THE *CARPENTER* CHRONICLE: A NEAR-PERFECT SURVEILLANCE

Susan Freiwald[*] *& Stephen Wm. Smith*[**]

On May 24, 1844, a crowd gathered inside the United States Supreme Court chambers in the basement of the Capitol, eagerly awaiting a demonstration of an amazing new communication technology. They watched as inventor Samuel F.B. Morse successfully sent the first long-distance telegraph message — "What hath God wrought?" — to a railroad station near Baltimore. While earlier demonstrations of the device had successfully sent messages between the House and Senate chambers, long-distance transmission was still an open question. Congress had provided $30,000 to underwrite Morse's successful experiment.[1] That day may well have marked the last time the Supreme Court was completely in step with modern communication technology.

Technological change inevitably presents new tools for the criminally minded. Law enforcement necessarily responds by using that same technology to develop new investigative tools to combat crime. In turn, the legislative and judicial branches adapt the law to the new technology to ensure that the proper balance is maintained between security and liberty.

Unfortunately, there is often a significant lag time between the arrival of new law enforcement technologies and the laws regulating their use. Moreover, the regulatory responses of the legislative and judicial branches are typically not well coordinated, significantly adding to the time delay before a fully formed regulatory scheme is in place.[2]

Carpenter v. United States[3] is the latest installment of this cat-and-mouse regulatory game. For well over a quarter century, law enforcement has surreptitiously converted the personal cell phone into a tracking device, capable of compiling a comprehensive chronicle of the user's

---

[*] Interim Dean and Professor of Law, University of San Francisco School of Law. The author would like to thank Cera Armstrong for her extremely helpful research and editing help with this case comment.

[**] Director, Fourth Amendment & Open Courts, Center for Internet and Society, Stanford Law School. In July 2018, he retired as United States Magistrate Judge, Southern District of Texas, Houston Division.

[1] *See generally First Telegraph Messages from the Capitol*, U.S. SENATE (May 2018), https://www.senate.gov/artandhistory/history/minute/First_Telegraph_Messages_from_the_Capitol.htm [https://perma.cc/3WHW-SPHV].

[2] *See generally* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 79–83 (2004) (describing the history of the regulation of wiretapping and modern electronic surveillance); *see also* Neil Richards, *The Third Party Doctrine and the Future of the Cloud*, 94 WASH. U. L. REV. 1441, 1447–65 (2017) (chronicling "the 'Fourth Amendment lag problem,'" *id.* at 1448).

[3] 138 S. Ct. 2206 (2018).

movements over an extended period of time. Finally, the Supreme Court has confronted the constitutionality of this practice and determined that a warrant based on probable cause is required by the Fourth Amendment.[4] In doing so, the *Carpenter* Court adopted a normative approach well suited for the question presented but long avoided by lower courts.[5] It also significantly circumscribed the "third party doctrine";[6] this new limitation will no doubt reverberate throughout many decisions involving nonpublic databases that hold vast and ever-growing amounts of our digital data.[7]

Scholars debate whether the legislative or the judicial branch is better equipped to adjust the balance between security and privacy as new tools become available. In the case of cell phone tracking, both branches were slow and neither was effective, permitting millions of searches that have now been declared unconstitutional. One lesson of *Carpenter* is that courts must not be reluctant to confront the challenges of twenty-first-century technology. Another is that Congress and state legislatures need to design a better system for ensuring that law enforcement is subject to public accountability before using these powerful new surveillance tools.

I. BACKGROUND

While the result in *Carpenter* has been warmly welcomed as a landmark victory for privacy advocates,[8] it was a long time coming. To see this, and to better understand the lessons of *Carpenter* for effective regulation of new policing techniques, a brief history of tracking-device law is in order. The story begins in the 1980s, when the Supreme Court established the basic constitutional framework for tracking devices in two cases, *United States v. Knotts*[9] and *United States v. Karo*.[10] Next, the baton was passed to Congress, which enacted statutes in the 1990s acknowledging that customers had *some* right to privacy in cell phone tracking data but largely avoiding the legal standard for court orders authorizing this type of surveillance. Finally, in the mid-2000s, the issue returned to the courts, leading to the *United States v. Jones*[11] decision in 2012 and culminating now in *Carpenter*.

---

[4] *Id.* at 2221.

[5] See *infra* section II.B, pp. 219–222, for a discussion of the Court's normative approach.

[6] *See Carpenter*, 138 S. Ct. at 2219–20.

[7] See *infra* section II.D, pp. 223–227, for a discussion of the third party doctrine.

[8] *See, e.g.*, Nathan Freed Wessler, *The Supreme Court's Groundbreaking Privacy Victory for the Digital Age*, ACLU (June 22, 2018, 2:30 PM), https://www.aclu.org/blog/privacy-technology/location-tracking/supreme-courts-groundbreaking-privacy-victory-digital-age [https://perma.cc/8NYX-DPYR].

[9] 460 U.S. 276 (1983).

[10] 468 U.S. 705 (1984).

[11] 565 U.S. 400 (2012).

A. The Supreme Court's Initial Approach to Tracking

The first Supreme Court decision dealing with tracking devices was *United States v. Knotts*. The Court considered a challenge to the warrantless monitoring of a beeper within a five-gallon drum of chloroform as it was transported by car to a remote cabin in Wisconsin.[12] The Court held that, because the movements of the vehicle on public highways were "voluntarily conveyed" to anyone who cared to look,[13] such monitoring did not violate the Fourth Amendment.[14] However, the Court was careful to note the possibility of a different result if the case had involved a twenty-four-hour "dragnet-type" of surveillance.[15]

A year later, the Court in *United States v. Karo* held that law enforcement monitoring of a beeper located within a private residence did constitute a search within the meaning of the Fourth Amendment.[16] By monitoring the beeper, which was hidden within a can of ether, law enforcement obtained information — such as whether a particular article or person was within the home at a particular time — that it could not have obtained by observation from outside the house.[17] The Court rejected the Government's contention that such surveillance should be free from any Fourth Amendment constraints: "Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight."[18] In a footnote, the Court reserved the issue whether a showing of reasonable suspicion rather than probable cause should suffice to justify the search.[19]

Knotts and *Karo* brought needed clarity to the legal limits upon this law enforcement technique. A dividing line was drawn between public and private space — tracking a vehicle on a public highway was not a search, but monitoring a device within the home or other constitutionally protected space was subject to Fourth Amendment constraints. Even so, in each case the Court had left itself additional work to do — that is, deciding how the Fourth Amendment might apply to long-term surveillance in public spaces and whether probable cause is required for a warrant to monitor inside the home. This set the stage for Congress to weigh in. Nearly a quarter century would pass before the Supreme Court would revisit the subject.

---

[12] *See Knotts*, 460 U.S. at 277.
[13] *Id.* at 281.
[14] *Id.* at 285.
[15] *Id.* at 284.
[16] 468 U.S. 705, 715 (1984).
[17] *Id.* at 714–15.
[18] *Id.* at 716.
[19] *Id.* at 718 n.5.

B. Legislative Reaction: ECPA, CALEA, WCPSA, and the USA PATRIOT Act

The first federal legislation to deal with tracking devices was the Electronic Communications Privacy Act of 1986[20] (ECPA), a wide-ranging and complex statute. Briefly, Title I of the Act amended the federal wiretap statute to cover the interception of electronic communications.[21] Title II, known as the Stored Communications Act (SCA), governs law enforcement access to stored communications and customer transaction records in the hands of third party service providers.[22] Law enforcement can compel those providers to disclose customer records in response to a court order issued under 18 U.S.C. § 2703(d) (a so-called "D order").[23] Such an order must be based upon proof of "specific and articulable facts showing . . . reasonable grounds to believe that . . . the records or other information sought[] are relevant and material to an ongoing criminal investigation."[24] This "specific and articulable facts" threshold is substantially less demanding than that required for a probable cause warrant. Title III, known as the Pen/Trap Statute, covers pen registers and trap/trace devices, which record the phone numbers called and received by a target phone.[25] Because the Supreme Court in *Smith v. Maryland*[26] held such information unprotected by the Fourth Amendment,[27] the legal hurdle for a court order authorizing pen/trap surveillance is very low — a law enforcement officer need only certify that the phone numbers are relevant to an ongoing criminal investigation.[28]

A small piece of ECPA, known as the Tracking Device Statute, consists entirely of two sentences codified at 18 U.S.C. § 3117. The first sentence, subsection (a), specifies when a court may authorize the use of such a device outside its jurisdiction; the second sentence, subsection (b), defines "tracking device" in the broadest of terms: "[A]n electronic or mechanical device which permits the tracking of the movement of a person or object."[29] As finally enacted, the statute did not address the legal threshold for tracking warrants.[30] Evidently Congress was content to defer to future Supreme Court decisions to clarify the applicable

---

20 Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).
21 *See id.* §§ 101–111, 100 Stat. at 1848–59.
22 *See id.* §§ 201–202, 100 Stat. at 1860–68.
23 *See* 18 U.S.C. § 2703(d) (2012).
24 *Id.*
25 *See* Pub. L. No. 99-508, §§ 301–302, 100 Stat. at 1868–72.
26 442 U.S. 735 (1979).
27 *Id.* at 745–46.
28 18 U.S.C. §§ 3121–3127.
29 *Id.* § 3117.
30 *See id.*

Fourth Amendment standards.[31] For our purposes it is noteworthy that the statutory definition of "tracking device"[32] is sufficiently technology neutral to cover future advances in tracking technology, including cell phones.[33]

In the 1990s Congress enacted two laws specifically recognizing the capacity of a cell phone to reveal the location of its user: the Communications Assistance for Law Enforcement Act of 1994[34] (CALEA) and the Wireless Communication and Public Safety Act of 1999[35] (WCPSA). Congress passed CALEA to help law enforcement retain its existing surveillance capacities in the face of technological change in the telecommunications industry.[36] The statute requires telecommunications companies to ensure that their equipment continues to allow the government, pursuant to a court order or other lawful authorization, to access "call-identifying information" reasonably available to them.[37]

Privacy advocates challenged this assistance provision before it passed, on the ground that law enforcement would use the broad definition of call-identifying information to track cell phone users under the very lenient pen register standard.[38] Then–FBI Director Louis Freeh, the driving force behind CALEA, vigorously pushed back against this charge, disclaiming any intent to "enlarge or reduce the government's authority" for electronic surveillance.[39] To further allay the opposition's

---

[31] *See Electronic Communications Privacy Act: Hearing on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties & the Admin. of Justice of the H. Comm. on the Judiciary*, 99th Cong. 256 (1986) (statement of Clifford S. Fishman, Professor of Law, Catholic University of America Law School) (explaining that "investigators and judges often must guess" when use of electronic tracking devices constitutes a search requiring a warrant).

[32] Subsequently, Congress approved amendments to Rule 41 specifying the procedural requirements for a tracking device warrant, *see* FED. R. CRIM. P. 41, and expressly incorporated the definition of "tracking device" found in 18 U.S.C. § 3117(b), FED. R. CRIM. P. 41(a)(2)(E).

[33] *See In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 754 (S.D. Tex. 2005) [hereinafter *S. Smith I*].

[34] Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. §§ 1001–1010 (2012)).

[35] Pub. L. No. 106-81, 113 Stat. 1286 (codified as amended in scattered sections of 47 U.S.C.) (authorizing the deployment of a nationwide 9-1-1 emergency service for wireless phone users called "enhanced 9-1-1," 47 U.S.C. § 615a-1(a)).

[36] Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949, 975–76 (1996).

[37] 47 U.S.C. § 1002(a)(2).

[38] *See* Freiwald, *supra* note 36, at 976–77. Regarding the leniency of the pen register standard, see 18 U.S.C. § 3122(b)(2) (2012), which requires that pen/trap applications contain "a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency."

[39] *See Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Tech. & the Law of the S. Comm. on the Judiciary and the Subcomm. on Civil & Constitutional Rights of the H. Comm. on the Judiciary*, 103d Cong. 27 (1995) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation).

concerns, the FBI director proposed a clarifying proviso, eventually codified at 47 U.S.C. § 1002(a)(2):

> [I]nformation acquired solely pursuant to the authority for pen registers and trap and trace devices . . . shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number) . . . .[40]

This CALEA proviso marked the first explicit congressional recognition that cell site data could track the location of the phone user. The proviso makes clear that, in Congress's judgment, location data was more sensitive than the mere phone numbers dialed, and deserving of more legal protection. However, Congress did not specify exactly what legal process would be required to give law enforcement access to that data — only that mere "relevance" was not a high enough standard.[41]

The next statutory reference to call location information occurred in WCPSA, a 1999 law that authorized a nationwide emergency service for wireless phone users.[42] The Act also amended the Telecommunications Act of 1996[43] to place limits on the carrier's use or disclosure of a cell phone user's location information. Existing law already obliged the carrier to protect the confidentiality of "customer proprietary network information" (CPNI), that is, information about a customer's use of the service which the carrier acquires solely by virtue of the carrier-customer relationship.[44] In order to enhance privacy protection for wireless consumers, the new statute amended the definition of CPNI to include "location," and added the following section:

> (f) Authority to use location information.—
>
> For purposes of subsection (c)(1) of this section, *without the express prior authorization of the customer*, a customer shall not be considered to have approved the use or disclosure of or access to . . . call location information concerning the user of a commercial mobile service . . . other than in [an emergency situation].[45]

In other words, WCPSA tied certain strings to call location data, pulling them out of the realm of ordinary business records belonging solely to the carrier.[46]

---

40 47 U.S.C. § 1002(a)(2)(B).

41 *See* 18 U.S.C. § 3123(a)(1).

42 *See* 47 U.S.C. §§ 615, 615a-1.

43 Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C.).

44 *Id.* § 222(f), 110 Stat. at 149.

45 47 U.S.C. § 222(f) (emphasis added).

46 The privacy concerns animating this legislation foreshadowed those later cited by the Supreme Court in *Jones* and *Carpenter*. "[This] technology also avails wireless companies of the ability to locate and track individual's movements throughout society, where you go for your lunch break; where you drive on the weekends; the places you visit during the course of a week is your business. It is your private business, not information that wireless companies ought to collect, monitor, disclose, or use without one's approval. . . . Wherever your cell phone goes becomes a monitor of all of your activities." 145 CONG. REC. H9860 (daily ed. Oct. 12, 1999) (statement of Rep. Markey).

From these two statutes it is safe to conclude that, by the end of the twentieth century, Congress (1) understood that a cell phone could track a user's location, and (2) gave cell phone customers some control over the disclosure of their call location data. Once again, Congress did not spell out the precise legal authority (probable cause versus something less) required for law enforcement access to the data, but it did recognize that cell phone location data is entitled to more protection than phone numbers dialed.

In 2001, the USA PATRIOT Act[47] ("Patriot Act") expanded ECPA's definition of a pen register to include "dialing, routing, addressing, or signaling information transmitted by" a phone or other electronic communication device.[48] Proponents touted this amendment as a way to update the Pen/Trap Statute to cover email and other forms of electronic communication over the internet.[49] Nothing in the legislative history suggested that the new definition would alter the legal standards for tracking devices such as cell phones.[50]

C. Cell Phone Tracking in the Lower Courts

Even so, in the wake of the Patriot Act, law enforcement agencies began to seek court orders approving real-time tracking of cell site location information[51] ("CSLI"), based on what would later be dubbed a "hybrid" order.[52] These hybrid orders bore no resemblance to the probable cause Rule 41 tracking warrants traditionally used for beeper devices like those used in *Knotts* and *Karo*.[53] Instead, hybrid orders were said to be authorized by a mix of two very different parts of ECPA — the Pen/Trap Statute and the SCA.[54] Under the hybrid theory, law enforcement could prospectively monitor a cell phone user's location for up to sixty days (similar to a pen/trap order) based on a showing of

---

Other members expressed similar worries. *E.g.*, *id.* at H9862 (statement of Rep. Green) ("[W]e do not want Big Brother looking over our shoulders . . . .").

47 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of the U.S. Code).

48 *Id.* § 216(c)(2), 115 Stat. at 290. The amendment included a similar expansion of the definition of "trap and trace device." *Id.* § 216(c)(3), 115 Stat. at 290.

49 *See* 147 CONG. REC. S11,006–07 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy); 147 CONG. REC. H7197 (daily ed. Oct. 23, 2001) (statement of Rep. Conyers).

50 *S. Smith 1*, *supra* note 33, at 761.

51 As explained in the *Carpenter* opinion, cell phones function by continuously connecting to a set of radio antennas called cell sites. 138 S. Ct. at 2211–12. Each time a mobile phone signal connects to a cell site, it generates a time-stamped record known as cell site location information, or CSLI. *Id.*

52 Patricia L. Bellia, *The Memory Gap in Surveillance Law*, 75 U. CHI. L. REV. 137, 160–61 (2008) (explaining that law enforcement officials relied upon invoking "pen/trap provisions as well as provisions in the SCA," *id.* at 160, to compel production of location data without a warrant).

53 *See* FED. R. CRIM. P. 41.

54 For a discussion of the Pen/Trap Statute and the SCA, see *supra* text accompanying notes 22–25.

specific and articulable facts (similar to a D order) rather than probable cause.[55]

According to law enforcement, then, cell phones were not subject to the statutory and constitutional constraints upon other location monitoring devices, like the beepers used in *Knotts* or *Karo*. Best of all, these devices were voluntarily carried by the targets themselves — installation was a simple matter of a few keystrokes or flipped switches at the provider's end, as opposed to surreptitious entry on private property at night.[56]

For several years, judges approved these novel hybrid orders without challenge. In the latter half of 2005, a handful of federal magistrate judges finally began to question the legal underpinnings of these tracking orders, as a matter of both statutory interpretation and constitutional law.[57] The nub of their concern was that nothing in ECPA or its amendments expressly authorized separate legal standards for tracking by cell phone.[58] A cell phone easily fits within the technology-neutral definition in the Tracking Device Statute.[59] According to these magistrate judges, if Congress had intended to create an entirely new regime of electronic surveillance by cell phone, it chose a perversely complicated way of going about it.[60] One magistrate judge compared the hybrid theory to a

---

[55] *See, e.g.*, *In re* Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register and a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 396 F. Supp. 2d 294, 296–97 (E.D.N.Y. 2005) [hereinafter *Orenstein 1*].

[56] *See ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights & Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 30 (2010) (statement of Matt Blaze, Associate Professor, University of Pennsylvania) [hereinafter *June 2010 Location Hearing*] ("[T]he 'tracking device' is now a benign object already carried by the target — his or her own telephone."); Michael Isikoff, *FBI Tracks Suspects' Cell Phones Without a Warrant,* NEWSWEEK (Feb. 19, 2010, 7:00 PM), https://www.newsweek.com/fbi-tracks-suspects-cell-phones-without-warrant-75099 [https://perma.cc/S45X-9U9F] (describing Sprint's "dedicated website" allowing law enforcement to access location records "from their desks").

[57] *See, e.g.*, *S. Smith 1*, *supra* note 33, at 753–65. This was actually the second published opinion on the topic. Magistrate Judge Orenstein had issued a decision reaching the same conclusion two months earlier, but the government had not presented the hybrid argument in support of that application. *See Orenstein 1*, *supra* note 55, at 295–98. A comprehensive critique of the hybrid theory may be found at *In re Application of the U.S. for an Order Authorizing (1) Installation and Use of a Pen Register and Trap & Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking*, 441 F. Supp. 2d 816, 827–36 (S.D. Tex. 2006).

[58] *See, e.g.*, *S. Smith 1*, *supra* note 33, at 757 ("Because the government cannot demonstrate that cell site tracking could never under any circumstance implicate Fourth Amendment privacy rights, there is no reason to treat cell phone tracking differently from other forms of tracking under 18 U.S.C. § 3117, which routinely require probable cause.").

[59] *See* 18 U.S.C. § 3117(b) (2012) ("As used in this section, the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object.").

[60] *See, e.g.*, *Orenstein 1*, *supra* note 55, at 313–14 (concluding that allowing the government to "bypass the super-warrant requirement applicable to the interception of wire and electronic communications . . . by describing [them] as 'electronic storage' . . . would plainly frustrate the intent of Congress in enacting and repeatedly preserving" certain requirements of Title III of ECPA).

"three-rail bank shot" that was little more than "a retrospective assemblage of disparate statutory parts to achieve a desired result."[61] As he explained:

> The most glaring difficulty in meshing these disparate statutory provisions is that with a single exception they do not cross-reference one another. . . . CALEA does refer to the Pen/Trap Statute, but only in the negative sense of disclaiming its applicability. Surely if these various statutory provisions were intended to give birth to a new breed of electronic surveillance, one would expect Congress to have openly acknowledged paternity somewhere along the way.[62]

Other magistrate judges (as well as a few district judges) soon began to weigh in with published decisions of their own. The government's hybrid theory was rejected by the majority of these cases, in various jurisdictions around the country.[63]

Instead of appealing these adverse magistrate judge rulings on prospective CSLI, the Department of Justice (DOJ) retreated from its stance on real-time precise tracking of cell phones via GPS or multiple cell-tower data. In such cases, the DOJ began seeking "precise location warrants" under Rule 41 based on probable cause.[64]

In practice this was not as big a retreat as might otherwise appear, because the government continued to request and receive limited CSLI data (that is, data from the single tower connecting the phone at the beginning and end of the call) as a customer record based on a D Order. In earlier years, providers maintained CSLI records for only a short period of time, usually a matter of weeks.[65] Fortunately for law enforcement, telecoms were now moving toward longer retention periods of a year or more, as companies saw the potential for huge profits by monetizing such location data, and the costs of data storage continued to plummet.[66] Moreover, by invoking the mantle of business records,[67] the

---

[61] *S. Smith 1*, *supra* note 33, at 765.

[62] *Id.* at 764.

[63] *June 2010 Location Hearing*, *supra* note 56, at 81, 93 Ex. B. Jurisdictions that rejected the hybrid theory included Brooklyn, Manhattan, Baltimore, Boston, Washington, D.C., Fort Wayne (Indiana), Milwaukee, Austin, Corpus Christi, Houston, Pittsburgh, and Puerto Rico. *Id.* at 93 Ex. B.

[64] Even so, the government was careful not to describe these as tracking warrants, and avoided using the standard tracking warrant application forms prescribed by the Administrative Office. *See, e.g.*, *In re* Application of the U.S. for an Order Authorizing Prospective & Continuous Release of Cell Site Location Records, 31 F. Supp. 3d 889, 899 n.51 (S.D. Tex. 2014).

[65] *See* Telephone Interview with Michael Sussman, Partner, Perkins Coie LLP; Albert Gidari, Jr., Partner, Perkins Coie LLP; and Michael McAdoo, Dir., Law Enf't Compliance, T-Mobile USA, Inc. (Feb. 7, 2006).

[66] *See June 2010 Location Hearing*, *supra* note 56, at 27–28 (statement of Matt Blaze, Associate Professor, University of Pennsylvania).

[67] The government also began to expand the definition of historical CSLI, taking the view that location data associated with cell phone use becomes a "record" for purposes of the SCA as soon as it is captured and digitally resides on the provider's system. *See Orenstein 1*, *supra* note 55, at 312.

government could take advantage of the so-called "third party doctrine." Under a broad view of that doctrine, if a person knowingly and voluntarily provides information to a "third party" (for example, a bank or phone company), that person has no reasonable expectation of privacy in the information she has shared.[68] Until *Carpenter*, that doctrine was the government's strongest legal argument against any Fourth Amendment protection for this tracking data.

One of the first opinions to challenge the acquisition of historical CSLI came in 2008. The Western District of Pennsylvania — in an opinion signed by all five magistrate judges — ruled that no form of historical cell site data was obtainable under a D Order, reasoning that ECPA's text and legislative history drew no "distinction between real-time ('prospective') and stored ('historic') cell-phone-derived movement/location information."[69] The court rejected the application of the third party doctrine of *Smith v. Maryland* on the ground that the customer had not voluntarily and knowingly shared her CSLI with her provider and so had not assumed the risk of its disclosure.[70]

The government promptly appealed the district court order affirming this decision to the Third Circuit, marking the first time an appellate court considered law enforcement access to CSLI.[71] However, that court dodged the constitutional issue. Construing the SCA, the court held that magistrate judges had discretionary authority to require a warrant for such data when necessary, but offered no guidance on exercising that discretion.[72]

In 2010, Magistrate Judge Orenstein, who had authored the very first cell site opinion,[73] issued a new opinion rejecting an application for a D Order for historical cell site data,[74] relying on the recent decision of the

---

This "instantaneous storage" theory effectively erases any meaningful distinction between prospective and historical CSLI. *Id.*

[68] *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).

[69] *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 601 (W.D. Pa. 2008) [hereinafter *Lenihan*] (writing on behalf of all magistrate judges in the district), *aff'd*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), *vacated*, 620 F.3d 304 (3d Cir. 2010).

[70] *Id.* at 614–15.

[71] In 2000, the D.C. Circuit affirmed an order of the FCC requiring that location data be included within the CALEA assistance standard for telecom manufacturers. U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 463–64 (D.C. Cir. 2000). The court did not address the question of the legal standard for government access to that data. *See id.* For an interesting overview of the lengthy CALEA standards process from the providers' perspective, see Albert Gidari, Jr., Keynote Address, *Companies Caught in the Middle*, 41 U.S.F. L. REV. 535 (2007).

[72] 620 F.3d at 319.

[73] *See supra* note 57.

[74] *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 736 F. Supp. 2d 578, 589 (E.D.N.Y. 2010) [hereinafter *Orenstein 2*] (unpublished order noting written opinion to follow), *rev'd*, No. 10-MC-0550 (E.D.N.Y. Nov. 29, 2010).

D.C. Circuit in *United States v. Maynard*.[75] Judge Orenstein agreed with *Maynard*'s conclusion "that people in this country have a reasonable expectation of privacy in their movements over extended periods of time."[76] A few months later, a Houston magistrate judge, one of the authors of this Comment, issued an opinion reaching the same result, relying not only upon the prolonged surveillance doctrine of *Maynard* but also upon recent advances in the precision of location-based technology.[77] Such advances made it inevitable that cell site data would reveal nonpublic information from inside a home or other constitutionally protected space, in violation of the tracking device ruling in *United States v. Karo*.[78] The government appealed to the Fifth Circuit.

Directly confronting the Fourth Amendment question, the Fifth Circuit held that orders for historical cell records under the SCA did not "categorically" violate the Fourth Amendment.[79] The panel majority reasoned that cell site records were ordinary business records in which the customer had no reasonable expectation of privacy, explicitly relying upon the third party doctrine of *United States v. Miller*[80] and *Smith v. Maryland*.[81] In *Miller*, the Supreme Court had found no Fourth Amendment search when the government subpoenaed the defendant's bank records, including his deposit slips, transaction statements, and check copies stored by his bank.[82] Similarly, the *Smith* Court found no Fourth Amendment search when the government had the phone company install a pen register to obtain a paper record of the telephone numbers that Smith dialed when placing telephone calls from his landline phone.[83]

---

[75] 615 F.3d 544 (D.C. Cir. 2010). This decision was ultimately taken to the Supreme Court in *United States v. Jones*, 565 U.S. 400 (2012), which affirmed on different grounds. Across two concurring opinions, five Justices agreed with the lower court's reasoning that GPS monitoring of a vehicle's movements over twenty-eight days impinges on a reasonable expectation of privacy, even if those movements were disclosed to the public at large. *Id.* at 430 (Alito, J., concurring in the judgment); *id.* at 415 (Sotomayor, J., concurring).

[76] *Orenstein 2*, *supra* note 74, at 593; *see also* Orin Kerr, *Fourth Amendment Stunner: Judge Rules that Cell-Site Data Protected by Fourth Amendment Warrant Requirement*, VOLOKH CONSPIRACY (Aug. 31, 2010, 2:46 AM), http://volokh.com/2010/08/31/fourth-amendment-stunner-judge-rules-that-cell-site-data-protected-by-fourth-amendment-warrant-requirement/ [https://perma.cc/3FTR-CV8Q]. No appeal was taken from this decision.

[77] *In re* Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 835–40 (S.D. Tex. 2010), *vacated*, 724 F.3d 600 (5th Cir. 2013) [hereinafter *S. Smith 2*].

[78] *Id.* at 836–37. District Judge Hughes affirmed the decision. *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d at 602–03.

[79] *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d at 615.

[80] 425 U.S. 435, 443 (1976).

[81] 442 U.S. 735, 743–44 (1979); *see In re Application of the U.S. for Historical Cell Site Data* 724 F.3d at 611–15.

[82] *Miller*, 425 U.S. at 437–38.

[83] *Smith*, 442 U.S. at 737, 745–46.

Other circuits soon followed the Fifth Circuit's lead in finding no reasonable expectation of privacy in cell site location records.[84] Unlike the Fifth Circuit decision, which arose from a magistrate judge's denial of the initial application, each of the later circuit cases arose in the context of a motion to suppress CSLI and related evidence at trial.[85] Like the Fifth Circuit,[86] each court assumed that the SCA authorized the production of the cell phone user's call location data,[87] and ignored the statutory protections for such data contained in CALEA and WCPSA. Despite a smattering of dissenting opinions,[88] each court ultimately sided with the Fifth Circuit by deciding that the third party rule of *Smith* and *Miller* applied to cell site data and compelled a rejection of the Fourth Amendment claim.[89] In the summer of 2017, despite the lack of a circuit split on the Fourth Amendment question, the Supreme Court granted certiorari to review the Sixth Circuit decision in *Carpenter v. United States*.[90]

II. THE DECISION

Carpenter is the latest in a trilogy of decisions in which the Supreme Court has finally begun to confront modern surveillance tools used by law enforcement. The first of these was the 2012 decision in *United States v. Jones*. FBI agents had installed a GPS tracking device on the defendant's vehicle and remotely monitored the vehicle's movements for twenty-eight days.[91] Writing for the Court, Justice Scalia found the installation and use of the device to be a Fourth Amendment search based on the government's physical trespass of the vehicle.[92] At the same time, five Justices agreed that surreptitious long-term monitoring of the vehicle also impinged on reasonable expectations of privacy, even if those movements were in public view.[93] In 2014, in *Riley v. California*,[94] the Court considered the warrantless search of a cell phone incident to an

---

[84] *See* United States v. Thompson, 866 F.3d 1149, 1160 (10th Cir. 2017); United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016) (en banc); United States v. Carpenter, 819 F.3d 880, 890 (6th Cir. 2016), *rev'd*, 138 S. Ct. 2206; United States v. Davis, 785 F.3d 498, 517 (11th Cir. 2015) (en banc).

[85] *Carpenter*, 819 F.3d at 884; United States v. Graham, 796 F.3d 332, 341 (4th Cir. 2015), *rev'd en banc*, 824 F.3d 421; *Davis*, 785 F.3d at 500.

[86] *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 606 (5th Cir. 2013).

[87] *See Thompson*, 866 F.3d at 1152; *Graham*, 824 F.3d at 437; *Carpenter*, 819 F.3d at 886; *Davis*, 785 F.3d at 511.

[88] *Graham*, 824 F.3d at 441 (Wynn, J., dissenting in part and concurring in the judgment); *Davis*, 785 F.3d at 533 (Martin, J., dissenting).

[89] *See Thompson*, 866 F.3d at 1158; *Graham*, 824 F.3d at 427; *Carpenter*, 819 F.3d at 887; *Davis*, 785 F.3d at 511–13.

[90] Carpenter v. United States, 137 S. Ct. 2211 (2017) (mem.).

[91] United States v. Jones, 565 U.S. 400, 403 (2012).

[92] *Id.* at 404–05.

[93] *See id.* at 415 (Sotomayor, J., concurring); *id.* at 430 (Alito, J., concurring in the judgment).

[94] 134 S. Ct. 2473 (2014).

arrest.[95] Recognizing that the cell phone is a unique device with a vast store of sensitive information, the Court unanimously held that police officers generally must obtain a warrant before searching the contents of a phone.[96] In *Carpenter*, the Court was faced with a blend of those two cases — long-term surreptitious tracking (*Jones*) by a uniquely powerful device (*Riley*) capable of near-perfect surveillance.

A. Overview

In 2011, several RadioShack and T-Mobile stores were robbed in Ohio and Michigan.[97] Police arrested four men suspected of participating in those robberies.[98] From one of those suspects, the police learned of several more accomplices and their cell phone numbers.[99] With that information, prosecutors obtained two court orders for location tracking data from the cell phones of several suspects, including Timothy Carpenter.[100] One order sought records for 152 days of calls but yielded records spanning 127 days from MetroPCS.[101] The second order requested seven days of records but yielded data for two days from Sprint.[102] Together, the data furnished prosecutors with "12,898 location points cataloging Carpenter's movements — an average of 101 data points per day."[103]

Before trial, Carpenter moved to suppress that cell site data.[104] Carpenter had argued that the collection of this data was a search under the Fourth Amendment and that therefore the police were required to obtain a warrant based on probable cause, whereas they had merely satisfied the "reasonable grounds" standard of a D Order under the SCA.[105] This argument was rejected, and Carpenter was ultimately convicted and sentenced to over 100 years for robbery and firearms offenses.[106]

On appeal, the Sixth Circuit affirmed, holding that Carpenter lacked a reasonable expectation of privacy in his cell phone location data be-

---

[95] *Id.* at 2484.
[96] *Id.* at 2494–95.
[97] *Carpenter*, 138 S. Ct. at 2212.
[98] *Id.*
[99] *Id.*
[100] *Id.*
[101] *Id.*
[102] *Id.*
[103] *Id.*; *see also* Stephen E. Henderson, Carpenter v. United States *and the Fourth Amendment: The Best Way Forward*, 26 WM. & MARY BILL RTS. J. 495, 496–502 (2017) (providing background on the decision and an explanation of the way the providers gathered Carpenter's CSLI).
[104] *Carpenter*, 138 S. Ct. at 2212.
[105] *Id.*; *see also* Brief for Petitioner at 47–48, *Carpenter*, 138 S. Ct. 2206 (No. 16-402); *supra* text accompanying note 24 (quoting the D Order standard).
[106] *Carpenter*, 138 S. Ct. at 2213.

cause it was noncontent information that he had shared with his wireless carriers.[107]

Writing for the Supreme Court in a 5–4 decision, Chief Justice Roberts held the acquisition of CSLI to be a search under the "reasonable expectation of privacy" doctrine.[108] The Chief Justice applied the test articulated in *Katz v. United States*,[109] under which a government official conducts a Fourth Amendment search when the official intrudes into a "private sphere" in which "an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable.'"[110] In addition, the majority found that cell site records, due to their unique and revealing nature, were not subject to the third party doctrine of *Smith* and *Miller*.[111]

After finding a Fourth Amendment search, the Court quickly dispatched the warrant question. Reaffirming the warrant requirement as the default rule for a Fourth Amendment search,[112] the Court clarified that reasonableness requires a warrant or a warrant exception for law enforcement searches to uncover evidence of crimes.[113]

Chief Justice Roberts's opinion attracted enough votes — from Justices Ginsburg, Breyer, Sotomayor, and Kagan — to achieve a majority.[114] But the case also generated four separate dissents.[115] Justice Kennedy dissented on the ground that CSLI should fall within the scope of the third party doctrine.[116] He argued that the majority had drawn an "illogical" distinction between CSLI and other phone or credit card records.[117] Justice Alito dissented on the ground that CSLI acquisition may be compelled by a subpoena subject to relevance review.[118] Justice Thomas's dissent rejected the *Katz* test as inconsistent with the Fourth Amendment, properly understood, and found that Carpenter lacked a claim under a strictly property-based approach.[119] Justice Gorsuch stood completely alone, neither joining the other dissenters nor having

---

107 United States v. Carpenter, 819 F.3d 880, 886–90 (6th Cir. 2016).

108 *Carpenter*, 138 S. Ct. at 2222–23.

109 389 U.S. 347 (1967).

110 *Carpenter*, 138 S. Ct. at 2213 (alteration and internal quotation marks omitted in original) (quoting Smith v. Maryland, 442 U.S. 735, 740 (1979)).

111 *Id.* at 2217.

112 *Id.* at 2221.

113 *Id.* This holding clearly signals the answer to the question left open in *Jones*, which failed to specify the procedure required for GPS tracking searches. The answer is the same as in *Riley*: get a warrant. *See Carpenter*, 138 S. Ct. at 2215, 2217 (approving of the *Jones* concurrences' assertions that long-term GPS monitoring of public movements impinges on expectations of privacy, which would make a warrant necessary).

114 *Id.* at 2211.

115 *Id.*

116 *Id.* at 2223–24 (Kennedy, J., dissenting).

117 *Id.* at 2224.

118 *See id.* at 2255 (Alito, J., dissenting).

119 *See id.* at 2235–36 (Thomas, J., dissenting).

them join him. He rejected both the third party doctrine and the *Katz* approach; however, he was openly sympathetic to a property-based argument for Fourth Amendment protection based on the WCPSA, but found the argument had been forfeited due to insufficient development in the courts below.[120]

B. The Multifactor Analysis

In adding flesh to the bones of the reasonable expectation of privacy test, the majority evaluated several factors of CSLI acquisition to determine whether CSLI acquisition is a search under the Fourth Amendment.[121] The Court included in its multifactor analysis several familiar factors that courts had used to decide Fourth Amendment requirements applicable to such surveillance techniques as bugging, wiretaps, video surveillance, and email acquisitions.[122] In those cases, courts inquired whether the technique was (1) *hidden*, (2) *continuous*, (3) *indiscriminate*, and (4) *intrusive*.[123] Although the Court did not list these four factors explicitly, they were clearly central to its holding, together with the expense and effort required to compile the data.[124]

1. Hidden. — The Court expressed concern over this feature of CSLI acquisition, declaring that government access to CSLI contravenes society's expectation "that law enforcement agents and others would not . . . *secretly* monitor and catalogue" a person's every movement.[125] Hidden surveillance requires procedural hurdles to keep it in check because it lacks the safeguards that exposure provides to more public forms of surveillance.[126]

2. Continuous. — The Court then called attention to the continuity of CSLI acquisition, explaining that the retrospective nature of CSLI permits the government to "travel back in time to retrace a person's

---

[120] *See id.* at 2264, 2267–68, 2272 (Gorsuch, J., dissenting).

[121] *See id.* at 2234 (Kennedy, J., dissenting) (recognizing that the majority conducted a "multifactor analysis"). The majority recognized that individuals do have a reasonable expectation of privacy in CSLI despite disclosure to a third party, whereas in *Smith* and *Miller* no reasonable expectation of privacy existed. *See id.* at 2216–17 (majority opinion).

[122] *See id.* at 2216–20; *see also* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 745–46 (2011).

[123] *See* Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, 5 n.20, 15–18 (describing these four principles and collecting cases illustrating their importance to appellate courts).

[124] *See Carpenter*, 138 S. Ct. at 2215–16; *see also* Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents out of* United States v. Jones, 123 YALE L.J. ONLINE 335, 348–49 (2014).

[125] *Carpenter*, 138 S. Ct. at 2217 (emphasis added) (quoting United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring in the judgment)).

[126] *See, e.g.*, Berger v. New York, 388 U.S. 41, 56, 60 (1967).

whereabouts" for the amount of time the providers retain the records.[127] The suspect "has effectively been tailed every moment of every day for five years."[128]

3. Indiscriminate. — The Court described acquired CSLI as "all-encompassing," which raises the risk that nonincriminating information about the subject or others will be revealed.[129] In fact, location information "is continually logged for all of the 400 million devices in the United States — not just those belonging to persons who might happen to come under investigation."[130] That poses the danger of government fishing expeditions through databases, just as the British had threatened the security of the Founders with the abusive general warrants and writs of assistance that originally inspired the Fourth Amendment.[131]

4. Intrusive. — The Court's biggest concern was the intrusiveness of CSLI disclosure. The method furnishes "an intimate window into a person's life,"[132] as well as "deeply revealing"[133] information about families, politics, religion, health, professions, and sex partners.[134] Relying on statistics about how Americans use their cell phones, the Court compared tracking a cell phone to attaching an ankle monitor to the user of the phone.[135]

5. Expense and efficiency. — The fact that it is so cheap and efficient to obtain CSLI means that with a short amount of time and limited resources, law enforcement may acquire a tremendous amount of information that, using more traditional techniques, would have taken much longer and cost much more to acquire. In effect, the new method dispenses with friction as a source of privacy protection.[136] It also illus-

---

127 *Carpenter*, 138 S. Ct. at 2218; *see also S. Smith 2*, *supra* note 77, at 839–40; Freiwald, *supra* note 122, at 738–40.

128 *Carpenter*, 138 S. Ct. at 2218. Five years is a reference to the providers' data retention period. *Id.*

129 *Id.* at 2217.

130 *Id.* at 2218 (noting further that "this newfound tracking capacity runs against everyone"); *see id.* (noting that, should the Court adopt the Government's view, "[o]nly the few without cell phones could escape this tireless and absolute surveillance"); *id.* at 2219 (noting that CSLI tracking is possible "of not only Carpenter's location but also everyone else's").

131 *See* Henry F. Fradella et al., *Quantifying* Katz*: Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289, 326–27 (2011). Note that while the Court referenced the need to be mindful of "Founding-era understandings" of the Fourth Amendment, *Carpenter*, 138 S. Ct. at 2214, a discussion of surveillance practices in the Founding era is entirely lacking from the majority's opinion.

132 *Carpenter*, 138 S. Ct. at 2217.

133 *Id.* at 2223.

134 *Id.* at 2217.

135 *Id.* at 2218.

136 *See* Bankston & Soltani, *supra* note 124, at 337; Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1345 (2015).

trates, as in *Riley*, how a quantitative difference can become a qualitative difference with new technology.[137] The difference in the power of the surveillance simply cannot be ignored. The Court evinced concern about these realities when it described CSLI as "remarkably easy, cheap, and efficient compared to traditional investigative tools."[138]

In sum, the Court seized upon both the sensitivity of CSLI and the problematic nature of the method by which law enforcement agencies acquire it.[139] Those complementary rationales mean that focusing only on the nature of the records themselves misses an essential part of the Court's analysis. The majority held that the Fourth Amendment is implicated not only because CSLI is too revealing but also because, when agents acquire CSLI, either by working with the providers *or by using their own devices*, they achieve surveillance that is "near perfect" due to its hidden, continuous, and indiscriminate nature.[140] The *Carpenter* Court generalized a reasonable expectation of privacy in "the whole of [a person's] physical movements"[141] and held that law enforcement agents intrude on those expectations when they secretly monitor and catalogue an individual's "every single movement" by acquiring CSLI.[142]

Justice Harlan, the author of the concurrence in *Katz* that established the reasonable expectation of privacy test,[143] recognized the truth: the *Katz* test requires judges to make a normative judgment about what should be private.[144] According to Justice Harlan, "[t]he critical question . . . is whether under our system of government, as reflected in the Constitution, we *should* impose on our citizens the risks of the electronic

---

137 *See* Riley v. California, 134 S. Ct. 2473, 2489–91 (2014).

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

139 *Cf.* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 71–72 (2013) (advocating a focus on the method of surveillance in determining Fourth Amendment constraints).

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

141 *Id.* at 2217.

142 *Id.* (quoting United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring in the judgment)); *see also id.* at 2219 ("Accordingly, when the Government accessed CSLI from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements.").

143 *See* Katz v. United States, 389 U.S. 347, 360–62 (1967) (Harlan, J., concurring).

144 United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting); *see also* Henderson, *supra* note 103, at 515–17; Susan N. Herman, *The USA PATRIOT Act and the Submajoritarian Fourth Amendment*, 41 HARV. C.R.-C.L. L. REV. 67, 110–11 (2006); Richards, *supra* note 2, at 1487–88. The Court had implicitly recognized as much when it later described *Katz* as having turned on the defendant's *justifiable reliance* on the privacy of the public telephone booth from which he placed his calls. *See* Kyllo v. United States, 533 U.S. 27, 33–34 (2001); *see also* United States v. Warshak, 631 F.3d 266, 285–86 (6th Cir. 2010) (using normative language in finding an email acquisition a Fourth Amendment search).

listener or observer without at least the protection of a warrant requirement."[145] The *Carpenter* Court fully embraced the normative approach of *Katz*.[146]

C. Rubrics Not Taken

At the beginning of the majority opinion, Chief Justice Roberts acknowledged that "no single rubric definitively resolves which expectations of privacy are entitled to protection."[147] This was perhaps a tacit recognition that the *Katz* test provides little to tether an inquiry, as Justice Gorsuch lamented in his dissent.[148]

The multifactor analysis provides a framework for what to consider when applying the reasonable expectation of privacy test, but the approach nonetheless depends upon the Justices' own views about the nature of the surveillance method. That is a normative approach, rather than one that would ground a reasonable expectation of privacy analysis on positive law reflected elsewhere,[149] or empirical studies of people's actual expectations.[150] It is also not an originalist one, as Justice Thomas would have preferred.[151] Nor is it a textual approach that insists that the interest intruded upon be one of the categories explicitly mentioned in the Fourth Amendment. In *Jones*, the Court had found a physical intrusion on an "effect," the car.[152] Another mode of analysis not followed was the public versus private space distinction that had proven decisive in *Karo*;[153] indeed, *Karo* was not even cited by the majority.

---

145 *White*, 401 U.S. at 786 (emphasis added); *see also* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 403 (1974) ("The ultimate question . . . is a value judgment.").

146 *See Carpenter*, 138 S. Ct. at 2217.

147 *Id.* at 2213–14.

148 *Id.* at 2264–66 (Gorsuch, J., dissenting). Many critics have complained about the circularity of the *Katz* approach, which requires courts to determine reasonable expectations of privacy based on what is reasonable. *See, e.g.*, *Kyllo*, 533 U.S. at 34 (listing a number of sources that criticize the *Katz* test as circular).

149 *See, e.g.*, Wireless Communication and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286 (codified as amended at scattered sections of 47 U.S.C.).

150 *See, e.g.*, Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727, 732, 740–42 (1993); Fradella et al., *supra* note 131, at 343–71.

151 *See Carpenter*, 138 S. Ct at 2236–44 (Thomas, J., dissenting); *id.* at 2247 (Alito, J., dissenting); *see also* Herman, *supra* note 144, at 123–24 (discussing how Justice Scalia adopted an originalist approach in *Kyllo* to find thermal imaging of a home to be a Fourth Amendment search).

152 United States v. Jones, 565 U.S. 400, 404 (2012). The *Jones* Court recognized that nontrespassory acquisitions of location data would involve a *Katz* analysis, but it put off conducting that analysis and the "thorny problems," *id.* at 412, associated with it for another day. *Id.* at 411–13. With *Carpenter*, that day arrived.

153 *See* United States v. Karo, 468 U.S. 705, 713–15 (1984).

The Court further chose to disregard the facile content versus noncontent framework adopted by the Sixth Circuit below and urged by the Government and its supporting amici.[154]

The Court did not defer to the legislature, as advocated by several of the dissenters.[155] As we have seen, this approach is flawed. Congress has long recognized the cell phone tracking problem but was content to legislate on the margins, deferring to courts on the hard question of legal standards. The dissenters assumed (because it had been uncontested below) that CSLI was included within the customer records covered by D orders, but there is good reason to doubt it. The SCA does not mention CSLI, nor does it refer to user data. While civil liberties advocates had for tactical reasons refrained from making this argument in court, it seems far more plausible that the SCA really did not apply to CSLI at all.[156]

D. Reining in the Third Party Doctrine

The *Carpenter* majority found that the third party doctrine placed no obstacle in the way of Fourth Amendment regulation of CSLI acquisition, contrary to the judgment of all five circuit courts that had considered the issue.[157]

Many courts and commentators have too literally interpreted the *Smith* Court's statement that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[158] That broad reading holds that virtually any investigative method that

---

[154] *See* Henderson, *supra* note 103, at 504–05 (describing that distinction); *see also* Brief for the United States at 36–38, *Carpenter*, 138 S. Ct. 2206 (No. 16-402); *Amicus Curiae* Brief for National District Attorneys Association in Support of Respondent at 10, *Carpenter*, 138 S. Ct. 2206 (No. 16-402); Brief of Professor Orin S. Kerr as Amicus Curiae in Support of Respondent at 4, *Carpenter*, 138 S. Ct. 2206 (No. 16-402).

[155] *See, e.g.*, *Carpenter*, 138 S. Ct. at 2265 (Gorsuch, J., dissenting); *see also Jones*, 565 U.S. at 429–30 (Alito, J., concurring in the judgment).

[156] *See In re* Application of the U.S. for an Order Authorizing Prospective & Continuous Release of Cell Site Location Records, 31 F. Supp. 3d 889, 892 n.11 (S.D. Tex. 2014); Nathaniel Gleicher, Comment, *Neither a Customer Nor a Subscriber Be: Regulating the Release of User Information on the World Wide Web*, 118 YALE L.J. 1945, 1950–52 (2009) (noting ambiguity in the SCA phrase "customer of or subscriber to"); Recent Case, In re Application of the United States for Historical Cell Site Data, *724 F.3d 600 (5th Cir. 2013)*, 127 HARV. L. REV. 1220, 1226–27 (2014); *cf. In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register with Caller Identification Device and Cell Site Location Auth. on a Certain Cellular Tel., 415 F. Supp. 2d 663, 666 (S.D. W. Va. 2006) (holding that CALEA proviso's reference to "subscriber" did not protect phone users who were not subscribers).

[157] *See, e.g.*, United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016) (relying on the third party doctrine as applied in *Smith v. Maryland*, 442 U.S. 735 (1979)), *rev'd and remanded*, 138 S. Ct. 2206; United States v. Davis, 785 F.3d 498, 511 (11th Cir. 2015) (en banc); *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 614 (5th Cir. 2013).

[158] *See Carpenter*, 138 S. Ct. at 2216 (quoting *Smith*, 442 U.S. at 743–44). The expectation is lost by voluntary sharing, "even if the information is revealed on the assumption that it will be used only for a limited purpose." *Id.* (quoting United States v. Miller, 425 U.S. 435, 443 (1976)).

involves acquiring information from a third party rather than the target of the investigation falls outside the Fourth Amendment.[159] Following that approach, law enforcement acquisition of CSLI is not a search, because agents obtain the information from third party cell phone service providers.[160]

The *Carpenter* Court dispensed with that overbroad reading and significantly narrowed the doctrine's scope. First, the Court distinguished records obtained in *Carpenter* from those at issue in *Miller* and *Smith*.[161] Miller had exposed negotiable instruments used in commercial transactions to bank employees in the ordinary course of their jobs.[162] In *Smith*, the pen register determined only the numbers dialed on a landline telephone.[163] By contrast, Carpenter's providers collected CSLI without his involvement and painted a detailed picture of his life.[164] Due to the "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,"[165] the majority concluded that the government's request for CSLI was a significant and inappropriate extension of the third party cases.[166]

The Court went back to the principles underlying the third party cases, as it had done in *Riley v. California* with the search-incident-to-arrest exception to the warrant requirement. *Riley* had found searches of cell phones as different from searches of other physical objects carried in pockets as a trip to the moon is from a horseback ride.[167] The *Riley* Court therefore rejected mechanical application of that exception to cell phone searches and returned to the principles from which the doctrine had been derived. The principle underlying third party cases was the assumption of risk inherent in voluntarily and knowingly sharing one's data with a third party. The assumption of risk framework rests on a

---

159 *See id.* at 2262 (Gorsuch, J., dissenting) (asserting that "*Smith* and *Miller* teach that the police can review" a host of private information about us so long as it "reside[s] on third party servers").

160 *See, e.g.*, *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d at 610–11.

161 *Carpenter*, 138 S. Ct. at 2217.

162 *Id.* at 2216.

163 *Id.*

164 *Id.* at 2216, 2218–20. It is worth arguing, as Justice Brennan did in *Miller*, that bank records can also provide a detailed view of a person's behavior and associations, but that argument did not prevail in *Miller*. United States v. Miller, 425 U.S. 435, 451 (1976) (Brennan, J., dissenting).

165 *Carpenter*, 138 S. Ct. at 2219.

166 *Id.* at 2220 (finding that the detailed chronicle of CSLI "implicate[d] privacy concerns far beyond those considered in *Smith* and *Miller*").

167 Riley v. California, 134 S. Ct. 2473, 2488 (2014) ("The United States asserts that a search of all data stored on a cell phone is 'materially indistinguishable' from searches of these sorts of physical items. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon." (citation omitted)).

shaky foundation; the precedents upon which it is based do not support it, and neither *Smith*'s nor *Miller*'s facts fit well within it.[168]

Rather than questioning the premises of the assumption of risk approach, however, the *Carpenter* majority merely held it inapplicable to CSLI. The Court disagreed with the five circuits that had equated the decision to use a cell phone with voluntarily and knowingly sharing one's CSLI with one's provider.[169] The majority held that Carpenter had not knowingly and voluntarily shared his CSLI with his provider because CSLI was automatically generated by the provider, so the only way to have avoided sharing CSLI would have been to disconnect his cell phone from the network entirely.[170] That is not a realistic choice in this era, when carrying a cell phone "is indispensable to participation in modern society."[171] Because Carpenter did not voluntarily assume the risk of "turning over a comprehensive dossier of his physical movements," the Court found the third party doctrine no bar to Fourth Amendment protection.[172]

The Court also rejected an argument that was a variation of the third party doctrine based on compulsory process. Under that theory, when the government compels the disclosure of businesses' records, the government may use a subpoena subject only to a relevance standard of review. Justice Alito, in dissent, strongly advocated that approach.[173] He argued that compulsory process of third party records does not require the same standard of review as searches of homes and the like based on the precedents.[174] But those cases did not involve materials or

---

168 *See* Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121, 147–58 (tracing and criticizing the history of the third party doctrine and describing the limited reach of *Smith* and *Miller*).

169 *See, e.g.*, *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 612–14 (5th Cir. 2013).

170 *Carpenter*, 138 S. Ct. at 2219–20.

171 *Id.* at 2220.

172 *Id.* Yet another formulation of the third party doctrine considers the exposure of information out in the open to waive Fourth Amendment protection because of the assumption of risk that a police officer may be among the watching public. *See* Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y (SPECIAL ISSUE) 1, 6–7, 7 n.30 (2012). The Court noted that it had accepted, in *Jones*, the possibility of a reasonable expectation of privacy in public movements. *Carpenter*, 138 S. Ct. at 2220; *see also supra* text accompanying note 93.

173 *Carpenter*, 138 S. Ct. at 2254 (Alito, J., dissenting); *see also id.* at 2255 (opining that the precedents establish use of a subpoena as a "constructive search" subject to less demanding review than a warrant). The government made the same argument in *Warshak*. *See* United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010); *see also* Bellia & Freiwald, *supra* note 168, at 131–32.

174 *Carpenter*, 138 S. Ct. at 2254; *see also* Bellia & Freiwald, *supra* note 168, at 171–72 (arguing for a rule that "the target [of a search] must be entitled to raise the claim that warrantless compelled disclosure of her emails and related attributes would violate her Fourth Amendment rights" because the third party cannot raise that claim on behalf of the target).

information in which the targets held a reasonable expectation of privacy.[175]

The majority pointed out that Justice Alito and the government had improperly conflated a two-step process: first, the determination of whether there is a reasonable expectation of privacy in the records at issue, and second, the selection of the appropriate standard.[176] The majority recognized that the target will have no reasonable expectation of privacy in the vast majority of records cases, particularly when the government subpoenas a corporation's own records.[177] But when the target's reasonable expectation of privacy in the records converts the records into the modern-day equivalent of an individual's own papers or effects, then the warrant requirement should apply, whether those records are stored with the target or a third party.[178]

The majority correctly noted that the *Miller* opinion had followed the same sequence.[179] It had first determined that Miller lacked a reasonable expectation of privacy in his records[180] and then concluded that no warrant was needed.[181] The logic did not go the other way; it was not that the records were records, per se, that obviated a reasonable expectation of privacy and the need for a warrant.[182] Accepting the government's argument would effectively permit it to dictate a lower standard of review just by choosing the lesser process of compelled disclosure. That could not be right.[183]

The Court's determination that the judiciary, and not the executive branch, must determine the extent of Fourth Amendment protection for CSLI seems obvious once articulated. Because of the odd history of subpoena law, however, *Carpenter* marks the first time the Court has explicitly announced the possibility of reasonable expectations of privacy in records stored with a third party.[184] That raises the questions of

---

175 *See* Bellia & Freiwald, *supra* note 168, at 141–47 (tracing the history of the compelled disclosure precedents that involved requests for corporate documents); *see also id.* at 171–72.

176 *See Carpenter*, 138 S. Ct. at 2222; *see also* Bellia & Freiwald, *supra* note 168, at 143–46 (describing how a proper reading of the precedents, including *Miller*, requires a court to *separately* consider whether a reasonable expectation of privacy in materials sought by subpoena requires greater Fourth Amendment protection, even though a subpoena based on reasonableness is sufficient to bring the target themselves before a court).

177 *Carpenter*, 138 S. Ct. at 2222.

178 *Id.*

179 *See id.* at 2221–22.

180 United States v. Miller, 425 U.S. 435, 442 (1976).

181 *Id.* at 444.

182 *Carpenter*, 138 S. Ct. at 2215 n.2, 2221–22; *see also* Bellia & Freiwald, *supra* note 168, at 141–47 (discussing subpoena precedents); Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 823–24 (2005).

183 *See Carpenter*, 138 S. Ct. at 2222 (criticizing Justice Alito's approach for permitting "official curiosity" as a justification for government collection of any documents (quoting United States v. Morton Salt Co., 338 U.S. 632, 652 (1950))).

184 *See id.* at 2217.

what the repercussions will be for this significant retrenchment of the third party doctrine, and why it took so long for the Court to protect CSLI. We take up both questions in Part III.

III. WHAT HATH SCOTUS WROUGHT?

The Court cautioned that its decision "is a narrow one" and proceeded to list a number of matters left for another day — real-time CSLI, cell tower dumps, conventional surveillance techniques such as security cameras, business records incidentally revealing location information (for example, credit card transactions), and other collection techniques involving foreign affairs or national security.[185] Even so, the scope and rationale of the opinion send clear signals for certain other location monitoring techniques. More broadly, the multifactor *Katz* approach reaffirmed by the *Carpenter* majority provides a useful framework for courts to evaluate Fourth Amendment limits on the state's access to digital databases unrelated to physical location. Finally, the extraordinary length of time to settle the constitutionality of this vintage investigative technique has disturbing implications for law enforcement accountability under our democratic system.

A. Impact on Other Location Monitoring Techniques

1. Real-time CSLI. — This category affords the safest prediction. Real-time monitoring of cell phone location over time is presumptively a search and will require a warrant, for several reasons. First, the third party doctrine is not implicated here because the provider does not routinely generate or maintain business records containing precise location data like GPS. Second, the multifactor analysis of *Carpenter* would seem equally applicable to prospective location data. Such data is just as hidden, continuous, indiscriminate, intrusive, and inexpensive as historical CSLI. Third, as Chief Justice Roberts has told us, a monitored cell phone is tantamount to an ankle monitor, the quintessential tracking device.[186] In the words of one prominent journalist on the technology beat, cell phones are "the world's most effective tracking devices, even when they are turned off."[187] The procedures for obtaining a tracking-device warrant are well established under Rule 41.[188] Under that rule as amended in 2006, a magistrate judge must issue a warrant to install or use a tracking device upon a showing of probable cause.[189]

---

[185] *Id.* at 2220.

[186] *Id.* at 2218.

[187] JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE 141 (2014).

[188] *See* FED. R. CRIM. P. 41.

[189] *Id.* 41(d)(1). It is true that, as the drafters of the amended rule noted, the Supreme Court in *Karo* had left open the question of whether a tracking device warrant could be based on a lesser

What if the duration of the real-time surveillance is less than seven days? While *Carpenter* did not address that question,[190] the Court's earlier tracking device cases do provide an answer. As we have seen, *Knotts* and *Karo* drew the line between monitoring a public versus private space, without regard to the duration of the monitoring period.[191] Given that cell phones are routinely used inside the home (even in the shower),[192] as well as other places withdrawn from public view, it is difficult to imagine that *Karo* would allow warrantless monitoring for *any* length of time, day or night. Probably for this very reason, prudent prosecutors have avoided the risk of suppression in the past by seeking a tracking device warrant to authorize monitoring over any period of time, no matter how brief. The same practice is likely to be followed here, with probably the same result. Short-term monitoring of cell phones ought to generate no more difficulty for appellate courts than has been the case for other tracking devices.

2. Historical CSLI for Fewer than Seven Days. — There is room for doubt here under a multifactor analysis, because the level of intrusiveness is not the same as in *Carpenter*. But other Fourth Amendment rubrics — the *Karo* public versus private space analysis, or the property-based approach favored by Justice Gorsuch — might well result in a warrant requirement for even a moment's worth of location data. It is also noteworthy that the *Carpenter* majority did not appear eager to tie the warrant requirement to a particular time frame.[193] As in the case of real-time CSLI, a prudent prosecutor would be well advised to seek a warrant in such cases, avoiding the risk of a successful motion to suppress this key evidence.

---

showing than probable cause, and so the new rule was not intended to resolve that issue. *See* FED. R. CRIM. P. 41 advisory committee's note to 2006 amendment. However, *Carpenter* has now answered that question. If, as the Court held, a warrant based on probable cause is required for historical cell site data, what could possibly justify a lesser standard for prospective CSLI?

190 *See Carpenter*, 138 S. Ct. at 2217 n.3 ("[W]e 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."); *id.* at 2220 ("We do not express a view on . . . real-time CSLI . . . .").

191 United States v. Karo, 468 U.S. 705, 716 (1984); United States v. Knotts, 460 U.S. 276, 282 (1983); *see also* Kyllo v. United States, 533 U.S. 27, 37 (2001) ("In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes.").

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

193 At oral argument, Chief Justice Roberts and Justice Ginsburg both took strong exception to the ACLU's fallback position that Fourth Amendment protection would kick in only for at least "one week's worth of CSLI." *See* Transcript of Oral Argument at 7, 11, *Carpenter*, 138 S. Ct. 2206 (No. 16-402), https://www.supremecourt.gov/oral_arguments/argument_transcripts/2017/16-402_6khn.pdf [https://perma.cc/WDT6-PNRQ]; Reply Brief for Petitioner at 12, *Carpenter*, 138 S. Ct. 2206 (No. 16-402).

3. Cell Site Simulator. — This is also an easy case to predict. A cell site simulator (such as a Stingray or Triggerfish)[194] is a device employed by law enforcement to locate a target device within a defined area. Posing as a real cell tower, the device causes each cell phone within the area to transmit a registration signal revealing its number and location.[195] The case for Fourth Amendment protection of cell site simulator location data would seem even stronger than in *Carpenter*. The data gathered by the cell site simulator is generated by law enforcement, not the provider, and so the third party doctrine of *Miller* and *Smith* is not even arguable here. Another problem with the cell site simulator is the breadth of the area under search. Allowing a police van to troll the streets of a neighborhood or town in order to locate a particular phone raises the specter of an illegal general warrant.[196] Perhaps for these reasons it has been DOJ policy since 2016 to seek a Rule 41 warrant to authorize use of these devices.[197] Based on such legal and practical concerns, law enforcement use of cell site simulators will in all likelihood be subject to the Fourth Amendment.

4. Cell Tower Dumps. — One very valuable technique in solving crime is the "tower dump," in which law enforcement seeks an order compelling providers to release historical cell site data for a specific tower or towers providing service to a crime scene.[198] This is the scenario most likely to require resolution of the durational limit to *Carpenter*'s historical CSLI holding. In the past, law enforcement has obtained D orders for the short span of time — often less than an hour — during which the crime occurred. Unlike the lengthy surveillance period at issue in *Carpenter*, the CSLI obtained in a tower dump will likely reveal only a snapshot of a phone's location at a given time.[199] On the other hand, the data obtained will not be merely the location of a single phone, but snapshots of the many hundreds or even thousands of phones in contact with the tower in that window of time.[200] Once again, this raises general warrant concerns that were not present in *Carpenter*. While the legal question here is much closer than the case

---

194 Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 178–79 (2012).

195 *See id.* at 126 n.28, 178–79.

196 *Cf.* United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010) (noting that "tenants have a legitimate expectation of privacy in their apartments" (citing United States v. Washington, 573 F.3d 279, 284 (6th Cir. 2009))).

197 DEP'T OF JUSTICE, DEPARTMENT OF JUSTICE POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY 3, https://www.justice.gov/opa/file/767321/download [https://perma.cc/5JLW-X8HN].

198 *In re* Application for Cell Tower Records Under 18 U.S.C. § 2703(d), 90 F. Supp. 3d 673, 674–75 (S.D. Tex. 2015).

199 *See, e.g.*, *id.* at 674.

200 *See, e.g.*, *id.*

of real-time CSLI or cell site simulators, prosecutors who wish to avoid the risk of suppression would be best served by obtaining a warrant, at least in cases not involving exigent circumstances.

5. Credit Card Transactions. — It seems a safe bet that credit card records will not be swept up in *Carpenter*'s holding. A credit card transaction may well disclose the card user's location at a point in time (especially if the purchase is made at a brick-and-mortar store). But unlike a cell phone, a credit card does not function as a tracking device, leaving a continuous trail of data tracking the user's movements over time. Instead, the location data is incidental to a financial transaction, exactly the type of transaction that *Miller* found to be outside the scope of Fourth Amendment protection.[201]

B. Nonlocation Digital Databases and the Third Party Doctrine

The Court's pullback of the third party doctrine requires closer analysis when it comes to privately maintained databases of nonlocation information. With increased digitization and the expansion of cloud computing, such databases have grown in number, size, and sensitivity.[202] Commercial databases containing records of purchases and web browsing reveal tremendous information about our beliefs, habits, and preferences. We increasingly store detailed health information with providers, such as diet companies and fitness trackers.[203] Social networking companies know our friends, lovers, and political causes, not just because we discuss them online, but because we form the bonds there.[204]

As we have seen, *Carpenter* wipes out the argument that records, merely by their storage with a third party, are immune from Fourth Amendment protection by virtue of the third party doctrine. By the same token, the government's use of compelled disclosure to obtain records from a third party, or the target, does not foreclose a reasonable expectation of privacy inquiry concerning those records.[205] As Justice Alito explained in dissent, the majority's approach undermines settled subpoena practices of many investigative bodies.[206]

Under the approach announced in *Carpenter*, courts will need to consider whether the records sought are subject to a reasonable expectation of privacy. The multifactor test that *Carpenter* approved is one way to

---

[201] *See* United States v. Miller, 425 U.S. 435, 440 (1976) (holding that there was no Fourth Amendment protection for the defendant's business records with his bank).

[202] *See generally* Laura K. Donohue, *The Dawn of Social Intelligence (SOCINT)*, 63 DRAKE L. REV. 1061 (2015) (describing the rise of "[s]ocial intelligence (SOCINT), the collection of digital data about social relationships" that arises from "social sites, collaborative platforms, and interest-group formation," *id* at 1069).

[203] Richards, *supra* note 2, at 1464–65.

[204] Donohue, *supra* note 202, at 1069–72.

[205] *See Carpenter*, 138 S. Ct. at 2247 (Alito, J., dissenting).

[206] *Id.*

add substance to that inquiry. Another consideration that *Carpenter* addressed is how cheap and efficient it is to obtain tremendous amounts of personal information about the subject;[207] in other words, has the difficulty of obtaining information ceased to be a privacy protection? Courts may also look to other sources of law to help ground the inquiry. As we discussed in section I.B, considering the WCPSA and CALEA to show Congress's special concern for CSLI could have guided the Court in finding a reasonable expectation of privacy in the data. Courts could look to California, which, along with other states, has afforded warrant protection to a range of electronic information, including addressing data and data stored on electronic devices.[208] Whatever the method, courts may no longer merely avoid the question by hiding behind an overly broad interpretation of the third party rule.

C. Embarrassing the Future?

From a broader perspective, it is sobering to consider the length of time it took for the Court to reach a definitive answer on how the Constitution applies to the data continuously emitted by the signature device of our era — the cell phone. Consider the following time intervals preceding the *Carpenter* decision on June 22, 2018:

- 24 years after CALEA declared that subscriber location information was entitled to greater legal protection than phone numbers dialed;[209]
- 19 years after WCPSA required the customer's express prior consent before a provider could use or disclose a user's call location information;[210]
- 13 years after the first magistrate judge decisions declaring cell phones to be tracking devices and finding a reasonable expectation of privacy in CSLI;[211]
- 10 years after the first magistrate judge decisions finding historical CSLI to be protected by the Fourth Amendment.[212]

Nor were these time lags inconsequential. During the past quarter century, law enforcement was given free rein to engage in warrantless

---

[207] *See id.* at 2218 (majority opinion); *see also* Henderson, *supra* note 103, at 510–15 (discussing how surveillance methods may need more legal regulation as they become cheaper and therefore less restricted by cost).

[208] *See, e.g.*, CAL. PENAL CODE § 1546.1 (West 2017).

[209] *See* Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001–1010 (2012)).

[210] *See* Pub. L. No. 106-81, 113 Stat. 1286 (1999) (codified as amended in scattered sections of 47 U.S.C.).

[211] *See S. Smith 1*, *supra* note 33, at 765; *Orenstein 1*, *supra* note 55, at 323.

[212] *See, e.g.*, *Lenihan*, *supra* note 69, at 611–12.

surveillance of anyone with a cell phone, which meant nearly everyone in the United States. Operating outside the limits of the Fourth Amendment, they could obtain "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years."[213] The amount of user information collected by law enforcement is "astonishing," according to congressional testimony by a veteran industry lawyer in 2010.[214] The total number of CSLI orders is unknown, because court records are typically sealed, and law enforcement agencies are not required to tabulate them.[215] Even so, a ballpark estimate can be gleaned from the "transparency reports" of individual providers. The two largest carriers, AT&T and Verizon, reported a combined total of over 120,000 requests for CSLI each year in 2015 and 2016.[216] Significantly, the number of accounts searched is greater than the number of requests, because a single D order often compels information about several different phones — the officers in *Carpenter* obtained three D orders covering sixteen different phones.[217] Based on these data, it is reasonable to estimate at least 250,000 unlawful CSLI searches per year, totaling more than *four million* since the passage of the Patriot Act in 2001. This is a staggering volume of constitutional violations, now beyond any possible remedy.[218]

Given these numbers, there is unintended irony in Chief Justice Roberts's admonition that "the Court must tread carefully" when considering new technology with broad implications "to ensure that we do not 'embarrass the future.'"[219] It is one thing to tread carefully in tax cases, as Justice Frankfurter was discussing when he used the phrase quoted,[220] but quite another to refrain from correcting a widespread error that enabled constitutional violations on an epic scale.

---

213 *Carpenter*, 138 S. Ct. at 2220.

214 *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights & Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 31 (2010) (statement of Albert Gidari, Perkins Coie LLP) [hereinafter *May 2010 Location Hearing*].

215 *See* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 320–21 (2012) [hereinafter Smith, *Reforming ECPA's Secret Docket*]; Stephen Wm. Smith, *Are US Courts Going Dark?*, JUST SECURITY (May 6, 2016), https://www.justsecurity.org/30920/courts-going-dark/ [https://perma.cc/GN3K-5UAF].

216 *See* Amicus Brief of Electronic Frontier Foundation et al. in Support of Petitioner at 13–14, *Carpenter*, 138 S. Ct. 2206 (No. 16-402). Other carriers report a substantial number of requests for customer data, but do not specify how many of those are call location requests.

217 *See* United States v. Carpenter, 819 F.3d 880, 884 (6th Cir. 2016); *see also May 2010 Location Hearing*, *supra* note 214, at 31 (statement of Albert Gidari, Perkins Coie LLP) ("[A] single grand jury subpoena may list dozens of accounts for which subscriber information is sought.").

218 *See* Kevin S. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance*, 41 U.S.F. L. REV. 589, 589–90 (2007).

219 *Carpenter*, 138 S. Ct. at 2220 (quoting Nw. Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944)).

220 *Nw. Airlines*, 322 U.S. at 300.

In the same vein, but more profoundly misguided, is Justice Kennedy's repeated refrain that the Court "risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[221] This innocuous-sounding procrastination principle[222] is in reality a dangerous call to shirk the Court's responsibility of instructing lower courts on the law. For while the Supreme Court might choose to stay its hand on critical constitutional questions in order to avoid "risking error," lower courts do not have that luxury.

When federal agents come to court chambers with applications for surveillance orders, magistrate judges must grant or deny those applications consistent with their best understanding of the Fourth Amendment and applicable precedent. They do not have the option of avoiding a decision for fear of making a mistake, even when the current state of technology makes it difficult to know what the correct legal decision is.

One of the first cell site decisions written by a magistrate judge closed with just such a plea for guidance: "[T]his opinion . . . is written in the full expectation and hope that the government will seek appropriate review by higher courts so that authoritative guidance will be given the magistrate judges who are called upon to rule on these applications on a daily basis."[223]

It has taken thirteen years (and millions of illegal searches) to receive a final answer to that plea. To be sure, the Court itself is not entirely responsible for the delay. The appellate process normally grinds slowly, so even a normal case will have aged significantly by the time it reaches the Court. In *Carpenter*, for example, the relevant facts occurred in 2011, seven years before the Supreme Court announced its decision.[224] Similar seven-year gaps occurred between the Supreme Court decisions in *Jones*[225] and *Riley*[226] and the facts on which they were based. And in *City of Ontario v. Quon*,[227] a civil action brought by a public employee asserting Fourth Amendment rights in text messages on an employer-provided pager, the pager technology was nine years old by the time the

---

221 *Carpenter*, 138 S. Ct. at 2233 (Kennedy, J., dissenting) (quoting City of Ontario v. Quon, 560 U.S. 746, 759 (2010)).

222 As Mark Twain put it: "Never put off till to-morrow what you can do [the] day after to-morrow just as well." MARK TWAIN, *The Late Benjamin Franklin*, The Galaxy, July 1870, at 138, 138, *reprinted in* CONTRIBUTIONS TO THE GALAXY, 1861–1871, BY MARK TWAIN (SAMUEL LANGHORNE CLEMENS) 62, 62 (Bruce R. McElderry Jr. ed., 1961).

223 *S. Smith I*, *supra* note 33, at 765.

224 *Carpenter*, 138 S. Ct. at 2212.

225 United States v. Jones, 565 U.S. 400, 402 (2012).

226 *See* Riley v. California, 134 S. Ct. 2473 (2014); United States v. Wurie, 612 F. Supp. 2d 104, 106 (D. Mass. 2009), *rev'd and remanded,* 728 F.3d 1 (1st Cir. 2013), *aff'd sub nom. Riley*, 134 S. Ct. 2473.

227 560 U.S. 746 (2010).

Supreme Court issued its decision in 2010, practically an eternity in the digital age.[228]

Given the normal lifespan of a Supreme Court case, there is no sound reason why the Supreme Court should slow-walk its decisions on critical legal issues posed by advancing technology. On the contrary, the Court should be keen to provide timely guidance to lower courts wrestling with Fourth Amendment questions about new law enforcement techniques, deployed on a massive scale. Anything less runs the risk of abdicating the judiciary's institutional responsibility to check executive power, as envisioned by the Constitution.

As *Carpenter* also makes clear, courts should not resort to doctrinal shortcuts in an effort to avoid the normative Fourth Amendment analysis that *Katz* requires. By affirming a normative approach to Fourth Amendment analysis under a reasonable expectation of privacy test, the Court has indicated that these cases may no longer be resolved by mechanical resort to an overbroad third party doctrine or, as some courts have done, recourse to a simplistic content versus noncontent analysis.[229] As discussed, there are several tools available to conduct the normative analysis required by *Carpenter*, but there are no easy shortcuts.

In the case of cell site location surveillance, all branches of government fell short. Initially, Congress passed a comprehensive regulatory scheme, but it was exceptionally complex and constantly in need of updating as technology developed. Some updates were passed in the 1990s, but they were sometimes so Delphic in nature (for example, CALEA), that they created as much confusion as clarity. At other times they were clear enough (for example, WCPSA), but their impact was blunted by law enforcement and private industry. Bills designed to resolve the CSLI problem were proposed but not passed.[230] On the judiciary side, some magistrate judges acted as the canary in the coal mine, but their impact was diffused by sealing orders, judge shopping, and strategic nonappeals by the government.[231] That left the executive branch, via self-regulation, to operate in a Fourth Amendment–free zone for over two decades.

It may be time to rethink our current system of policing, which permits law enforcement to act first and receive constitutional constraints

---

[228] *See id.* at 750. By that time, of course, the alphanumeric pager's role in society had become clear — it had no meaningful role.

[229] *See* Freiwald, *supra* note 123, at 12–14 (describing third party doctrine and noncontent shortcuts); *see also* United States v. Carpenter, 819 F.3d 880, 886 (6th Cir. 2016) ("[A]lthough the content of personal communications is private, the information necessary to get those communications from point A to point B is not.").

[230] *See e.g.*, ECPA Modernization Act of 2017, S. 1657, 115th Cong.; GPS Act, H.R. 1062, 115th Cong. (2017); GPS Act, S. 237, 114th Cong. (2015); Electronic Communications Privacy Act of 2000, H.R. 5018, 106th Cong.

[231] *See* Smith, *Reforming ECPA's Secret Docket*, *supra* note 215, at 314, 328.

later. One fix would include requiring police agencies to adopt rules in advance, with democratic input and accountability, before any new law enforcement technique can be lawfully employed.[232] Another approach is the European model, under which law enforcement may not engage in a particular investigative method until it has been fully authorized by statute.[233] What seems difficult to deny is that the current approach is an embarrassment to the present, and its continuation will surely embarrass the future.

---

[232] Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 1827, 1827 (2015); Christopher Slobogin, *Policing as Administration*, 165 U. PA. L. REV. 91, 91 (2016).

[233] *See generally* Kiel Brennan-Marquez & Stephen E. Henderson, *Fourth Amendment Anxiety*, 55 AM. CRIM. L. REV. 1, 33 (2018) ("[W]hen privacy and liberty norms are in flux, as they currently are given recent and rapid technological change, police *should* seek the assistance of legislatures in governing investigatory methods, and they *must* seek the approval of courts." (footnote omitted)); Susan Freiwald & Sylvain Métille, *Reforming Surveillance Law: The Swiss Model*, 28 BERKELEY TECH. L.J. 1261 (2013) (discussing CrimPC, a Swiss surveillance law, in the context of European law).