of this material, on the theory that no one reasonably expects any of it will be kept private. But no one believes that, if they ever did." (citing Smith v. Maryland, 442 U.S. 735 [1979]); and United States v. Miller, 425 U.S. 435 [1976]).

48 442 U.S. 735 (1979).

49 425 U.S. 435 (1976).

50 Stingrays are privacy-invasive devices used to find individuals by masquerading as cell towers. They force all mobile phones within range to emit identifying signals, which can be used to precisely locate not only a particular suspect, but countless bystanders as well. *See generally*, Stephanie K. Pell & Cristopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 Harv. J. Law & Tech. 1 (2014).

51 *See* Email from Sergeant Kenneth Castro, Sarasota Police Dep't, to Terry Lewis (Apr. 15, 2009, 11:25 AM), https://www.aclu.org/sites/default/files/assets/aclu_florida_stingray_police_emails.pdf [hereinafter Castro Email] (released in response to a public records request).

52 For a discussion of parallel construction, *see, e.g.*, Natasha Babazadeh, *Concealing Evidence: "Parallel Construction," Federal Investigations, and the Constitution*, 22 Va. J.L. & Tech. 1 (2018).

53 *See, e.g.*, Castro Email, *supra* note 52; Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes,* Usa Today (Aug. 24, 2015, 7:51 AM), http://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181.

54 *See, e.g.*, Letter from Amy S. Hess, Assistant Dir., Operational Tech. Div., to Captain David Salazar, Milwaukee Police Dep't (Aug. 13, 2013), https://assets.documentcloud.org/documents/2190206/milwaukee-pd-fbi-nda-13aug2013.pdf.

55 *See* Cox, *supra* note 29; Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall St. J. (Feb. 7, 2020, 7:30 AM), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600.

56 Levinson, *supra* note 23.

57 *See* Press Release, Sen. Ron Wyden, Wyden, Warren, Markey, Schatz Secure DHS IG Investigation of CBP Phone Location Data Surveillance Program (Dec. 2. 2020), https://www.wyden.senate.gov/news/press-releases/wyden-warren-markey-schatz-secure-dhs-ig-investigation-of-cbp-phone-location-data-surveillance-program.

58 *See* Letter from J. Russell George, Inspector Gen. for Tax Admin., to Sen. Ron Wyden and Sen. Elizabeth Warren (Sept. 30, 2020), https://www.wyden.senate.gov/imo/media/doc/093020%20IRS%20Reply%20to%20Wyden%20Warren.pdf.

59 *See* Paige St. John, *The Untold Story of How the Golden State Killer Was Found: A Covert Operation and Private DNA*, L.A. Times (Dec. 8, 2020, 5:00 AM), https://www.latimes.com/california/story/2020-12-08/man-in-the-window.

60 *See* Dep't of Justice, Interim Policy: Forensic Genetic Genealogical DNA Analysis And Searching (2019), https://www.justice.gov/olp/page/file/1204386/download.

61 Katz v. United States, 389 U.S. 347, 361 (1967).

62 United States v. Tuggle, 2021 U.S. App. LEXIS 20841, at *4–5 (7th Cir. July 14, 2021).

63 *See* Rakas v. Illinois, 439 U.S. 128, 133–34, 36 (1978).

64 Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

65 In a Ninth Circuit case addressing the constitutionality of the National Security Agency's telephony metadata program, the court disputed the government's contention that the defendant could not vicariously assert the rights of others whose data was swept up in the program. *See* United States v. Moalin, 973 F.3d 977, 989–92 (9th Cir. 2020). The court noted that the fact that others have data in the database and that the government has the ability to aggregate and analyze that data made the defendant's own metadata considerably more revealing.

66 *Carpenter*, 138 S. Ct. at 2217 (citing United States v. Jones, 565 U.S. 400, 415 [2012] [Sotomayor, J., concurring]).

67 *See* United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

68 *See*, *e.g.*, David C. Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J. L. & Tech. 381, 415 (2013).

69 2 F.4th 330 (4th. Cir. 2021).

70 *See* Leaders of a Beautiful Struggle v. Balt. Police Dep't, 979 F.3d 219, 223 (4th Cir. 2020), *rev'd en banc*, 2 F.4th 330 (4th. Cir. 2021).

71 *Id.* at 228.

72 *See* Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330 (4th. Cir. 2021).

73 *Id.* at 341 (quoting United States v. Carpenter, 138 S. Ct. 2206, 2215–19 [2018]).

74 *Id.* at 342 (quoting United States v. Jones, 565 U.S. 400, 415–17 [Sotomayor, J., concurring]).

75 *Id.* at 343.

76 *See id.* at 344.

77 *Id.* at 344–45 (quoting *Carpenter*, 138 S. Ct. at 2218) (emphasis in original).

78 *See id.* at 346 (citing *Carpenter*, 138 S. Ct. at 2218; Kyllo v. United States, 533 U.S. 27, 36 & n.4).

79 973 F.3d 977 (9th Cir. 2020).

80 *See id.*

81 484 Mass. 493 (2020).

82 ALPRs are cameras, mounted on top of patrol cars and on city streets that can scan up to 1,800 license plates per minute, day or night, and record that data along with the time and location of the scan in databases easily accessible to the police.

83 *McCarthy*, 484 Mass. at 506 (quoting *Carpenter*, 138 S. Ct. at 2218) (second alteration in original).

84 *Id.* at 507.

85 Similarly, in *ACLU v. Superior Ct. of L.A. Cnty.*, the California Supreme Court recognized that disclosure of a week's worth of county-wide raw, unaltered license plate scan data can "jeopardize the privacy of everyone associated with a scanned plate," despite the fact that law enforcement has argued that plate numbers cannot automatically be linked to specific individuals. 400 P.3d 432, 440 (Cal. 2017).

86 996 F.3d 374 (7th Cir. 2021).

87 *Id.* at 389 (citing *Carpenter*, 138 S. Ct. at 2217); *cf.* Tracey v. State, 152 So. 3d 504, 520 (Fla. 2014) (holding real-time data violated the Fourth Amendment); Commonwealth v. Almonor, 120 N.E.3d 1183 (Mass. 2019) (holding real-time data violated the Massachusetts state constitution). And in *State v. Muhammad*, the Washington Supreme Court held that a cell phone ping used to locate the defendant's vehicle in real time is a search under the Fourth Amendment and the Washington state constitution. 451 P.3d 1060 (Wash 2019).

88 2021 U.S. App. LEXIS 20841 (7th Cir. July 14, 2021).

89 *Id.* at *34; *see also* United States v. Moore-Bush, 963 F.3d 29, 42 (1st Cir.), *reh'g en banc granted, opinion vacated*, 982 F.3d 50 (1st Cir. 2020) ("[a] pole camera does not track the whole of a person's movement over time . . . [it] capture[s] only a small slice of the daily lives of any residents."). *But cf.* Commonwealth v. Mora, 150 N.E.3d 297, 302 (Mass. 2020) (concluding that seven months of "continuous, long-term pole camera surveillance targeted at the [defendants'] residences" was likely a search under the Fourth Amendment and "certainly" a search under the state's constitutional equivalent).

90 No. 2:20-cv-05044, 2021 WL 1220690 (C.D. Cal. Feb. 23, 2021) (appeal pending).

91 *See id.* at *6.

92 *Id.* at *3.

93 569 U.S. 435 (2013).

94 *See id.* at 464. *But see. id.* at 466–68 (Scalia, J., dissenting) (likening the government's program to a "general warrant").

95 136 S. Ct. 2160 (2016).

96 *Id.* at 2184.

97 *Id.* at 2178.

98 Orin Kerr has argued the Fourth Amendment allows law enforcement to purchase user records as "an end-run around the warrant requirement," although he recognizes "[a]rguments exist for why a different rule may be justified someday." *See* Orin S. Kerr, *Buying Data and the Fourth Amendment* (Hoover Working Grp. on Nat'l Sec., Tech. & Law, Aegis Series) (forthcoming 2021), https://ssrn.com/abstract=3880130.

99 Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (declining to extend the third-party doctrine to CSLI but stating "[w]e do not disturb the application of *Smith* and *Miller*").

100 *Id.*

101 *Id.*

102 *Id.* at 2233 (Kennedy, J., dissenting).

103 385 F. Supp. 3d 648 (N.D. Ill. 2019), *reconsideration denied*, No. 18 CR 185, 2020 WL 208826 (N.D. Ill. Jan. 14, 2020).

104 *See id.* at 650–53.

105 *Id.* at 652.

106 *See, e.g.*, *State v. Muhammad*, 451 P.3d 1060 (Wash 2019).

107 No. 2:20-cv-05044, 2021 WL 1220690 (C.D. Cal. Feb. 23, 2021) (appeal pending).

108 *Id.* at *4.

109 981 F.3d 961 (11th Cir. 2020).

110 *Id.* at 968 (collecting cases).

111 *See, e.g.*, United States v. Gratkowski, 964 F.3d 307, 311 (5th Cir. 2020).

112 *See* Charlie Savage, *Intelligence Analysts Use US Smartphone Location Data Without Warrants, Memo Says*, N.Y. Times (Jan. 25, 2021), https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html (DIA does not construe Carpenter as "requir[ing] a judicial warrant endorsing purchase or use of commercially available data for intelligence purposes"); Aleaziz & Haskins, *supra* note 24 (reporting on internal DHS memo stating agency officers did not need a warrant to search the data).

113 United States v. Moalin, 973 F.3d 977, 990 (9th Cir. 2020) (noting "[t]he distinctions between *Smith* and this case are legion and most probably constitutionally significant").

114 138 S. Ct. 1518 (2018).

115 *See id.* at 1529, 1531.

116 *See id.* at 1529.

117 *Id.* Even a serious violation of the rental agreement has no impact on expectation of privacy. *See id.*

118 *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 745 (1979) (noting "[w]e are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation."); United States v. Owens, 782 F.2d 146, 150 (10th Cir. 1986) (holding a motel's private terms do not govern a lodger's expectation of privacy).

119 Carpenter v. United States, 138 S. Ct. 2206, 2234 (2018) (Kennedy, J., dissenting).

120 *See id.* at 2214 (majority opinion) (quoting Boyd v. United States, 116 U.S. 616, 630 [1886]).

121 *See supra* previous discussion of the Fourth Amendment and third-party privacy rights.

122 *Carpenter*, 138 S. Ct. at 2218.

123 In both *Carpenter* and *Birchfield*, the Supreme Court took issue with this argument, recognizing that courts must take into consideration the entire quantity of data to which law enforcement has access, not just the narrow slice of it they choose to rely on to prove their case. *Id.* at 2217; Birchfield v. North Dakota, 136 S. Ct. 2160, 2177–78 (2016).

124 *See* Stanford v. Texas, 379 U.S. 476, 481–86 (1965) (describing writs of assistance and their influence on the drafters of the Fourth Amendment); *see also* William J. Cuddihy, The Fourth Amendment: Origins and Original Meaning 602–1791 at 363 (2009); Steagald v. United States, 451 U.S. 204, 220 (1981) ("The general warrant specified only an offense . . . and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched.").

125 Riley v. California, 573 U.S. 373, 403 (2014).

126 (1763) 98 Eng. Rep. 489 (KB).

127 (1765) 95 Eng. Rep. 807 (KB).

128 *Wilkes*, 98 Eng. Rep. at 490.

129 *Id.*

130 *Id.* at 484.

131 *See* Tenn. Const. art. I, § 7; Va. Const. art. I, § 10; N.C. Const. art. I, § 20; Md. Const., Dec. of R. art. 26 (each outlawing general warrants explicitly); *cf. e.g., Mass. Const.* art. XIV ("Every subject has a right to be secure from all unreasonable searches, and seizures, of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, . . . if the order, in the warrant, to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the persons or objects of search, arrest, or seizure[.]").

132 Stanford v. Texas, 379 U.S. 476, 481–82 (1965); *see also* Maryland v. King, 569 U.S. 435, 467 (2013) (Scalia, J. dissenting) (discussing foundations for the Fourth Amendment and the antifederalists' concerns that without a bill of rights, "the general, suspicionless warrant would be among the Constitution's 'blessings.'").

133 *King*, 569 U.S. at 469 (Scalia, J. dissenting). *Id.* at 467 (noting that the Fourth Amendment requires individualized suspicion, even for searches where a warrant is not constitutionally necessary).

134 *See* Ybarra v. Illinois, 444 U.S. 85, 91 (1979) ("mere propinquity" to criminal activity insufficient to establish probable cause).

135 Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 348 (4th. Cir. 2021) (quoting Messerschmidt v. Millender, 565 U.S. 535, 560 [Sotomayor, J., dissenting]).

136 *See* July 8 Mem. Op. and Order, *supra* note 19; Mem. Op. and Order, In re Search of Info. Stored at Premises Controlled by Google, No. 20-mc-00392 (N.D. Ill. Aug. 24, 2020), ECF No. 13, https://www.eff.org/document/re-search-info-stored-premises-controlled-google-no-20-m-392-2020-us-dist-lexis-152712-nd; *See* Mem. Op. and

Order, In re Search of Info. Stored at Premises Controlled by Google, No. 20-mc-00392 (N.D. Ill. Jul. 24, 2020), ECF No. 5, https://www.eff.org/document/re-search-information-stored-premises-controlled-google-no-20-m-392-nd-ill-july-24-2020; Mem. Op. and Order, In the Matter of the Search of Info. that is Stored at the Premises Controlled by Google, LLC, No. 21-mj-5064-ADM (D. Kan. June 4, 2021), ECF No. 2, https://ecf.ksd.uscourts.gov/cgi-bin/show_public_doc?2021mj5064-2.

137 July 8 Mem. Op. and Order, *supra* note 19.

138 444 U.S. 85 (1979).

139 July 8 Mem. Op. and Order, *supra* note 19.

140 *See* Steagald v. United States, 451 U.S. 204, 220 (1981).

141 Marron v. United States, 275 U.S. 192, 196 (1927).

142 Searches of app-generated location data and FGG searches are arguably worse than general warrants because there is currently no court oversight at all; the only constraints on police officers' actions come from department policies or company pushback, if either of these exist, and if either could be considered a true constraint.

143 *See* Google Decl. *supra* note 10, ¶ 23.

144 Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

145 *See* S.B. S8183, 2019 Leg. (N.Y. 2020), https://www.nysenate.gov/legislation/bills/2019/s8183 / (reintroduced as Assemb. B. A84A, 2021 Leg. (N.Y. 2021), https://www.nysenate.gov/legislation/bills/2021/A84).

146 Fourth Amendment Is Not For Sale Act, S. 1265, 117th Cong. § 2(e)(1)(E)(i)(I)(bb) (2021); *see also* Press Release, Sen. Ron Wyden, Wyden, Paul and Bipartisan Members of Congress Introduce the Fourth Amendment Is Not for Sale Act (Apr. 21, 2021), https://www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-members-of-congress-introduce-the-fourth-amendment-is-not-for-sale-act-.

147 S.B. 187, 2021 Leg., 442nd Sess. (Md. 2021), https://mgaleg.maryland.gov/2021RS/bills/sb/sb0187T.pdf.

148 New York State Senate Bill S296A is identical. *See* S.B. S296A, 2021 Leg. (N.Y. 2021), https://www.nysenate.gov/legislation/bills/2021/s296/amendment/a.

149 Assemb. B. A84A, 2021 Leg. (N.Y. 2021), https://www.nysenate.gov/legislation/bills/2021/A84.

150 *See id.*

151 *See* Shannon Flynn, *13 Cities Where Police Are Banned from Using Facial Recognition Tech*, Innovation & Tech Today (Nov. 18, 2020), https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech.

152 Both California and Vermont have enacted moratoria on at least some police use of face recognition, and Virginia has effectively banned its use, at least for now. Bryan Anderson, *New Law Bans California Cops from Using Facial Recognition Tech on Body Cameras*, Sacramento Bee (Oct. 10, 2019, 2:08 PM), https://www.sacbee.com/news/politics-government/capitol-alert/article235940507.html; *see also* ACLU of Vermont Statement on the Enactment of S.124, the Nation's Strongest Statewide Ban on Law Enforcement Use of Facial Recognition Technology, ACLU Vt. (Oct. 8, 2020, 2:15 PM), https://www.acluvt.org/en/news/aclu-vermont-statement-enactment-s124-nations-strongest-statewide-ban-law-enforcement-use; H.B. 2031, Spec. Sess. (Va. 2021), https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+HB2031ER+hil.

153 *See* ACLU Vt., *supra* note 153.

154 *See* Tracy Rosenberg, *Oakland Passes Facial Recognition Ban*, Oakland Priv. (July 17, 2019), https://oaklandprivacy.org/oakland-passes-facial-recognition-ban.

155 *See* Chris Weiland, *Victory in Minneapolis*, Restore the Fourth (Feb. 19. 2021), https://rt4.mn/2021/02/19/victory-in-minneapolis.

156 *See* Art Raymond, *Bill Targets How Police Use Info Showing Where You've Been and What Internet Searches You Make*, Deseret News (Feb. 25, 2021, 9:52 PM), https://www.deseret.com/utah/2021/2/25/22301633/reverse-location-reverse-keyword-law-enforcement-search-ban-utah-legislature-aclu-personal-privacy; S.B. 251, 2021 Gen. Sess. (2021 Utah), https://le.utah.gov/~2021/bills/static/HB0251.html. There may be more momentum behind New York's bill, however; although it failed to get out of committee during the 2020 legislative session, it was reintroduced for 2021–22.

157 Fourth Amendment Is Not For Sale Act, S. 1265, 117th Cong. § 2(e)(1)(E)(i)(I)(bb) (2021); *see also* Press Release, Sen. Ron Wyden, *supra* note 147.

158 *See* Fourth Amendment Is Not For Sale Act, S. 1265, 117th Cong. § 2(e)(1)(E)(i)(I)(bb) (2021).

159 Fourth Amendment Is Not For Sale Act, S. 1265, 117th Cong. § 2(i)(3)(B) (2021).

160 *See* Press Release, Sen. Ron Wyden, *supra* note 147.

161 *See* Press Release, Rep. Zoe Lofgren, Nadler, Lofgren Introduce Bicameral Fourth Amendment Is Not for Sale Act (Apr. 21, 2021), https://lofgren.house.gov/media/press-releases/nadler-lofgren-intro-bicameral-fourth-amendment-not-sale-act.

162 *See, e.g.*, Mike Orcutt, *Why Congress Can't Seem to Fix This 30-Year-Old Law Governing Your Electronic Data*, MIT Tech. Rev. (Feb. 17, 2017), https://www.technologyreview.com/2017/02/17/243544/why-congress-cant-seem-to-fix-this-30-year-old-law-governing-your-electronic-data.

163 *See* Virginia Hughes, *Two New Laws Restrict Police Use of DNA Search Method*, N.Y. Times (May 31, 2021), https://www.nytimes.com/2021/05/31/science/dna-police-laws.html; *Maryland HB30*, TrackBill, https://trackbill.com/bill/maryland-house-bill-30-public-safety-dna-analysis-search-of-data-base/1612577.

164 Montana passed a similar law around the same time, but it is much more limited. *See* Jennifer Lynch, *Maryland and Montana Pass the Nation's First Laws Restricting Law Enforcement Access to Genetic Genealogy Databases*, Elec. Frontier Found. (June 7, 2021), https://www.eff.org/deeplinks/2021/06/maryland-and-montana-pass-nations-first-laws-restricting-law-enforcement-access.

165 S.B. 187, 2021 Leg., 442nd Sess. (Md. 2021), https://mgaleg.maryland.gov/2021RS/bills/sb/sb0187T.pdf.

166 *See, e.g.*, Raynor v. State, 99 A.3d 753 (2014) (testing of DNA that defendant inadvertently left on chair at a police station was not a "search" for Fourth Amendment purposes).

167 A similar approach was successful in passing the California Electronic Communications Privacy Act (CalECPA). *See* Susan Freiwald, *At the Privacy Vanguard: California's Electronic Communications Privacy Act (CalECPA)*, 31 Berkeley Tech. L. J. 132, 143–47 (2018).

168 *See* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

169 *See* United States v. Bridges, 344 F.3d 1010, 1016 (9th Cir. 2003).

170 *See* Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971); Andresen v. Maryland, 427 U.S. 463, 480 (1976).

27 26 25 24 23 22 21 7 6 5 4 3 2 1

The preferred citation for this publication is Jennifer Lynch, *Modern-Day General Warrants and the Challenge of Protecting Third-Party Privacy Rights in Mass, Suspicionless Searches of Consumer Databases*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2104 (September 23, 2021), available at https://www.lawfareblog.com/modern-day-general-warrants-and-challenge-protecting-third-party-privacy-rights-mass-suspicionless.

About the Author

JENNIFER LYNCH

Jennifer Lynch is the surveillance litigation director at the Electronic Frontier Foundation and leads EFF's legal work challenging government abuse of search and seizure technologies. She also founded EFF's Street Level Surveillance Project. She has been awarded the *Free Speech and Open Government Award* and been named to the Daily Journal's 2021 list of lawyers who "Defined the Decade" for her work on privacy and policing.

The Jean Perkins Foundation Working Group on National Security, Technology, and Law

The Jean Perkins Foundation Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the *Lawfare* blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith is the chair of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams /national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION