AN A.S. PRATT PUBLICATION
NOVEMBER/DECEMBER 2018
VOL. 4 • NO. 9

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 4 | NUMBER 9 | NOVEMBER-DECEMBER 2018

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [4] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [281] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2018–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Carpenter v. United States: A Revolution in Fourth Amendment Jurisprudence?

By Christopher C. Fonzone, Kate Heinzelman, and Michael R. Roberts*

The U.S. Supreme Court's decision in Carpenter v. United *States is the latest in a line of cases in which the Court has applied the Fourth Amendment in light of changed technological circumstances. Commentators have variously described the decision as groundbreaking or incremental. In fact, the decision has the potential to be either. By holding that individuals have a reasonable expectation of privacy in historical cell-site locational information ("CSLI") held by cellular service providers, the Court limited the so-called third-party doctrine and suggested that aspects of new digital technologies alter the constitutional privacy analysis in ways not yet clearly reflected in statutes or cases. At the same time, the Court explicitly stated that its opinion is "narrow," thereby tempering expectations of a sea change in Fourth Amendment jurisprudence. Despite this attempt to downplay the opinion's significance, however, the Court's tightening of the third-party doctrine, which generally denies Fourth Amendment protection for information provided to third parties, may well make* Carpenter *the most important privacy decision in a generation. At the very least, the opinion is sure to spawn debate in lower courts about how far its rationale should extend. In the meantime, holders of digital data should seek to understand the decision's impact on their businesses and monitor how lower courts and government officials apply its pronouncements in practice.*

Nearly 90 years ago, in *Olmstead v. United States*,[1] the Court held that the Fourth Amendment permitted warrantless wiretapping, at least as long as the government does not trespass on the defendant's property when installing the tap. The *Olmstead* decision was five to four and, in dissent, Justice Brandeis expressed incredulity about his colleagues' failure to account for technological developments in their understanding of the Fourth Amendment's protections:

* Christopher C. Fonzone (cfonzone@sidley.com) is a partner in Sidley Austin LLP's Privacy and Cybersecurity practice, focusing on a wide range of issues related to information technology and cybersecurity, such as data protection, information security and management, and cyber governance and preparedness. Before joining the firm, he was deputy assistant and deputy counsel to President Obama and the legal adviser to the National Security Council. Kate Heinzelman (kheinzelman@sidley.com) is a counsel in the firm's Healthcare and Privacy & Cybersecurity practices, who focuses on enforcement and regulatory issues in healthcare and privacy/cybersecurity. Prior to joining the firm, she served as deputy general counsel at the Department of Health & Human Services and as associate counsel to President Obama. Michael R. Roberts (mrroberts@sidley.com) is an associate in the firm's Privacy and Cybersecurity group. His practice focuses on issues related to cybersecurity, privacy, and information law. Prior to joining the firm, he completed an internship at The White House in the Office of the Counsel to Vice President Biden.

[1] 277 U.S. 438 (1928).

> Time works changes, brings into existence new conditions and purposes. Therefore, a principle, to be vital, must be capable of wider application than the mischief which gave it birth. This is peculiarly true of constitutions. They are not ephemeral enactments, designed to meet passing occasions. . . . The progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping. Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions. . . . Can it be that the Constitution affords no protection against such invasions of individual security?[2]

Justice Brandeis's dissent proved prescient, as the Supreme Court overruled *Olmstead* nearly 40 years later in the landmark case of *Katz v. United States*.[3] And Justice Brandeis's dissent presaged a long line of decisions grappling with how the Fourth Amendment's protections apply to novel search techniques afforded by the "progress of science."[4] Indeed, the trend has accelerated in the last decade as cases involving computer and personal electronic device searches have increasingly found their way to the Court.[5]

Carpenter v. United States did not involve a search of a personal computer or device. Rather, it concerned the collection of historical cell site location information, or CSLI, from wireless carriers. CSLI is time-stamped information about the location of a cellular phone, and wireless carriers collect this information as a phone connects to a cell site near its location. In *Carpenter*, law enforcement sought to connect a suspect of a crime to the scene of several robberies by obtaining this information about the location of his cell phone from his wireless carriers. They sought the records pursuant to a court order issued under the Stored Communications Act, which authorizes the acquisition of CSLI and other types of records even in the absence of a probable cause warrant.

The issue before the Court in *Carpenter* was whether the government could compel wireless providers to turn over CSLI without securing a probable cause warrant. Longstanding Supreme Court precedent, commonly known as the "third-party doctrine," instructs that individuals generally have no "reasonable expectation of privacy" in, and that the Fourth Amendment therefore does not protect, information voluntarily turned over to others. *Carpenter* thus has implications that potentially reach far

---

[2] *Id.* at 472-75 (Brandeis, J., dissenting).

[3] 389 U.S. 347 (1967).

[4] *See, e.g., Kyllo* v. *United States*, 533 U. S. 27 (2001) (heat sensor).

[5] *See Riley v. California*, 134 S. Ct. 2473 (2014) (search of cellphone incident to arrest); *United States* v. *Jones*, 565 U.S. 400 (2012) (tracking device on car); *City of Ontario v. Quon,* 560 U.S. 746 (2010) (search of pager).

beyond its facts, as courts have interpreted the doctrine as applying broadly to all sorts of business records and other information in the custody of third parties.[6] The Supreme Court had crafted the third-party doctrine, however, long before the ubiquity of digital technologies and cheap electronic storage placed an extraordinary amount of potentially revealing personal information into the hands of social media companies, communications service providers, application providers, advertisers, and others. And prior to *Carpenter*, the Court had not yet addressed what is likely the most important Fourth Amendment question of the time: does the "third-party doctrine" mean that the Fourth Amendment is silent about when the government may turn to private companies for access to the digital tracks left by cellphones, computers, and the Internet of Things?

In *Carpenter*, the Court channeled Justice Brandeis's *Olmstead* dissent in answering "no" to that important question – at least as applied to *Carpenter's* facts.[7] To be sure, the Court emphasized that its decision is "narrow" and pertains exclusively to historical CSLI. But by holding that the Fourth Amendment protects historical CSLI held by a third party, the Court signaled a readiness to apply constitutional protections to "new conditions." *Carpenter* could thus mark a key inflection point in Fourth Amendment law.

Moreover, unlike many Fourth Amendment cases, *Carpenter* is directly relevant to private industry. In today's digital economy, nearly every company holds data about or from individuals, which law enforcement may seek to obtain directly from those companies. Companies, in turn, have taken a variety of positions on these requests and their obligations to their customers in connection with them. In light of the decision's importance to holders of data, this article outlines the background, key aspects, and potential implications of the *Carpenter* decision.

THE *CARPENTER* CASE

Facts

In *Carpenter*, a suspect confessed to a series of robberies and provided law enforcement with the cell phone numbers of alleged accomplices. The Federal Bureau of Investigation ("FBI") also reviewed the suspect's call records to identify numbers he had called around the time of the crimes. Prosecutors used these numbers to apply for a court order under the Stored Communications Act, which allows the government to secure orders to compel production of certain records when it "offers specific and

[6] The Stored Communications Act makes clear, however, that a warrant is required to obtain "the *contents* of a wire or electronic communication[] that is in electronic storage in an electronic communications system for one hundred and eighty days or less." 18 U.S.C. § 2703(a). The *Warshak* case, discussed further below, has significant implications for the 180-day dividing line the Stored Communications Act established.

[7] *See Carpenter v. United States*, 585 U.S. __ (2018) (hereinafter "Slip op.").

articulable facts showing that there are reasonable grounds to believe" the records sought "are relevant and material to an ongoing criminal investigation."[8] Granting this application, a federal magistrate judge ordered Timothy Carpenter's wireless carriers to produce "cell/site sector" information for the window of time coinciding with the robberies. In particular, one order sought 152 days of CSLI from a provider, which produced records spanning 127 days. A second order requested seven days of CSLI from another provider, which yielded two days of records. Collectively, the providers produced nearly 13,000 location points detailing Carpenter's movements over a four-month period. The question before the Court in *Carpenter* was whether the government violated Carpenter's Fourth Amendment rights by obtaining this CSLI without a warrant supported by probable cause.

"Reasonable Expectation of Privacy"

In a 5-4 decision, the Court determined that the government had violated Carpenter's Fourth Amendment rights, because Carpenter had a "reasonable expectation of privacy" in the CSLI and thus the government could secure it only after showing probable cause. The Court began its analysis with its landmark decision in *Katz*.[9] *Katz* holds that "the Fourth Amendment protects people not places," and that a warrant is generally required when an individual "seeks to preserve something as private," and the expectation of privacy is "one that society is prepared to recognize as reasonable."[10] The Court then explained that "no single rubric resolves which expectations of privacy are entitled to protection" under Katz[11] and acknowledged that requests for historical CSLI records do "not fit neatly under existing precedents" but instead "lie at the intersection of two lines of cases."[12]

- Jones *and Location Tracking*. The first line of cases, the Court noted, concerns a person's "expectation of privacy in his physical location and movements" and culminates in the Court's 2012 decision in *United States v. Jones*,[13] which addressed the installation of a GPS tracking device on a suspect's vehicle. Although *Jones* turned on the FBI's physical trespass of the vehicle, *Carpenter* observed that five Justices in *Jones* agreed that "privacy concerns would be raised by, for example, 'surreptitiously activating a stolen vehicle detention system'" or "conducting GPS tracking" of a suspect's cell phone.[14] In short, the Court

[8] 18 U.S.C. § 2703(d).

[9] In dissent, Justice Thomas explicitly called on the Court to reconsider *Katz*, and Justice Gorsuch essentially did as well. *See* Slip op. at 1-2, 17-21 (Thomas, J., dissenting); Slip op. 6-9 (Gorsuch, J., dissenting).

[10] *Katz v. United States*, 389 U.S. 347, 351 (1967).

[11] Slip op. at 5.

[12] *Id.* at 7.

[13] 565 U.S. 400 (2012).

[14] Slip op. at 8 (quoting *Jones*, 565 U.S. at 426, 428 (Alito, J., concurring in the judgment)).

understood this line of cases to suggest that a person has a reasonable expectation of privacy in "detailed, encyclopedic, and effortlessly compiled" information that tracks the person's movements.[15]

- *The Third-Party Doctrine*. The second line of cases establishes the third-party doctrine. As the *Carpenter* Court recognized, prior cases considering an individual's banking records (*United States v. Miller*) and the phone numbers dialed by an individual (*Smith v. Maryland*) underscored that a person has no legitimate expectation of privacy in information voluntarily turned over to third parties, "even if that information is revealed on the assumption that it will be used only for a limited purpose."[16]

What's Important about CSLI?

After reviewing the two sets of decisions, and observing the tension between them, the Court explained that the logic of *Smith* and *Miller* does not easily extend to "the qualitatively different category of cell-site records."[17] In particular, the Court noted that, "when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements."[18] Therefore, the Court squarely declined to apply the third-party doctrine in the case before it. Instead, the Court held that Carpenter had a reasonable expectation of privacy in his CSLI. Thus, the Court held that the CSLI was constitutionally protected, and that the government's acquisition of the information was, as a result, a search under the Fourth Amendment.

In explaining its decision that individuals have a reasonable expectation in that cell phone information, the Court noted several "unique" attributes of historical CSLI. For instance:

- "Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts."[19]

---

[15] Separately, in *Riley v. California*, 134 S. Ct. 2473 (2014), the Court held that an arrestee's cell phone could not be searched without a warrant pursuant to the Fourth Amendment exception for searches incident to arrest. In so holding, the Court noted the problem in extending this doctrine to digital devices, stating that "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of" physical objects, like "a wallet, or a purse" that an arrestee might have on them at the time of arrest.

[16] *United States v. Miller,* 425 U.S. 435, 443 (1976); *see also Smith v. Maryland,* 442 U.S. 735, 743-44 (1979).

[17] Slip op. at 11.

[18] *Id.*

[19] *Id.* at 12.

- "[T]he timestamped data 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.'"[20]
- "[C]ell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense."[21]
- "[Individuals] compulsively carry cell phones with them all the time."[22]
- "[T]he retrospective quality of the data . . . gives police access to a category of information otherwise unknowable."[23]

The Court further rejected the government's argument, echoed by Justice Kennedy in dissent, that CSLI should not receive constitutional protection because it is less precise than GPS information. The Court explained that the information was detailed enough to indicate that Carpenter was at the site of the robberies.[24] Moreover, the Court asserted that its decision should consider the rapidly improving accuracy of CSLI.

More fundamentally, the Court rejected the government's reliance on the third-party doctrine:

> The Government's position [that the third-party doctrine controls this case] fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years. Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible. There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today. The Government thus is not asking for a straight forward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information.[25]

The Court also emphasized that an underlying rationale of the third-party doctrine – "voluntary exposure" – does not "hold up when it comes to CSLI."[26] As the Court explained, a cell phone "logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up," and because "apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail

[20] *Id.* (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).
[21] *Id.* at 12-13.
[22] *Id.* at 13.
[23] *Id.*
[24] *Id.* at 14.
[25] *Id.* at 15.
[26] *Id.* at 17.

of location data," CSLI is therefore "not truly shared as one normally understands the term."[27] In other words, "in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements."[28]

What about Subpoenas?

Another critical aspect of the Court's decision concerns the use of subpoenas to compel the production of information. Having held "that the acquisition of Carpenter's CSLI was a search," the Court also concluded "that the Government must generally obtain a warrant supported by probable cause before acquiring such records."[29] In so ruling, the Court rejected the position articulated in Justice Alito's dissent, which argued that the warrant requirement and its probable cause standard do not apply here because the government acquired records using compulsory process (*i.e.*, by issuing an order or subpoena requiring a party to produce specific documents), rather than through the direct taking of evidence (*i.e.*, having law enforcement officers enter a private premises). Reviewing the cases that Justice Alito cited in support of this proposition, the Court noted that all of those decisions, including the third-party doctrine cases cited above, "contemplated requests for evidence implicating diminished privacy interests or for a corporation's own books," and that the Court had accordingly "never held that the Government may subpoena third parties for records in which the suspect had a reasonable expectation of privacy."[30] The Court thus held a warrant was generally required to obtain a week's worth of historical CSLI,[31] although specific exceptions, like exigent circumstances, may justify proceeding without one in certain cases.

WHAT TO MAKE OF IT?

Carpenter is the first case requiring the Court to decide whether the third-party doctrine applies to new digital technologies.[32] Particularly given the ways in which law enforcement officials can use the Stored Communications Act, and the number of statutes that permit the government to acquire third-party information with less than a

---

[27] *Id.* (internal quotations omitted).

[28] *Id.* (quoting *Smith,* 442 U.S. at 745).

[29] *Id.* at 18.

[30] *Id.* at 19-20.

[31] The opinion stated that it did not resolve how much CSLI must be at issue to bring the Fourth Amendment into play, stating: "we need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search." Slip op. at 11 n.3.

[32] The Court has commented on the doctrine in other recent cases. *See, e.g.*, *Riley v. California*, 134 S. Ct. 2473, 2492–93 (2014) (stating that the government could not rely on *Smith* in a case involving a cell phone because there was no dispute that the phone itself had been searched, and noting that "call logs typically contain more than just phone numbers; they include any identifying information that an individual might add, such as the label 'my house'").

showing of probable cause,[33] *Carpenter* has potentially dramatic consequences not only for the government, but also for private industry holders of data.

A Narrow Decision

These possible consequences may have led the Court to go out of its way in emphasizing that its decision was a "narrow one." Indeed, recognizing that it "must tread carefully" when considering new technologies to "ensure that [it does] not 'embarrass the future,'"[34] the Court specifically identified a litany of things that its opinion was *not* doing:

> We do not express a view on matters not before us: real-time CSLI or "tower dumps" (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of Smith and Miller or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security.[35]

In short, the Court made a concerted effort to preemptively limit its decision to historical CSLI. Despite this effort, however, before the ink was even dry on the slip opinion, commentators were trying to parse *Carpenter*'s implications.[36] To be sure, *Carpenter's* narrow holding means that any attempts to predict its impact are speculative. The Court will have to consider the scope of the third-party doctrine again, and those cases will shape the trajectory of Fourth Amendment jurisprudence. That is not to say, however, that *Carpenter* itself will not have a near-term impact. To the contrary, notwithstanding its limited holding, several implications emerge for government, companies, and the lower courts that will have to grapple with its meaning.

---

[33] *See generally* Congressional Research Service, *Administrative Subpoenas in Criminal Investigations: A Brief Legal Analysis* (December 19, 2012).

[34] *Id.* at 17-18 (quoting *Northwest Airlines, Inc.* v. *Minnesota*, 322 U. S. 292, 300 (1944)).

[35] *Id.*

[36] *See, e.g.,* Orin Kerr, *Understanding the Supreme Court's* Carpenter *Decision*, LAWFARE (June 22, 2018), *available at* https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision; David Kris, *Carpenter's Implications for Foreign Intelligence Surveillance*, LAWFARE (June 24, 2018), *available at* https://www.lawfareblog.com/carpenters-implications-foreign-intelligence-surveillance; Marty Lederman, *Carpenter's Curiosities (and its Potential to Unsettle Longstanding Fourth Amendment Doctrines)*, BALKINIZATION (June 26, 2018), *available at* https://balkin.blogspot.com/2018/06/carpenter-s-curiosities-and-its.html; Paul Rosenzweig, *Carpenter v. United States and the Law of the Chancellor's Foot*, LAWFARE (June 27, 2018), *available at* https://www.lawfareblog.com/carpenter-v-united-states-and-law-chancellors-foot.

Limits on the Third-Party Doctrine

Most importantly, *Carpenter* makes clear that the third-party doctrine is not unbounded. In retrospect, this is perhaps unsurprising. *Katz*, for instance, held that an individual has a reasonable expectation of privacy in "wagering information" that the FBI heard through a listening device while the defendant voluntarily transmitted it over the phone.[37] But *Smith* and *Miller* contain extremely broad language. For example, *Smith* explicitly states, "[t]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[38] Thus, there was a perception that the third-party doctrine was something of a bright-line rule – a perception that *Carpenter* dispelled.

But What Limits? Protected and Unprotected Information

After *Carpenter*, to what sorts of information does the third-party doctrine continue to apply? In light of *Carpenter*'s self-declared narrowness, noted earlier, there is no definitive answer. Yet several categories appear to emerge:

- *Twentieth-Century Records.* First, *Carpenter* does not change the third party doctrine's limitations on the protection of certain information. Traditional business records, like those in *Miller* and *Smith*, fall into this category. As noted above, the Court explicitly stated that its decision would not "disturb the application" of those cases, and separately emphasized that there is a "world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today."[39] Overall, a pretty good shorthand of what the third-party doctrine still plainly covers is what one commentator has referred to as "20th Century business records," like the bank records at issue in *Miller*, the phone numbers at issue in *Smith*, or at least limited use of "conventional surveillance techniques and tools, such as security cameras."[40]
- *CSLI and what else?* At the opposite end of the spectrum is information that *Carpenter* indicates falls outside the third-party doctrine, and that is protected by a reasonable expectation of privacy. *Carpenter* holds that at least seven days of historical CSLI falls into this category. The Court's decision also appears to confirm that another type of information—the content of emails—receives full Fourth Amendment protection. This is important because the Stored Communications Act contemplates law enforcement officials being able to use an administrative subpoena or court order to obtain the "contents of a wire or electronic communication" in certain circumstances without demonstrating

[37] *Katz*, 389 U.S. at 348.
[38] *Smith*, 442 U.S. at 743-44.
[39] Slip op. at 15.
[40] *See* Kris, *supra* n.36.

probable cause.[41] In 2010, the U.S. Court of Appeals for the Sixth Circuit held in *United States v. Warshak* that this provision was unconstitutional as applied to email communications, and that the Constitution required the government to obtain a probable cause warrant before requiring providers to turn over such communications.[42] The *Carpenter* Court refers to *Warshak* in its opinion – as do both Justice Kennedy and Justice Gorsuch in their dissents – and it would be difficult to argue that email contents are not "'modern-day equivalents of an individuals' own 'papers' or 'effects,'" which the Court's opinion strongly suggests "should receive full Fourth Amendment protection."[43]

But What Limits? Unanswered Questions

Yet beyond these two types of information, *Carpenter's* implications are less clear. Indeed, the Court explicitly reserves the question of whether the information that would seem to bear the closest resemblance to the historical CSLI at issue in *Carpenter* – real-time CSLI, historical CSLI covering shorter time periods, and "tower dumps" – should be treated the same way. In essence, concluding that *Carpenter* finds any further types of information to be constitutionally protected requires relying on inferences from its reasoning, rather than its explicit holding. The Court's own view was that it is only in the "rare case" that a "suspect has a legitimate privacy interest in records held by a third party."[44]

After *Carpenter*, then, how is one to think about the other, ever-expanding categories of information produced or enabled by modern technologies and held by third-parties that the Court does not explicitly address? Do individuals have a reasonable expectation of privacy in their own biometric information, their DNA, or their GPS coordinates?

Carpenter does not definitively answer these questions. But it would be a mistake to say, as some commentators have, that *Carpenter* provides little or no guidance on how to think about the scope of the Fourth Amendment's protection or the third-party doctrine. Even if *Carpenter* does not articulate an explicit test, the Court does extensively identify the attributes of historical CSLI that make it constitutionally protected. For example, the nature and value of the information, in that it provides an "all-encompassing" record of an individual's movements; the sheer amount of information that can be collected by looking retrospectively; how easy it is for law enforcement to get the information, as compared to using traditional, manpower-intensive surveillance techniques; and the fact that individuals do not in any real sense "voluntarily" share the information with third parties. Types of information that share these attributes are more likely to be considered outside the scope of the third-party doctrine.

---

[41] *See* 18 U.S.C. § 2703(b).
[42] *See United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).
[43] *See* Slip op. at 21; *id.* at 13 (Kennedy, J., dissenting); Slip op. at 15 (Gorsuch, J., dissenting).
[44] *Id.* at 21.

To be sure, as Justice Alito states in his dissent, case-by-case adjudication will be necessary to identify the precise contours of how *Carpenter*'s reasoning applies to other types of information.[45] But in the meantime, holders of such information have no choice but to turn to *Carpenter* for guidance on when they should require a warrant before turning over information in their possession – including by considering whether the information they hold shares the attributes identified above.

CARPENTER IN THE LOWER COURTS

Another place the holders can look for guidance is the lower courts, where *Carpenter* has already started to inform analyses of the third-party doctrine. To be sure, courts may be slow to grapple with the full range of *Carpenter*'s implications, as the "good faith" exception to the exclusionary rule will keep courts from reaching the issue in some cases.[46] But recent decisions have applied *Carpenter*, with courts generally taking

[45] *See* Slip op. at 1 (Alito, J., dissenting) (noting that the Court's opinion "guarantees a blizzard of litigation").

[46] In the months since *Carpenter*, the U.S. Courts of Appeals for the Second and Fourth Circuits—and district courts in the Second, Third, Sixth, Seventh, and Ninth Circuits—have each relied on the "good faith" exception to dismiss *Carpenter*-based challenges. *See United States v. Zodhiates*, No. 17-839-CR (2d Cir. Aug. 21, 2018); *United States v. Blake*, No. 3:16-CR-111 (JBA) (D. Conn. Aug. 20, 2018) ("Since *Carpenter* was decided, the Court is aware of five other district courts—in the Third, Sixth, Seventh, and Ninth Circuits—to have addressed this precise question, as well as the Court of Appeals for the Fourth Circuit. Every one of these courts, writing in the seven weeks since *Carpenter* was decided, has declined to suppress evidence arising out of a pre-C*arpenter*, routine acquisition of cell site location information pursuant to the Stored Communications Act"); *United States v. Darmon Vonta Shaw*, No. CR 5:17-26-KKC (E.D. Ky. Aug. 3, 2018) (same); *United States v. Rojas-Reyes*, No. 1:16-CR-00123 (TWP) (DML) (S.D. Ind. July 17, 2018) (same); *United States v. Kevin Coles*, No. 1:16-CR-212 (M.D. Pa. Aug. 2, 2018) (same); *United States v. James Deshawn Williams*, No. 2:17-CR-20758 (VAR) (DRG) (E.D. Mich. Aug. 2, 2018) (same); *United States v. Chavez*, No. 15-CR-00285 (LHK) (N.D. Cal. June 26, 2018).

a cautious approach.[47] However, one decision illustrates *Carpenter*'s potential impact. Relying on *Carpenter*, the U.S. Court of Appeals for the Seventh Circuit recently held that the collection of smart-meter data at 15 minute intervals constitutes a search (though it also found the search to be reasonable in the absence of a warrant).[48]

GOVERNMENTAL ENFORCEMENT PROGRAMS AND THE SUBPOENA AUTHORITY

Alongside questions about how *Carpenter* affects the third-party doctrine, the Court's discussion of subpoena authority raises questions about how the decision will affect government enforcement programs that rely on that power.[49] As discussed above, *Carpenter* held that because the CSLI at issue was protected by a reasonable expectation of privacy, the information could only be obtained through a probable

[47] A number of district courts have rejected *Carpenter* claims on the grounds that the Court qualified its decision by stating, "We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras." Slip op. at 18. *See, e.g.*, *United States v. Tolbert*, No. CR-14-3761 (JCH) (D.N.M. July 27, 2018) (denying defendant's motion to suppress evidence obtained by law enforcement through the use of grand jury subpoenas directed towards two providers to uncover identifying information relating to his IP address and email accounts and noting, "[t]he information subpoenaed by law enforcement in this case is much more like the bank and telephone records in *Miller* and *Smith* than the comprehensive, detailed, and long-term location information in *Carpenter*."). *See also United States v. Tuggle*, No. 16-CR-20070 (JES) (JEH) (C.D. Ill. July 31, 2018) (internal citations omitted) ("The cameras only captured what would have been visible to any passerby in the neighborhood. Thus, this case is unlike the thermal imaging that was found to be a search in *Kyllo*. And while the Supreme Court has recently extended Fourth Amendment protections to address surveillance methods implicating new technologies, the surveillance here used ordinary video cameras that have been around for decades"); *United States v. Tirado*, No. 16-CR-168 (E.D. Wis. Aug. 21, 2018) (citing *Tuggle*, denying defendants' motion to suppress evidence obtained via the use of pole cameras, and noting, "[i]t is undisputed that the cameras used here did not record events inside the home or otherwise permit the police to see things an officer standing on the street could not see.").

[48] *See Naperville Smart Meter Awareness v. City of Naperville*, No. 16-3766 (7th Cir. Aug. 16, 2018) ("in this context, a choice to share data imposed by fiat is no choice at all. If a person does not—in any meaningful sense—"voluntarily 'assume the risk' of turning over a comprehensive dossier of physical movements" by choosing to use a cell phone, *Carpenter*, 138 S. Ct. at 2220 (quoting *Smith*, 442 U.S. at 745, 99 S. Ct. 2577), it also goes that a home occupant does not assume the risk of near constant monitoring by choosing to have electricity in her home. We therefore doubt that *Smith* and *Miller* extend this far."). *See also State v. Sylvestre*, No. 4D17-2116 (Fla. Dist. Ct. App. Sept. 5, 2018) (internal quotations and citations omitted) ("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. This is especially true when the cell phone is in a private residence, or other private locations beyond public thoroughfares including doctor's offices, political headquarters, and other potentially revealing locales.").

[49] The Court's own view was the impact of its decision was limited in this regard; the opinion states: "The Government will be able to use subpoenas to acquire records in the overwhelming majority of investigations." Slip op. at 21.

cause warrant, not a subpoena. Commentators disagree about whether this aspect of the Court's decision is revolutionary.[50]

Although the Court had not reached the issue prior to *Carpenter*, the basic conundrum is not new. In 2013, following the Sixth Circuit's *Warshak* decision, then-SEC Chair Mary Jo White wrote to Senator Patrick Leahy, the Chairman of the Senate Judiciary Committee, to explain that *Warshak* "greatly impeded the SEC's ability to serve administrative subpoenas on ISPs absent the consent of the subscriber."[51] White explained that this, in turn, was problematic because "for the Commission to obtain . . . important evidence and create a complete investigative record, it needs to preserve the authority to subpoena the ISPs to obtain any deleted or otherwise not available – or not produced – e-mails." White noted that the SEC, as a *civil* enforcement agency, could not obtain a warrant pursuant to the Federal Rules of Criminal Procedure, and thus would be unable to obtain such evidence. *Carpenter* makes clear this issue will endure, particularly absent congressional intervention to clarify enforcement authorities.

THE FUTURE OF THE FOURTH AMENDMENT: THE COURT AND CONGRESS

Finally, another important aspect of *Carpenter* is what the decision demonstrates about how the Court, as currently composed, may resolve related Fourth Amendment questions. As one commentator has pointed out, the breadth of Justice Gorsuch's rationale in dissent (in which he argues that "just because you *have* to entrust a third party with your data doesn't necessarily mean you should lose all Fourth Amendment protections in it"[52]) appears potentially more protective of individual privacy than the position the majority staked out, thereby indicating that a sixth Justice holds a broad view of privacy protection in this area.[53] And the division of opinion among the Justices on the Court didn't stop there. Justice Kennedy wrote a dissent (in which Justices Thomas and Alito joined), but Justices Thomas and Alito each also wrote separately (with Justice Thomas also joining Justice Alito's opinion). Each of these opinions sets forth a different potential pathway for resolving future questions about the third-party doctrine's applicability.

The various opinions suggest at least three distinct approaches to those future questions: (1) examine each new technology case-by-case, focusing on the individual's reasonable expectation of privacy even in information that an individual has shared with a third party; (2) draw a distinction (regardless of an individual's reasonable

[50] *Compare* Orin Kerr, *Does Carpenter Revolutionize the Law of Subpoenas?* LAWFARE (June 26, 2018), https://www.lawfareblog.com/does-carpenter-revolutionize-law-subpoenas, *with* Lederman, *supra*.

[51] Letter from SEC Chair Mary Jo White to the Honorable Patrick J. Leahy (Apr. 24, 2013), *available at* https://www.sec.gov/about/letters/white-leahy-letter-ecpa-042413.pdf.

[52] Slip op. at 16 (Gorsuch, J., dissenting).

[53] Lederman, *supra*.

expectation) between information the government obtains from individuals (for which it would need a warrant) and information obtained from third parties through other forms of legal process; and (3) look to external sources (*e.g.*, positive law, property law) to determine whether an individual maintains a reasonable expectation of privacy in information shared with third parties. For now, the first approach seems to have the upper hand, and all five Justices in *Carpenter*'s majority remain on the Court.

There is also, of course, another way. In the past, when difficult line-drawing questions have arisen about the application of the Fourth Amendment, Congress has enacted legislation in an attempt to balance the constitutional equities. After the Watergate-era uncovering of surveillance abuses, the Foreign Intelligence Surveillance Act weighed the Fourth Amendment's protections against the need for the government to collect information within the United States for national security and counter-intelligence purposes. Similarly, the Wiretap and Stored Communications Acts were early attempts to draft rules of the road for evidence gathering in the Digital Age. *Carpenter*'s narrow approach leaves space for Congress to reset these rules and establish a new balance between law enforcement access and individual privacy for today's records. Indeed, state legislatures have already been fairly active in this area, with various states enacting laws addressing topics from cell phone location tracking to automated license plate recognition. It remains to be seen whether Congress will follow their lead.