Building on Carpenter: Six New Fourth Amendment Challenges Every Defense Lawyer Should Consider

The implications of the Supreme Court’s decision in *Carpenter v. United States* are just now coming into view as lower courts begin to apply *Carpenter’s* lessons to other forms of modern surveillance. In *Carpenter*, the Court held that a warrant is required to access more than six days of historical “cell site location information” — data obtained from the cellphone service provider indicating where a phone is connected to the cellular network. But the Court’s reasoning was not so limited. Instead, *Carpenter* marked another milestone in the Court’s process of rethinking Fourth Amendment doctrines in the digital age.

This article offers a snapshot of some current investigative techniques that may be ripe for constitutional challenges in a post-*Carpenter* world.

**Picturing the Post-Carpenter Landscape**

Broadly speaking, two kinds of cases will be most directly affected by the *Carpenter* ruling: “location tracking” cases and “third-party records” cases. As *Carpenter* was quick to acknowledge, “personal location information maintained by a third party … does not fit neatly under existing precedents.” Instead, it implicates two, previously distinct strands of Fourth Amendment law: (1) the “public space” doctrine, which concerns the privacy of one’s physical location and movements; and (2) the “third-party” doctrine, which governs the privacy of things people share with others. Accordingly, this article first examines three new location tracking technologies through a post-*Carpenter* lens, and then addresses government access to other kinds of data maintained by third parties.

It is important to bear in mind, however, that there may be significant overlap and interaction between these issues, as the *Carpenter* decision demonstrates. Rather than impose the rigidity of old doctrines on new technologies, the Court sought to preserve the “degree of privacy against government that existed when the Fourth Amendment was adopted.” The majority built on the Court’s landmark decisions in *United States v. Jones* and *Riley v. California* to once again recognize the guiding principle that digital is different — the idea that the old rules governing searches and seizures in the context of physical objects do not make much sense when applied to vast stores of digital data. In the end, the Court’s aim was to “secure the privacy of life against arbitrary power” regardless of changes in technology, and “place obstacles in the way of too permeating police surveillance.”

In this light, a host of sophisticated new investigative techniques appears to implicate some of the same privacy concerns that motivated a majority of the
Six Promising Avenues for Fourth Amendment Challenges

1. Historical Tower Dumps
2. Real-Time E911 Tracking
3. Real-Time Stingray Tracking
4. Online Accounts
5. Modern Bank Records
6. Smart Devices

Court in Carpenter, Riley, and Jones. From a location tracking perspective, Carpenter calls into question the constitutionality of so-called “tower dumps,” or demands for data about unknown phones that happened to connect with a given cell tower during a given period of time. It also implicates real-time or “prospective” cellphone tracking through the E911 system, which can use either GPS data or cell site location information to find a phone with government-mandated accuracy. And finally, it is yet another indication that the use of “Stingray” devices — designed to spoof a cellphone tower to find phones in real time — is constitutionally suspect.

Additionally, Carpenter cracked the armor of the “third-party doctrine,” signaling that the Fourth Amendment may protect other types of personal information held by third-party service providers like Google, Apple, or Facebook. Similarly, Carpenter speaks to the privacy of data captured by “smart” home devices that log activity and store data in the cloud. And it may prompt courts to reconsider the privacy of financial records to the extent they differ from physical checks or bank statements.

The following six sections provide promising avenues for future Fourth Amendment challenges that all defense lawyers should consider. Of course, many courts have not yet ruled on many of these issues, and there is sparse post-Carpenter case law available. As a result, this article is somewhat forward-looking, intended to serve as a starting point and reference document based on current trends.

Location Tracking Cases

Prior to Carpenter, the Supreme Court’s jurisprudence on location privacy revolved around the use of surveillance devices to directly monitor suspects. In United States v. Knotts and United States v. Karo, the government used hidden “beepers” to track suspects, whereas the Jones case involved a GPS tracker secretly installed on a car. Indeed, Justice Scalia, writing for Court in Jones, relied on the physical trespass caused by placing a GPS tracker on the undercarriage of the suspect’s car as the basis for finding a Fourth Amendment violation. It was only a shadow majority of concurrences in Jones that found the tracking itself to infringe on reasonable expectations of privacy. Carpenter explicitly endorsed those concurrences, and as a result, the defense bar has an opportunity to challenge other types of location tracking that also relies on third-party records, regardless of whether they involve a physical trespass.

1. Historical ‘Tower Dumps’

“Tower dumps” are demands for historical cell site location information (“CSLI”), similar to the records at issue in Carpenter. But instead of seeking the records about a suspect phone over the course of days, weeks, or months, a tower dump seeks records about an unknown number of phones over a relatively short period of time. It is a request for cellphone service providers to turn over data on every device that connected to specific cell sites with known physical locations over a given period of time, usually measured in minutes or hours. From an investigative standpoint, a tower dump might help identify phones that were present at the scene of a crime. It could also be used to identify participants at a political protest, congregants at a house of worship, or government whistleblowers.

Tower dumps have become increasingly routine in recent years, but there are few judicial opinions examining their constitutionality, and none issued since the Supreme Court decided Carpenter. From a Fourth Amendment perspective, tower dumps implicate many of the same concerns that troubled the Court in Carpenter, but they tend to sweep more broadly than deeply, affecting hundreds or thousands of people for a short time, as opposed to tracking one person over a long time. In fact, tower dumps may sweep so broadly that they amount to unconstitutional general warrants. They seek private cellphone records without any indication of who or how many people will have their privacy infringed, let alone probable cause for any one of them. Rather, such generalized, exploratory finishing expeditions and as a result, the Framers reviled. As Carpenter recognized, the Fourth Amendment must “contend with the seismic shifts in digital technology that made possible the tracking of not only [one person’s] location but also everyone else’s.”

Even if tower dumps are not outright unconstitutional, Carpenter makes it clear that a reasonable expectation of privacy exists in cellphone location data, which in turn triggers a warrant requirement. Of course, Carpenter also explicitly declined to decide the constitutionality of warrantless tower dumps, but the privacy interests in CSLI do not disappear simply because of the method used to obtain it. Depending on the context, tower dumps can provide an “intimate window” into the “privacies of life,” including one’s “familial, political, professional, religious, and sexual associations.” They can pierce the walls of private homes and businesses. And they function as a virtual time machine, granting “access to a category of information otherwise unknowable.”

While the duration of tower dumps may be more limited than the individual tracking in Carpenter, their reach is far broader, ensnaring potentially hundreds or thousands of unknown, innocent people. In this light, tower dumps appear to demand a warrant following Carpenter, and defense lawyers would be wise to challenge any warrantless collection of such data.

2. Real-Time E911 Tracking

Another issue that Carpenter recognized, but did not reach, is real-time location tracking of cellphones. One common way to do this is through the “Enhanced 911” (“E911”) system. By way of background, federal law mandates that all cellphones have the ability to convey their location to emergency
responder when 911 is dialed. Law enforcement, however, has the ability to enable this feature surreptitiously, even when the phone is not in use, 911 has not been called, and location services are not enabled. Depending on the service provider and the model of phone, the E911 system may use the phone's built-in GPS capabilities or else triangulate its location by “pinging” the device over the company's cellular network. Services providers then give law enforcement access to the phone's location through email updates, or they provide direct access through a purpose-built web portal.

The Supreme Court's concern over warrantless GPS tracking has been apparent since Jones, and the Carpenter Court noted that the “accuracy of CSLI is rapidly approaching GPS-level precision.” But unlike Jones, there is no need to install a physical device and commit a trespass in order to track a cellphone. Modern phones come factory-equipped to convey their location to service providers on demand, and by extension, to law enforcement through the E911 system. Consequently, there is a lingering argument that individuals lack a reasonable expectation of privacy in E911 data because it is not obtained directly, but through the third-party service provider. Carpenter, however, should put this contention to rest. Just like historical CSLI, E911 data can track a phone precisely, “beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales.”

And when the government “achieves [such] near perfect surveillance, [it is] as if it had attached an ankle monitor to the phone's user.” Here, Carpenter teaches that the intermediary role of third-party service providers is no longer fatal to Fourth Amendment challenges.

In fact, the government's use of the E911 system may not present a true third-party records issue at all. Rather than obtaining existing information, the government may effectively commandeering a service provider's system, causing location data to be transmitted directly through E911 channels without any voluntary activity on behalf of the user. In this respect, real-time tracking with E911 can operate as a direct search and seizure of a phone's location data, similar to the use of “Stingray” devices, as discussed next.

3. Real-Time 'Stingray' Tracking

A "Stingray" is the most well-known brand name of a device generally referred to as a “cell site simula-

tor.” It is a little larger than a briefcase and it works by mimicking a cell phone tower, like the cell sites used by service providers in Carpenter. The essential difference is that a Stingray connects to law enforcement instead of the cellphone service provider. It forces every phone within range to connect to it (instead of the real cellular network), revealing their unique assigned serial numbers. In short, the government does not just commandeer a service provider, it pretends to be one. Newer versions of the Stingray also have the capability to intercept voice and data transmissions.

Police use Stingrays in two ways. First, they can attempt to locate a known suspect's phone by scanning the area for its unique serial number. The range of Stingrays is limited, however, so their use often follows access to historical or real-time cellphone location records, which may not be able to pinpoint the location of a particular phone as accurately as a Stingray. The alternative is to canvass an area and scoop up data on all the devices in range. This technique may be used to identify the individuals present at a location and capture information about the phones they are using, functioning like a real-time, roving tower dump. And if used in the latter capacity, it may also function like a general warrant.

Stingrays capitalize on cell site location information, the same type of data at issue in Carpenter. But unlike Carpenter, the police generate and collect it themselves. There is no third party involved at all, and no need to invoke the third-party doctrine. Instead, Stingrays cause a direct search and seizure of nearby phones, commandeering their connections to the world. In this sense, the best analogy may be to Jones or Riley, with a clear element of trespass as well. Nonetheless, Carpenter offers additional ammunition against the warrantless use of Stingrays: the reasonable expectation of privacy in CSLI. As one Florida court recently put it, "If a warrant is required for the government to obtain historical cell site information voluntarily maintained and in the possession of a third party ... we can discern no reason why a warrant would not be required for the more invasive use of a cell site simulator." Other courts reached the same conclusion before Carpenter, and as of 2015, it is Justice Department policy for agents to obtain warrants for Stingrays.

4. Online Accounts

Cellphone service providers are hardly the only type of modern technology company to maintain private data about their users. Today, most Americans maintain personal accounts with technology giants like Apple, Facebook, Google, and Microsoft in order to access the internet, use search engines, check email, and post on social media. Indeed, the proliferation of “cloud-based” services has migrated much of the modern office online, not to mention diaries, photo albums, music libraries, and bookshelves. All these online activities generate third-party records that may include both the content of online communications and account activity as well as detailed “metadata” about how, when, and where a user interacted with the service.

Carpenter does not directly address the privacy afforded to the myriad third-party records generated by such online activities, but it stands to reason that third-party data with privacy interests on par with CSLI should also receive Fourth Amendment protection. Although the Supreme Court has never held that a warrant is required for government access to email, for example, both the Justices and the government assumed as much at oral argument in Carpenter, appearing to endorse the Sixth Circuit's decision in United States v. Warshak. Indeed, lower courts now routinely require warrants to search
email, instant messaging, and social media accounts, no matter how old the data — despite a 1986 law authorizing warrantless searches of data older than 180 days. Likewise, many companies will only disclose communications content pursuant to a warrant.

In the past, some courts have drawn a line between communications “content” and its associated “metadata,” but that distinction derives from the same, outdated 1986 law at issue in Carpenter. It is, in short, another relic of technology. The best evidence is the Carpenter decision itself, which made no distinction between the content of cellphone use and the CLSI metadata it generates. Instead, the Court found that such metadata can trigger Fourth Amendment privacy concerns, just as much as “content.” Indeed, in the post-Carpenter world, the distinction between content and metadata has rapidly lost its currency and may be open to new constitutional challenges.

Nonetheless, at least one post-Carpenter court has ruled that a warrant is not required to obtain the IP address associated with the use of messages sent over a private messaging app. An IP address is a unique number assigned to every internet-connected device; it is also capable of approximating the device’s physical location. Apps and online services record all user IP addresses out of necessity, usually creating a log that can be obtained by investigators. In United States v. Contreras, the Fifth Circuit found no privacy interest in that log, reasoning that the target IP address identified a static home location and did not track the user’s day-to-day movements.

But even if IP addresses cannot physically “track” people about town, they can still show one’s digital travels, personal curiosities, and online associations. Indeed, they may detail the nature of private online activity, revealing far more information than seven days’ worth of CSLI. Investigators need not stitch together location coordinates or assume any intentions; the activity will be plain to see from web logs and the records of internet service providers. As a result, some people opt to conceal their IP address through anonymity services like “Tor,” a worldwide relay system designed to mask a user’s true IP address. While the use of Tor may demonstrate a strong subjective expectation of privacy, it should not be necessary to assure Fourth Amendment protection. In addition to IP addresses, any similarly revealing metadata associated with personal online accounts may be ripe for Fourth Amendment challenge.

5. Modern Bank Records

United States v. Miller was one of the seminal third-party doctrine cases, involving subpoenaed “checks, deposit slips, two financial statements, and three monthly statements.” The Supreme Court found no reasonable expectation of privacy in these documents because they were “negotiable instruments” for use in commercial transactions, distinguishing them from otherwise “confidential communications.” Modern bank records, however, entail far more than canceled checks and bank statements. Rather, they may come closer to resembling “confidential communications” depending on the type of data at issue.

Today, banks offer many more services than they did in the 1970s, including e-commerce and mobile banking apps that track far more than just deposits and withdrawals, including a customer’s purchasing preferences, IP addresses, and cellphone location information. Some banks even track when and how a user types, taps, or swipes online in order to detect fraud. Moreover, mobile payment services like Venmo and PayPal have a “social” component and collect data about a user’s “friends and contacts,” a feature that enables transactions via text message.

Modern bank records have come a long way from the “negotiable instruments” of the 1970s. And as Carpenter makes clear, the privacy afforded to third-party data should be assessed on its own merits. Thus, to the extent that modern bank records now resemble “confidential communications” more than deposit slips or canceled checks, the Carpenter majority may be amendable to protecting them under the Fourth Amendment. Although one federal circuit has already reaffirmed Miller after Carpenter, the case involved traditional records such as bank statements and deposit slips. In the future, defense counsel should seek to distinguish the search of any nontraditional bank records and explain how they can reveal the same “intimate window into a person’s life” that the Carpenter decision seeks to protect.

6. Smart Devices

“Smart” devices have proliferated in recent years, imbuing ordinary objects with computing power and wireless connectivity — part of the so-called “Internet of Things” — from smartwatches and glasses, to refrigerators, utility meters, and “home” devices like the Amazon Echo and Apple HomePod. Smart devices track a great deal of personal information and are appealing targets for law enforcement investigation. If the data resides on the device itself, then it should receive the same Fourth Amendment protection as a computer or cellphone under Riley. But if the data resides in the “cloud” or in the hands of a third-party service provider, then Carpenter likely comes into play.

While courts are just beginning to consider this issue, one federal circuit has already applied the rationale in Carpenter to a smart utility meter. In Naperville Smart Meter Awareness v. City of Naperville, the Seventh Circuit held that the collection of smart-meter electricity data at 15-minute intervals constitutes a Fourth Amendment search. With respect to the privacy interests at stake, the panel found that the technology-assisted meter reading is at least as rich and invasive as the thermal imaging in Kyllo v. United States. Indeed, such detailed records of electricity usage can reveal “when people are home, when people are away, when people sleep and eat, what types of appliances are in the home, and when those appliances are used.” The court therefore declined to apply the third-party doctrine, concerned about leaving consumers with the choice between their privacy and using electricity.

The takeaway here is that the logic of Carpenter may extend well beyond cellphones and location data. Defense counsel should not be reluctant to invoke Carpenter.

Authors’ Note: Bringing a Fourth Amendment “location tracking” or “third-party records” challenge post-Carpenter may be daunting even for experienced defense counsel. NACDL’s Fourth Amendment Center is available to assist. Defense attorneys handling a challenging case that involves any of the issues discussed here should contact Fourth Amendment Center Director Jumana Musa (jmusa@nacdl.org) or Senior Litigation Counsel Michael Price (mprice@nacdl.org) for pro bono consultation or direct litigation assistance.
A Word of Caution: The Good Faith Exception

There was a great deal of hope that Carpenter would apply to pending cases in which law enforcement obtained cell site location information without a warrant. But a number of federal courts have held that warrantless acquisition of historical CSLI is subject to a “good faith” analysis, upholding pre-Carpenter searches on that basis. Defense counsel should expect the government to raise the “good faith” exception to any and all the issues raised supra. Defense counsel must be prepared to argue why the exception should not apply at all or why, based on the facts of the case, law enforcement officers should not be allowed to claim that they acted in good faith.

Conclusion

The push to apply Carpenter beyond historical cell site location information has only just begun. The Fourth Amendment challenges identified here are a sampling of the possibilities as modern technologies spawn new devices and new types of data of interest to law enforcement. Defense counsel should pay close attention to new cases invoking Carpenter and seek to understand how new technologies work in order to educate judges to preserve Fourth Amendment guarantees in the digital world.

Notes

2. Id. at 2217.
5. Id. at 2214 (quoting Kyllo v. United States, 533 U.S. 27 (2001)).
9. Id. (quoting Boyd v. United States, 116 U.S. 616 (1886)) (internal quotations omitted).
10. Id. (quoting United States v. Di Re, 332 U.S. 581 (1948)).
13. Id. at 952.
14. Id. at 964 (Alito, J., concurring); id. at 955 (Sotomayor, J., concurring).
15. Carpenter, 138 S. Ct. at 2215 (“The Court decided [Jones] based on the government’s physical trespass of the vehicle. … At the same time, five Justices agreed that related privacy concerns would be raised by, for example, ‘surreptitiously activating a stolen vehicle detection system’ in Jones’s case to track Jones himself, or conducting GPS tracking of his cellphone.”).


19. See In re Application, 930 F. Supp. 2d at 702 (tower dumps are “a very broad and invasive search affecting likely hundreds of individuals in violation of the Fourth Amendment”).

20. United States v. Knotts, 460 U.S. 276, 284 (1983) (“If such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.”).


23. Id. at 2217.

24. Id. at 2220.

25. Id. at 2217.

26. Id. at 2218.

27. See, e.g., Ellen Nakashima, Agencies Collected Data on Americans’ Cellphone Use in Thousands of ‘Tower Dumps,’ Wash. Post, Dec. 8, 2013 (each tower dump yielded “hundreds or thousands” of phone numbers belonging to innocent Americans); John Kelly, Cellphone Data Spying: It’s Not Just the NSA, USA Today, Dec. 8, 2013 (describing a Colorado case in which “at least several thousand people’s phones” were likely implicated).

28. Given the nature of tower dumps, counsel should also examine any warrant for lack of particularity and overbreadth.


31. See United States v. Pineda-Moreno, 617 F.3d 1120, 1125 (9th Cir. 2010).

32. Carpenter, 138 S. Ct. at 2219.


34. Carpenter, 138 S. Ct. at 2218.

35. Id.


37. A “Stingray” may also be referred to generically as an “International Mobile Subscriber Identity catcher” or “IMSI catcher.” Commercially, other brand names include “Triggerfish,” “Kingfish,” and “Hailstorm.” The “DRT 1101B” (or “dirt box”) is a cell site simulator that can monitor 10,000 devices at once, can be mounted to a plane, and can easily be used to identify the participants at a rally or protest. See Jennifer Lynch, DRT 1101B Survey Equipment Review, The Intercept, https://theintercept.com/surveillance-catalogue/drt-1101b/ (last visited Nov. 5, 2017); Kim Zetter, The Feds Are Now Using ‘Stingrays’ in Planes to Spy on Our Phone Calls, Wired (Nov. 14, 2014), https://www.wired.com/2014/11/feds-motherv3-stingray-stingrayers-mothering-planes/.


40. See, e.g., Sylvestre, 2018 WL 4212162, at *2.

41. Invoking a trespass theory could hold sway with Justice Gorsuch, whose dissent in Carpenter could have been a concurrence. A property law approach might also be appealing to Justices Alito and Thomas. See Michael Price, Carpenter v. United States and the Future Fourth Amendment, The Champion, June 2018, at 50.

42. Id. at *5.


45. Carpenter, 138 S. Ct. at 2231 (Kennedy, J., dissenting).

46. Id.

47. Additional third parties may be involved in these activities, either directly (e.g., through a browser extension) or indirectly (e.g., because of data sharing agreements). The nature of these records will depend on the particular policies of the individual companies involved.


49. United States v. Warshak, 631 F.3d 266, 285–286 (6th Cir. 2010) (email “is the technological scion of tangible mail” and it would “defy common sense to afford emails lesser Fourth Amendment protection”).

50. Compare 18 U.S.C. § 2703(a) (requiring a warrant for the “contents” of a communication that is in electronic storage for 180 days or less) with In re the Search of Three Hotmail Email Accounts, 2016 WL 1239916 (D. Kan. Mar. 28, 2016), rev’d in part, 212 F. Supp. 3d 1023; In re the Search of Information Associated with [redacted]@mac.com, 25 F. Supp. 3d 1, 7–9 (D.D.C. 2014), vacated, 13 F. Supp. 3d 157; In re [REDACTED]@gmail.com, 62 F. Supp. 3d 1100, 1103–04 (N.D. Cal. 2014). The 180-day rule was adopted as a product of the way email worked in 1986. Email providers did not store messages indefinitely on their servers; users were meant to log in and download messages to their personal computer; and any email not retrieved within 180 days was thought to be “abandoned” under the SCA. See Melissa Medina, The Stored Communications Act: An Old Statute for Modern Times, 63 Am. U. L. Rev. 267, 295-96 (2013).
of child pornography on a mobile messaging application called “Kik.” A
subpoena to Kik revealed an IP address that a
record search revealed was associated with
Frontier Communications. A subpoena
Frontier led to the defendant’s address,
which led to a search warrant to the
residence. In response to defense argument
that the government needed a warrant to
acquire the Frontier records, the court held
that the defendant had no reasonable
expectation of privacy in the family address
as contained in Frontier’s records.
54. See Gale Guthrie Weissman, What Is
an IP Address and What Can It Reveal About
You?, (Business Insider, May 18, 2015, 4:45
55. Contreras, 905 F.3d at 857.
56. See Lee Mathews, What Tor Is, and
Why You Should Use It to Protect Your Privacy,
Forbes (Jan. 27, 2017, 2:30 PM),
https://www.forbes.com/sites/leemathews/
2017/01/27/what-is-tor-and-why-do-people
-use-it-123718ec7d75; see also Brief for
Appellant, United States v. Ramos, 2018 WL
3477291 (5th Cir.), at 17 (“Ramos does not
concede that he had no privacy interest in
his IP address, which he was attempting to
conceal by using the Tor network.”).
57. See Price, 8 J. Nat’l Security L. & Pol’y
at 286-88.
58. United States v. Miller, 425 U.S. 435,
438 (1976).
59. Id. (emphasis added).
60. Kroft, “The Data Brokers: Selling Your
Personal Information,” March 9, 2014.
-selling-your-personal-information.
61. See Meyer, “Why Internet Banking
Fraud Is So Much More Than IP Addresses,”
www.bankerstoolbox.com/news/blog/
internet-banking-fraud-ip-addresses.
62. See Victor Luckerson, Your Bank
Wants to Know Where You Are at All Times,
Time (Mar. 4, 2016), http://time.com/
4247847/banks-tracking-cell-phone
-fraud/; Robin Sidel, Why Your Bank Wants to
Track Your Phone, Wall St. J. (Mar. 4, 2016),
https://www.wsj.com/articles/why
-your-bank-wants-to-track-your-phone
-1457087400.
63. Stacy Cowley, Banks and Retailers
Are Tracking How You Type, Swipe and Tap,
ytimes.com/2018/08/13/business/
behavioral-biometrics-banks-security.html.
64. See PayPal Privacy Policy,
https://www.paypal.com/us/webapps/mpp/ua/privacy-full#2 (last visited Nov. 8, 2018); Venmo Payment Activity & Privacy,
-us/articles/210413717-Payment
-Activity-Privacy (last visited Nov. 8, 2018);