FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

JUSTIN SANCHEZ, *Plaintiff-Appellant*, v. LOS ANGELES DEPARTMENT OF TRANSPORTATION; CITY OF LOS ANGELES, *Defendants-Appellees.*	No. 21-55285 D.C. No. 2:20-cv-05044-DMG-AFM OPINION

Appeal from the United States District Court
for the Central District of California
Dolly M. Gee, District Judge, Presiding

Argued and Submitted March 8, 2022
Pasadena, California

Filed May 23, 2022

Before: Kim McLane Wardlaw and Andrew D. Hurwitz, Circuit Judges, and Lee H. Rosenthal,* District Judge.

Opinion by Judge Hurwitz

---

* The Honorable Lee H. Rosenthal, Chief United States District Judge for the Southern District of Texas, sitting by designation.

SUMMARY[**]

Civil Rights

The panel affirmed the district court's order dismissing, for failure to state a claim, an action brought by an e-scooter user alleging that the City of Los Angeles' e-scooter permitting program, which requires e-scooter companies to disclose real-time location data for every device, violates the Fourth Amendment and California law.

As a condition of getting a permit, the Los Angeles Department of Transportation ("LADOT") required e-scooter operators to provide vehicle location data through an application programming interface called Mobility Data Specification ("MDS"). Used in conjunction with the operators' smartphone applications, MDS automatically compiles real-time data on each e-scooter's location by collecting the start and end points and times of each ride taken.

The complaint alleged that the MDS protocols provide the location of e-scooters with Orwellian precision. A City therefore allegedly could easily use MDS data in conjunction with other information to identify trips by individuals to sensitive locations. Because the location data could be preserved in accordance with LADOT data-retention policies, plaintiff alleged that the City could travel back in time to retrace a rider's whereabouts.

[**] This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

The panel first held that plaintiff's complaint alleged facts giving rise to Article III standing and therefore the panel rejected LADOT's assertion that the complaint was beyond the panel's constitutional purview because it was premised on a hypothetical invasion of privacy that might never occur. Drawing all reasonable inferences in favor of plaintiff as it was required to do at the Fed. R. Civ. P. 12(b)(6) stage, the proper reading of the complaint was that plaintiff alleged that the collection of the MDS location data itself—without more—violated his constitutional rights.

The panel concluded that the third-party doctrine, which provides that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties, foreclosed plaintiff's claim of a reasonable expectation of privacy over the MDS data.

Focusing first on "voluntary exposure," the panel had little difficulty finding that plaintiff knowingly and voluntarily disclosed location data to the e-scooter operators. Unlike a cell phone user, whose device provides location information by dint of its operation, without any affirmative act on the part of the user, plaintiff affirmatively chose to disclose location data to e-scooter operators each time he rented a device. Having voluntarily conveyed his location to the operator in the ordinary course of business, plaintiff could not assert a reasonable expectation of privacy.

The panel next determined that the nature of MDS location data indicated a diminished expectation of privacy. The data only discloses the location of an e-scooter owned by the operator and typically rerented to a new user after each individual trip. It was thus quite different than the information generated by a cell phone, which identifies the location of a particular user virtually continuously. The

panel declined the invitation to conclude that LADOT's collection of anonymous data about traffic movements was somehow rendered a search because it may be used in the future (in connection with other non-private material) to reveal an individual's previous locations. Because the third-party doctrine squarely applied to plaintiff's voluntary agreement to provide location data to the e-scooter operators, the collection of that data by LADOT was not a search and did not violate the Fourth Amendment or the California Constitution.

The panel affirmed the district court's dismissal of plaintiff's claim under the California Electronic Communications Privacy Act ("CalECPA") on the grounds that the statute did not provide plaintiff with authorization to bring an independent action to enforce its provisions.

Finally, the panel held that the district court did not err in dismissing the complaint without leave to amend. Because plaintiff had no reasonable expectation of privacy over the MDS location data, no additional facts could possibly have cured the deficiency with his constitutional claims. And, because the court rightly found that the CalECPA did not create a private right of action, dismissal of the statutory claim was also not error.

COUNSEL

Mohammad Tajsar (argued), ACLU Foundation of Southern California, Los Angeles, California; Jacob A. Snow, ACLU Foundation of Northern California, San Francisco, California; Jennifer Lynch and Hannah Zhao, Electronic Frontier Foundation, San Francisco, California; Douglas E. Mirell and Timothy J. Toohey, Greenberg Glusker Fields

Claman & Machtinger LLP, Los Angeles, California; for Plaintiff-Appellant.

Jonathan H. Eisenman (argued) and Jeffrey L. Goss, Deputy City Attorneys; Blithe S. Bock, Managing Assistant City Attorney; Scott Marcus, Chief Assistant City Attorney; Kathleen A. Kenealy, Chief Deputy City Attorney; Michael N. Feuer, City Attorney; Office of the City Attorney, Los Angeles, California; for Defendants-Appellees.

Kendra K. Albert and Mason A. Kortz, Cyberlaw Clinic, Harvard Law School, Cambridge, Massachusetts, for Amici Curiae Seven Data Privacy and Urban Planning Experts.

Brian E. Klein and Melissa A. Meister, Waymaker LLP, Los Angeles, California; Samir Jain and Gregory T. Nojeim, Center for Democracy & Technology, Washington, D.C.; Alan Buter, Megan Iorio, and Melodi Dincer, Electronic Privacy and Information Center; for Amici Curiae Center for Democracy & Technology, and Electronic Privacy Information Center.

Jordan R. Jaffe, Quinn Emanuel Urquhart & Sullivan LLP, San Francisco, California, for Amicus Curiae Kevin Webb.

Alana H. Rotter and Nadia A. Sarkis, Greines Martin Stein & Richland LLP, Los Angeles, California, for Amicus Curiae Open Mobility Foundation.

OPINION

HURWITZ, Circuit Judge:

Faced with a near-overnight invasion of motorized electric scooters ("e-scooters"), which cluttered sidewalks and interfered with street access, the City of Los Angeles adopted a permitting program and required e-scooter companies to disclose real-time location data for every device.[1] In this action, an e-scooter user claims that the location disclosure requirement violates the Fourth Amendment and California law. The district court dismissed the complaint for failure to state a claim. We affirm.

I.

Companies such as Bird, Lime, and Lyft began offering e-scooters for rent to the public in Los Angeles in 2017. The e-scooters are dockless, meaning they can be left anywhere after use and picked up by the next rider. They are also internet-connected, and are rented through the companies' smartphone applications, which charge riders based on the distance and duration of the trip taken.

In 2018, Los Angeles enacted a "Shared Mobility Device Pilot Program" to regulate the fledgling industry. L.A. Ord. 185,785 (Sept. 13, 2018). The program required companies to obtain a permit from the Los Angeles Department of Transportation ("LADOT") to offer e-scooters for rent and mandated that permittees "comply with all Department permit rules, regulations, indemnification, insurance and fee requirements." *Id*. As a condition of getting a permit,

[1] We use the term "e-scooter" to refer to the panoply of so-called micro-mobility devices offered for rent by permittees. *See* L.A. Ord. 185,785 (Sept. 13, 2018).

LADOT required e-scooter operators to provide vehicle location data through an application programming interface ("API")[2] called Mobility Data Specification ("MDS"). Used in conjunction with the operators' smartphone applications, MDS automatically compiles real-time data on each e-scooter's location by collecting the start and end points and times of each ride taken.[3] Because LADOT obtains data directly from the companies in real time, it can manage the public right-of-way actively and "communicate directly with product companies in real time using code."[4]

Plaintiff Justin Sanchez uses e-scooters to travel from his home to work, visit friends, frequent local businesses, and access places of leisure. His complaint asserts that the collection of MDS location data by LADOT violates the Fourth Amendment to the United States Constitution; Article I, Section 13 of the California Constitution; and the California Electronic Communications Privacy Act ("CalECPA"), Cal. Penal Code § 1546 *et seq.*

The complaint alleges that the MDS protocols provide the location of e-scooters with Orwellian precision, to within 1.11 centimeters of their exact location. It acknowledges that "MDS does not collect any information directly

[2] An API "acts as an intermediary between two other programs . . . to exchange information." Dave Johnson, *A guide to APIs, software that helps different apps work together,* Bus. Insider (May 13, 2021), https://www.businessinsider.com/what-is-an-api.

[3] LADOT also requires the submission of data on the specific route taken between those points within twenty-four hours of the trip.

[4] *See* "Mobility Data Specification: Information Briefing," L.A. Dep't of Transp. (Oct. 31, 2018), https://ladot.io/wp-content/uploads/2018/12/What-is-MDS-Cities.pdf.

identifying the rider of a particular vehicle." But, Sanchez alleges that government actors could subsequently "match users' trajectories in anonymized data from one dataset, with deanonymized data in another," and research indicates programmers "could identify 50% of people from only two randomly chosen data points in a dataset that contained only time and location data." The City therefore can "easily," he alleges, use MDS data in conjunction with other information to identify trips by individuals to sensitive locations. And, because the location data may be preserved in accordance with LADOT data-retention policies, Sanchez alleges that the City can travel back in time to retrace a rider's whereabouts.

The district court granted LADOT's motion to dismiss the complaint without leave to amend. *Sanchez v. L.A. Dep't of Transp.*, No. CV-20-5044-DMG, 2021 WL 1220690 (C.D. Cal. Feb. 23, 2021). It found that the LADOT program is not a search under the Fourth Amendment because Sanchez has no reasonable expectation of privacy over anonymous MDS location data. *Id.* at *4. It alternatively concluded that, even if the collection of MDS data were a search, it is a reasonable administrative one and thus constitutional. *Id*. at *5–6. Because "the right to be free from unreasonable searches under Art. I § 13 of the California Constitution parallels the Fourth Amendment inquiry," *Sanchez v. Cnty. of San Diego*, 464 F.3d 916, 928–29 (9th Cir. 2006), the district court also dismissed Sanchez's state constitutional claim. *Id.* at *2. And it rejected the CalECPA claim, finding that the statute did not provide Sanchez a private right of action. *Id*. at *6.

Finding any amendment futile, the district court dismissed the complaint with prejudice. *Id.* This timely appeal followed.

II.

LADOT first argues that we must dismiss Sanchez's claims because he lacks Article III standing. *See In re Apple iPhone Antitrust Litig.*, 846 F.3d 313, 319 (9th Cir. 2017) (noting that Article III standing is a jurisdictional requirement that may be raised "at any time"). LADOT argues that this complaint is beyond our constitutional purview because it is premised on a hypothetical future invasion of privacy that may never occur.

To establish Article III standing, "a plaintiff must show (i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief." *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2203 (2021). We must "assess whether the alleged injury to the plaintiff has a 'close relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit in American courts." *Id.* at 2204 (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341 (2016)). "[T]hose traditional harms may also include harms specified by the Constitution itself." *Id.* (citing *Spokeo*, 578 U.S. at 340; *Pleasant Grove City v. Summum*, 555 U.S. 460 (2009) (abridgment of free speech); *Church of Lukumi Babalu Aye, Inc. v. Hialeah*, 508 U.S. 520 (1993) (infringement of free exercise)). And, although "traditional tangible harms, such as physical harms and monetary harms," most "readily qualify as concrete injuries," "intangible harms can also be concrete." *Id.*

Applying this settled doctrine, we conclude that Sanchez's complaint alleges facts giving rise to Article III standing. The harm alleged is one "specified by the Constitution itself," *id.*—the violation of the Fourth Amendment guarantee against unreasonable searches and

seizures. Moreover, the alleged injury has a close nexus to those traditionally providing a "basis for a lawsuit in English or American courts," *Spokeo*, 578 U.S. at 341, such as "disclosure of private information" and "intrusion upon seclusion." *TransUnion*, 141 S. Ct. at 2204.

Drawing all "reasonable inferences" in favor of Sanchez as we are required to do at the Rule 12(b)(6) stage, the proper reading of this complaint is not, as LADOT asserts, that someone someday "*might* perform an analysis of device location data, which *might* disclose Sanchez's scooter-borne peregrinations." Rather, Sanchez alleges that the collection of the MDS location data itself—without more—violates his constitutional rights today.

It makes no difference for the purposes of determining Article III standing whether Sanchez's complaint states a valid Fourth Amendment claim. That "confuses the jurisdictional inquiry . . . with the merits inquiry." *Ecological Rights Found. v. Pac. Lumber Co.*, 230 F.3d 1141, 1151 (9th Cir. 2000). We therefore turn to the merits.

III.

The Fourth Amendment prohibits "unreasonable searches and seizures." U.S. Const. amend. IV. The initial issue for decision is whether LADOT's collection of MDS location data is a search for Fourth Amendment purposes.[5] Only if collection of the data is a search do we need to address the separate question of whether that search is

[5] Sanchez does not raise any independent arguments about the illegality of the data collection under the California Constitution, acknowledging that that inquiry is "functionally coterminous" with Fourth Amendment review.

unreasonable. *See Florida v. Jimeno*, 500 U.S. 248, 250 (1991).

For much of our Nation's history, the definition of a search under the Fourth Amendment was "tied to common-law trespass," focusing on whether government actors had obtained "information by physically intruding on a constitutionally protected area." *United States v. Jones*, 565 U.S. 400, 405, 406 n.3 (2012). In *Olmstead v. United States*, for example, the Supreme Court found that wiretaps attached to telephone wires on public streets did not constitute a search because "[t]here was no entry of the houses or offices of the defendants." 277 U.S. 438, 464 (1928).

The Court significantly expanded the doctrinal scope of the analysis in *Katz v. United States*, finding that the attachment of an eavesdropping device to a public telephone booth was a search, memorably stating that "the Fourth Amendment protects people, not places." 389 U.S. 347, 351 (1967). Its subsequent decisions have framed the inquiry as whether the challenged government action violates a person's "reasonable expectation of privacy," citing Justice Harlan's seminal *Katz* concurrence. *Id*. at 360. Thus, when an individual "seeks to preserve something as private," and that expectation of privacy is "one that society is prepared to recognize as reasonable," government intrusion into that private sphere generally qualifies as a search requiring a warrant supported by probable cause. *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (cleaned up).

A.

Thus, the essential inquiry is whether collection of MDS location data "violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001). Answering that question

implicates "the intersection of two lines of cases, both of which inform [an] understanding of the privacy interests at stake." *Carpenter v. United States*, 138 S. Ct. 2206, 2214–15 (2018). The first line "addresses a person's expectations of privacy in his physical location and movements." *Id*. at 2215. The second concerns the "line between what a person keeps to himself and what he shares with others," implicating the so-called third-party doctrine. *Id.* at 2216. That doctrine teaches that a person "has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743–44.

1.

In the first line of cases, Supreme Court decisions after *Katz* have considered a person's reasonable expectation of privacy with respect to his physical location and movements. In *United States v. Knotts*, the Court addressed police officers' use of a GPS "beeper" planted in a container to track an automobile to a remote cabin. *See* 460 U.S. 276, 281–82 (1983). Reasoning that a "person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another," the Court held that Knotts had no privacy interest in the information obtained through use of the beeper. *Id*. *Knotts* stressed the "limited use which the government made of the signals from [a] particular beeper" during a discrete "automotive journey." *Id.* at 284–85. But, the Court left for another day whether "different constitutional principles may be applicable" if "twenty-four-hour surveillance of any citizen of this country" were involved. *Id*. at 283–84.

Subsequently, the Court considered installation of a GPS tracking device on the defendant's vehicle and continuous remote monitoring of its movement for 28 days. *See Jones*, 565 U.S. at 402–03. Although the Court's opinion

ultimately turned on the physical trespass of the vehicle when the device was planted, *see id*. at 404–05, five Justices suggested in concurrences that reasonable privacy concerns would also be raised by "surreptitiously activating a stolen vehicle detection system" in Jones's car to track him or conducting GPS tracking of his cell phone, *id*. at 426 (Alito, J., joined by Ginsburg, Breyer, and Kagan, JJ., concurring in the judgment); *see also id*. at 415 (Sotomayor, J., concurring). They suggested that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Id*. at 430 (Alito, J., concurring); *see also id*. ("[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."); *id.* at 415 ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.") (Sotomayor, J., concurring).

Most recently, in *Carpenter*, the Court held that government collection of historical cell site location information ("CSLI") violated a reasonable expectation of privacy. Because "[m]apping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts," 138 S. Ct. at 2217, the Court concluded that "historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle . . . in *Jones*," *id*. at 2218. Acting as "almost a 'feature of human anatomy,'" the Court noted, a cell phone "faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Id*. (quoting *Riley v. California*, 573 U.S. 373, 385 (2014)).

"Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user." *Id*.

Carpenter also stressed the "retrospective quality of the data." *Id*. "In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection." *Id*. But, with historical CSLI, the government can "travel back in time to retrace a person's whereabouts, subject only to the retention policies of the wireless carriers," which kept those records for "up to five years." *Id*. "Unlike with the GPS device in *Jones*, police need not even know in advance whether they want to follow a particular individual, or when"—resulting in a "tireless and absolute surveillance" for anyone with a cell phone. *Id*. Accordingly, when the government acquired Carpenter's CSLI from wireless carriers, it violated his "reasonable expectation of privacy in the whole of his physical movements." *Id*. at 2219.

The Court repeatedly stated that the unique nature of cell phones raises Fourth Amendment concerns. *See id.* at 2218 ("While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time."); *see also Riley*, 573 U.S. at 395 (observing "nearly three-quarters" of cell phone users spend "most of the time" living "within five feet" of their phone). But it carefully underscored that the decision was "a narrow one," noting, "[w]e do not express a view on matters not before us: real-time CSLI or 'tower dumps.'" *Carpenter*, 138 S. Ct. at 2220. And, critically, the decision concluded: "We do not disturb the application of *Smith* and *Miller*." *Id*. It is this second line of cases—concerning a person's expectation of privacy with respect to information he voluntarily turns over to others—to which we next turn.

2.

The third-party doctrine teaches that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743–44; *see also United States v. Mohamud*, 843 F.3d 420, 442 (9th Cir. 2016) (noting that the "third-party doctrine" instructs "that a person's privacy interest is diminished where he or she reveals information to a third party, even in confidence"). This is true "even if the information is revealed on the assumption that it will be used only for a limited purpose." *United States v. Miller*, 425 U.S. 435, 443 (1976). "As a result, the Government is typically free to obtain such information from the recipient without triggering Fourth Amendment protections." *Carpenter*, 138 S. Ct. at 2216.

In *Miller*, investigating tax evasion, the government subpoenaed the defendant's banks, seeking cancelled checks, deposit slips, and monthly statements. *See* 425 U.S. at 438–39. The Court rejected Miller's Fourth Amendment challenge because he could "assert neither ownership nor possession" of these "business records of the banks." *Id*. at 440. Moreover, the Court found that the nature of the records confirmed Miller's limited expectation of privacy with respect to them. *See id*. at 442. The checks were "not confidential communications but negotiable instruments to be used in commercial transactions"; and the bank statements were "exposed to [bank] employees in the ordinary course of business." *Id*. Having "take[n] the risk, in revealing his affairs to another, that the information [would] be conveyed by that person to the Government," Miller's purported expectations of privacy were unavailing. *Id*. at 443.

Smith applied these principles to information conveyed to a telephone company. *See* 442 U.S. at 737–46. The Court held that the government's use of a "pen register"—which records the phone number dialed on a landline—was not a "search." *Id*. at 745–46. In so ruling, the Court noted its "doubt that people in general entertain any actual expectation of privacy in the numbers they dial." *Id*. at 742. Telephone users know, the Court reasoned, that the numbers are used "for a variety of legitimate business purposes" by the telephone company, including routing calls. *Id*. at 743. Thus, when Smith placed a call, he "voluntarily conveyed" the dialed numbers to the phone company by "expos[ing] that information to its equipment in the ordinary course of business." *Id*. at 744. He also "assumed the risk" that the company's records "would be divulged to police." *Id*. at 745. Thus, any subjective expectation Smith had that the numbers he dialed would be kept private "is not one that society is prepared to recognize as reasonable." *Id*. at 743 (cleaned up).

We have applied the "voluntary exposure" concept underpinning the third-party doctrine to find that a person has no reasonable expectation of privacy in the fact that he has booked a hotel room. *See United States v. Cormier*, 220 F.3d 1103, 1108 (9th Cir. 2000). So too, we have found that a person has no reasonable expectation of privacy in who comes and goes from the hotel room. *See Patel v. City of Montclair*, 798 F.3d 895, 900 (9th Cir. 2015); *see also United States v. Rosenow*, No. 20-50052, 2022 WL 1233236, at *13 (9th Cir. Apr. 27, 2022) (observing that a person has no expectation of privacy in information knowingly "provided to and used by internet service providers for the specific purpose of directing the routing of information"). The familiar proposition that an individual has no expectation of privacy over items left in "plain view"

of others derives from the same general principle. *See, e.g.*, *Horton v. California*, 496 U.S. 128, 133–34 (1990) ("If an article is already in plain view, neither its observation nor its seizure would involve any invasion of privacy."). The third-party doctrine has also been cited to explain why "neither the taxicab drivers nor passengers have a reasonable expectation of privacy in the pick-up and drop-off data collected by the GPS tracking aspect" of taxicab meters. *Azam v. D.C. Taxicab Comm'n*, 46 F. Supp. 3d 38, 50 (D.D.C. 2014).[6]

Nevertheless, as we recently observed, "commentators and two Supreme Court Justices have questioned the continuing viability of the third-party doctrine under current societal realities." *United States v. Moalin*, 973 F.3d 977, 992 (9th Cir. 2020).[7] Justice Sotomayor, for instance, has noted that the assumption-of-risk rationale underlying the doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring). And, in *Carpenter*, Justice Gorsuch remarked:

> Even our most private documents—those that, in other eras, we would have locked

[6] *See also* Orin S. Kerr, *Implementing Carpenter* (Dec. 14, 2018), THE DIGITAL FOURTH AMENDMENT (Oxford University Press), Forthcoming, USC Law Legal Studies Paper No. 18–29, https://ssrn.com/abstract=3301257 (suggesting that the "basic kind of record [at issue]—where a person was picked up, what path a person took, and where they were dropped off—is not new"); Orin Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009).

[7] *See, e.g.*, *Evan Frohman, 23PolicemenAndMe: Analyzing the Constitutional Implications of Police Use of Commercial DNA Databases*, 22 U. PA. J. CONST. L. 1495 (2020).

> safely in a desk drawer or destroyed—now reside on third party servers. *Smith* . . . teach[es] that the police can review all of this material, on the theory that no one reasonably expects any of it will be kept private. But no one believes that, if they ever did.

138 S. Ct. at 2262 (Gorsuch, J., dissenting).

And, of course, *Carpenter* itself rejected application of the third-party doctrine to government collection of historical CSLI. *See id*. at 2220. In so doing, the Court observed that it has "shown special solicitude for location information in the third-party context," citing the concurrences in *Jones*, *id*. at 2219–20, and concluded that the "detailed chronicle of a person's physical presence" presented by historical CSLI "implicates privacy concerns far beyond those considered in *Smith* and *Miller*," *id*. at 2220.

But, notably, *Carpenter* did not overrule *Smith* and *Miller*, despite Justice Gorsuch's invitation to do so. *See id.* at 2262 (dissenting opinion). Rather, it simply found the third-party doctrine inapplicable in the case before it, while expressly declining to "disturb the application of *Smith* and *Miller*" in other contexts. *Id.* at 2220. Specifically, the Court found that collection of historical CSLI fell outside the doctrine by focusing on its two underlying rationales—first, whether the nature of the material revealed to third-parties indicates a "reduced expectation of privacy," and, second, whether there was "voluntary exposure" of the information to others. *Id*. at 2219–20.

Addressing the first rationale, the Court noted that although one normally does not have an expectation of privacy in his movement on public streets, the "pervasive"

tracking of movements revealed by historical CSLI was different because it provided "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Id*. at 2220. The Court rejected the government's reliance on *Knotts* as failing "to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years." *Id*. at 2219. And it noted that "[t]here is a world of difference between the limited types of personal information addressed in *Smith* and *Miller*" and the "exhaustive chronicle of location information casually collected by wireless carriers today." *Id*. Thus, the reduced expectation of privacy normally occurring when one reveals his location by traveling on public streets was much diminished. *Id*.

Addressing the second rationale—"voluntary exposure"—the Court highlighted that CSLI is "not truly 'shared' as one normally understands the term." *Id*. at 2220. Rather, it recognized that CSLI is generated as a background function to cell phone use, simply by powering up the device. *See id*. Because carrying a cell phone "is indispensable to participation in a modern society," *Carpenter* concluded that "in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements." *Id.* (quoting *Smith*, 442 U.S. at 745).

B.

Relying heavily on the Court's statement in *Carpenter* that it has "shown special solicitude for location information in the third-party context," *id*. at 2219, Sanchez argues that we must treat the collection of MDS data as a search under the Fourth Amendment. But, because *Carpenter* expressly

stated that it was not disturbing the application of the third-party doctrine in contexts other than the collection of historical CSLI, that case only begins, rather than ends, our inquiry. Rather, as the Court did in *Carpenter*, we focus on whether application of the doctrine to this case would be consistent with its underlying rationales. *See Rosenow*, 2022 WL 1233236 at *12–13 (finding "*Carpenter* is distinguishable" and applying third-party doctrine). We conclude that the doctrine does apply here, foreclosing Sanchez's claim of a reasonable expectation of privacy over the MDS data.

Focusing first on "voluntary exposure," we have little difficulty finding that Sanchez knowingly and voluntarily disclosed location data to the e-scooter operators. Unlike a cell phone user, whose device provides location information "by dint of its operation, without any affirmative act on the part of the user," *Carpenter*, 138 S. Ct. at 2220, Sanchez affirmatively chose to disclose location data to e-scooter operators each time he rented a device. Indeed, his complaint concedes that, in order to charge him, an e-scooter operator necessarily must "track rides" by obtaining location data on the route taken. And, before renting an e-scooter, Sanchez must agree to the operator's privacy policies. Lyft's privacy policies, for instance, a copy of which Sanchez attached to his complaint, expressly state that "location data" will be collected, stored by the rental company, and shared with government authorities to "comply with any applicable . . . local law or regulation."

When Sanchez rents an e-scooter, he plainly understands that the e-scooter company must collect location data for the scooter through its smartphone applications. Thus, the voluntary exposure rationale fits far better here than in *Carpenter*. Having "voluntarily conveyed" his location to

the operator "in the ordinary course of business," Sanchez cannot assert a reasonable expectation of privacy. *Smith*, 442 U.S. at 744. Rather, because MDS data is knowingly disclosed as a central feature of his transaction with a third party—much like the route of a taxi ride is disclosed to a cab driver, *see Azam*, 46 F. Supp. 3d at 50—the situation fits comfortably within the ambit of *Smith* and *Miller*.

Second, the nature of MDS location data indicates a diminished expectation of privacy. The data only discloses the location of an e-scooter owned by the operator and typically rerented to a new user after each individual trip. It is thus quite different than the information generated by a cell phone, which identifies the location of a particular user virtually continuously.[8] Sanchez alleges that, armed with MDS data, government actors could later "easily" associate a given ride with an individual rider, using non-MDS information. But his complaint admits that the MDS data cannot be linked to a particular individual without more. We decline the invitation to conclude that LADOT's collection of anonymous data about traffic movements is somehow rendered a search because it may be used in the future (in connection with other non-private material) to reveal an individual's previous locations. Even accepting Sanchez's contention that anonymous MDS data can be used in the future to draw inferences about who was using a scooter at a particular time, "an inference is not a search." *Kyllo*, 533 U.S. at 37 n.4.

[8] It also makes the data unlike the telephony metadata collected by the NSA which we considered in *Moalin*, which included "comprehensive communications routing information" that "provides information about where a phone connected to the network, revealing data that can locate the parties" subject to the metadata capture. 973 F.3d at 991.

So too, in contrast to the CSLI at issue in *Carpenter* and the beeper tracking in *Jones*, the MDS data does not "pervasive[ly] track" users over an extended period, *see* 138 S. Ct. at 2220, instead capturing only the locations of e-scooters during discrete trips. Those e-scooters are continuously collected, recharged, and rerented. Even a regular rider could find herself using one e-scooter for her ride to work on Friday, picking up a different one to meet friends Saturday, and making her way home Sunday on yet another.

The location data is thus far afield from the dragnet, continuous monitoring of an identified individual's movements at issue in *Carpenter* and *Jones*.[9] For example, in *Carpenter*, authorities specifically requested cell records to trace the whereabouts of Timothy Carpenter over the course of 127 days. 138 S. Ct. at 2212. Here, the collection of MDS data is more like the remote monitoring of a discrete "automotive journey" in *Knotts*, 460 U.S. at 285, as MDS only collects route data and real-time location of an e-scooter for a single ride.

And, perhaps most obviously, e-scooters, unlike cell phones, are simply not "indispensable to participation in

[9] It also makes the MDS data collection far afield from the continuous monitoring central to the decisions in two recent cases upon which Sanchez extensively relies. *Leaders of a Beautiful Struggle v. Baltimore Police Department* involved the use of wide-angle cameras throughout the City of Baltimore, which "continuously records public movements." 2 F.4th 330, 347 (4th Cir. 2021) (en banc). And, in *Commonwealth v. McCarthy*, the Massachusetts Supreme Judicial Court emphasized that it was only with "enough cameras in enough locations"—allowing for continuous monitoring—that a program of automated readers capturing license plates could be said to "invade a reasonable expectation of privacy" and "constitute a search." 142 N.E.3d 1090, 1104 (Mass. 2020).

modern society." *Carpenter*, 138 S. Ct. at 2220. They are but one of many different means available for short-distance travel in some urban environments. Cell phones function for users as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, [and] newspapers"—and "also happen to have the capacity to be used as a telephone." *Riley*, 573 U.S. at 393. And, given "their immense storage capacity," cell phones allow users to carry in their pocket "millions of pages" of material—as if they carried around "every piece of mail they have received" or "every picture they have taken." *Id*. at 393–94. Cell phones are a "pervasive and insistent part of daily life" such that users are within several feet of them most of the time, with some "12% admitting that they even use their phones in the shower." *Carpenter*, 138 S. Ct. at 2218 (quoting *Riley*, 573 U.S. at 385, 395). By contrast, immediately following a ride, as Sanchez acknowledges in his complaint, an e-scooter user unceremoniously "leaves the scooter on the street."

We therefore conclude that the considerations animating the Court's "narrow" decision in *Carpenter* declining to apply the third-party doctrine are not present here. *See* 138 S. Ct. at 2220. Because the third-party doctrine squarely applies to Sanchez's voluntary agreement to provide location data to the e-scooter operators, the collection of that data by LADOT is not a search, and does not violate the Fourth Amendment or the California Constitution.[10]

[10] Because we find that collection of the MDS location data was not a search, we do not separately address the district court's determination that it was a reasonable one "in the context of safety and administrative regulations." *Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottwatomie Cnty. v. Earls*, 536 U.S. 822, 829 (2002).

IV.

We next review the dismissal of the CalECPA claim. That statute limits how state entities may access "electronic device information." Cal. Penal Code § 1546.1(a); *see id.* § 1546(g) (defining "electronic device information" as "any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device"). Except after adherence with certain procedures, *see* § 1546.1(b)–(k), it prevents state actors from: (1) compelling the production of electronic communication information from a service provider, *id.* § 1546.1(a)(1); (2) compelling the production of electronic device information from anyone other than the authorized possessor, *id.* § 1546.1(a)(2); and (3) accessing electronic device information by means of physical interaction or electronic communication with the device, *id.* § 1546.1(a)(3).[11]

But not anyone may sue for enforcement. The statute permits: (a) a person "in a trial, hearing, or proceeding" to "move to suppress" information obtained in violation of its provisions, *id.* § 1546.4(a); (b) the California Attorney General to "commence a civil action to compel any government entity" to comply with the restrictions, *id.* § 1546.4(b); and (c) a person whose information "is targeted by a warrant, order, or other legal process" inconsistent with the restrictions to "petition *the issuing court* to void or modify the warrant, order, or process, or to order the

[11] *See also* Bill Analysis, Senate Committee on Public Safety, SB 178 (March 23, 2015) at 1 ("The purpose of this bill is to require a search warrant or wiretap order for access to all aspects of electronic communications . . . .").

destruction of any information obtained in violation" of the restrictions, *id*. § 1546.4(c) (emphasis added).

Sanchez's relies on § 1546.4(c), claiming that the phrase "issuing court" refers to "courts with the authority to issue legal process"—and that because the district court has such authority, he has a private right of action. But, the plain text of the statute indicates that the term "issuing court" is one that previously issued "a warrant, order, or other legal process" that "targeted" an individual's information which the individual seeks to "void or modify." *Id*. § 1546.4(c). Because no court previously issued such an order here, the statute does not authorize Sanchez to bring an independent action to enforce its provisions. Indeed, in contrast, the statute expressly allows the California Attorney General to "commence a civil action" to enforce the statute. *Id*. at § 1546.4(b); *see Gikas v. Zolin*, 863 P.2d 745, 752 (Cal. 1993) ("The expression of some things in a statute necessarily means the exclusion of other things not expressed.").

V.

Finally, Sanchez challenges the dismissal of his complaint without leave to amend. A district court may dismiss a complaint without leave to amend if "the allegation of other facts consistent with the challenged pleading could not possibly cure the deficiency." *Albrecht v. Lund*, 845 F.2d 193, 195 (9th Cir. 1988) (cleaned up); *see also Kroessler v. CVS Health Corp.*, 977 F.3d 803, 815 (9th Cir. 2020) (futility of amendment justifies denying leave).

Accepting "as true all well-pleaded allegations of material fact," and construing them "in the light most favorable to the non-moving party," we find the district court did not err in dismissing the complaint without leave to

amend. *See Daniels-Hall v. Nat'l Educ. Ass'n*, 629 F.3d 992, 998 (9th Cir. 2010). Courts are to "consider the relevant factors and articulate why dismissal should be with prejudice instead of without prejudice," *Eminence Cap., LLC v. Aspeon, Inc.*, 316 F.3d 1048, 1052 (9th Cir. 2003), and the district court did so here. It correctly concluded that because Sanchez has no reasonable expectation of privacy over the MDS location data, no additional facts could possibly have cured the deficiency with his constitutional claims. And, because the court rightly found that the CalECPA does not create a private right of action, dismissal of the statutory claim was also not error.

AFFIRMED.

A guide to APIs, software that helps different apps work together

businessinsider.com/what-is-an-api

Dave Johnson May 13, 2021, 3:10 PM

- An application programming interface (API) is software that acts as an intermediary between two programs.
- APIs make it easy for apps to exchange information, data, pictures, and more.
- APIs also let apps have more features, since one program can just ask another program to perform a task.
- **Visit Insider's Tech Reference library for more stories.**

An API, or application programming interface, is software that acts as an intermediary between two other programs — or two components within a program — to exchange information. APIs are common types of computer code and form the foundation of our modern information architecture.

What to know about APIs

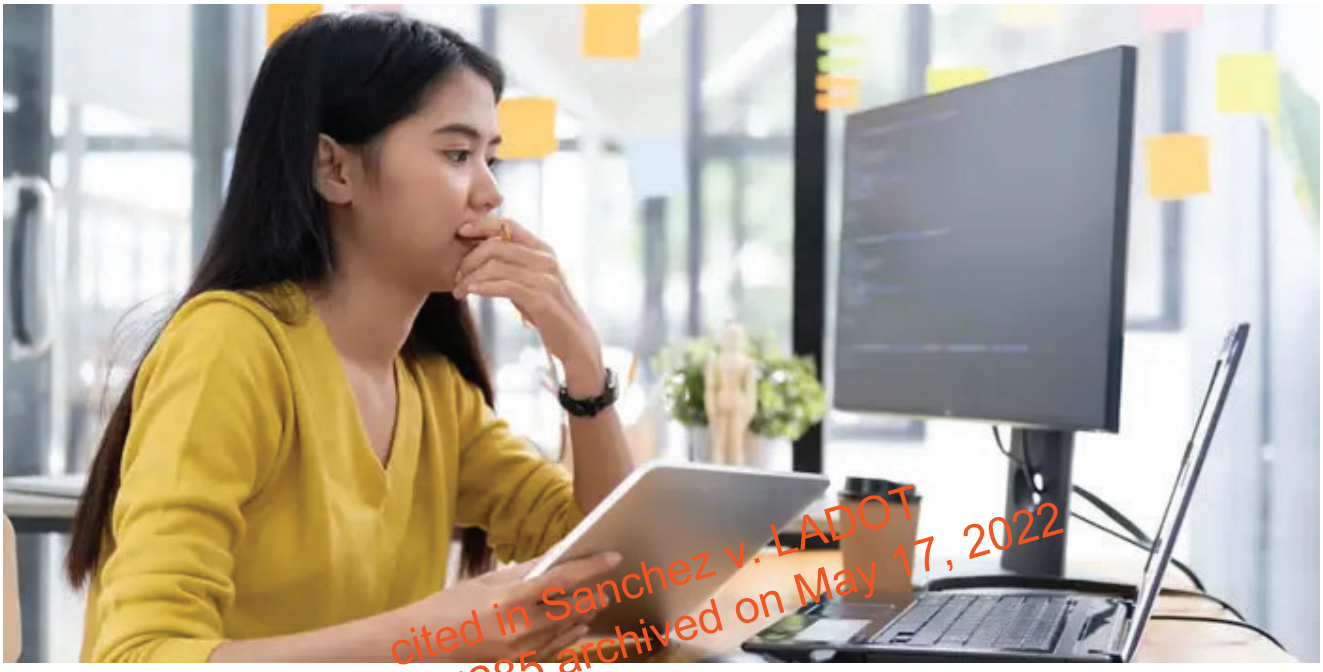
APIs consist of two components, and both are routinely referred to as "the API," which can be confusing:

- The technical specification that defines the details of what information is being exchanged between two programs, and the formal protocol for how that will be done.
- The software itself that serves as the intermediary between two programs.

APIs exist primarily to simplify the process of creating and maintaining software, in addition to extending and enhancing a program's capabilities.

Consider a program like a word processor, for example. In the earliest days of PCs, if a word processor like Microsoft Word needed to print a document, the developers had to include code that allowed the software to communicate with every printer a user might possibly own.

Windows solved that problem by offering a library of printer drivers built into the operating system; each driver only needed to be written once, and programs simply use the printer API to access any printer.



The introduction of APIs helped streamline software development.
Cavan Images/Getty Images

This is also an example of how APIs offer a layer of abstraction. The word processor doesn't need to know *how* to print to a particular printer; it simply sends a print request to the printer API, and the API handles the *how* of printing.

API specifications

Because APIs are the glue that binds different programs together, they need to follow standard protocols so that any developers who use the API understand how to integrate it into their code. There are a handful of common specifications in use today.

Each one of these is a different way to standardize the way data is exchanged between programs, which is important since an API should be able to work regardless of how the program is written or even what language is used to code it.

These are the most common protocols used to develop API specifications today:

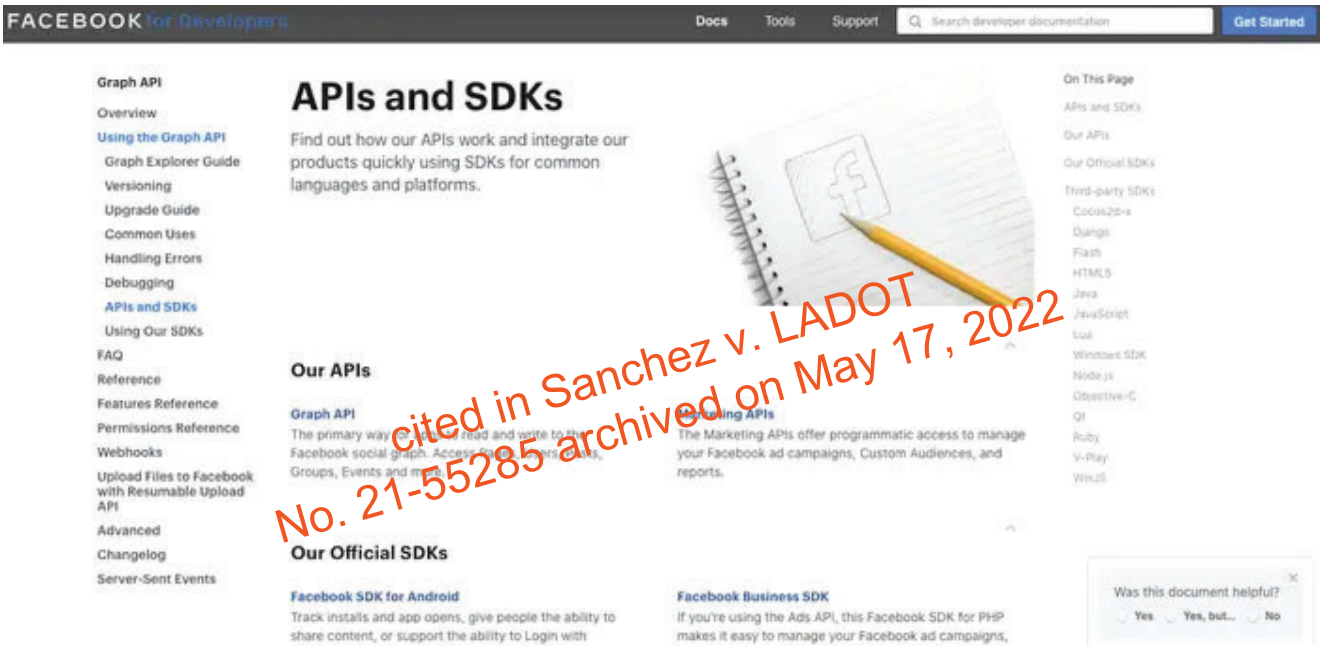
- Remote Procedure Call (RPC)
- Service Object Access Protocol (SOAP)

- Representational State Transfer (REST)
- GraphQL

APIs in the real world

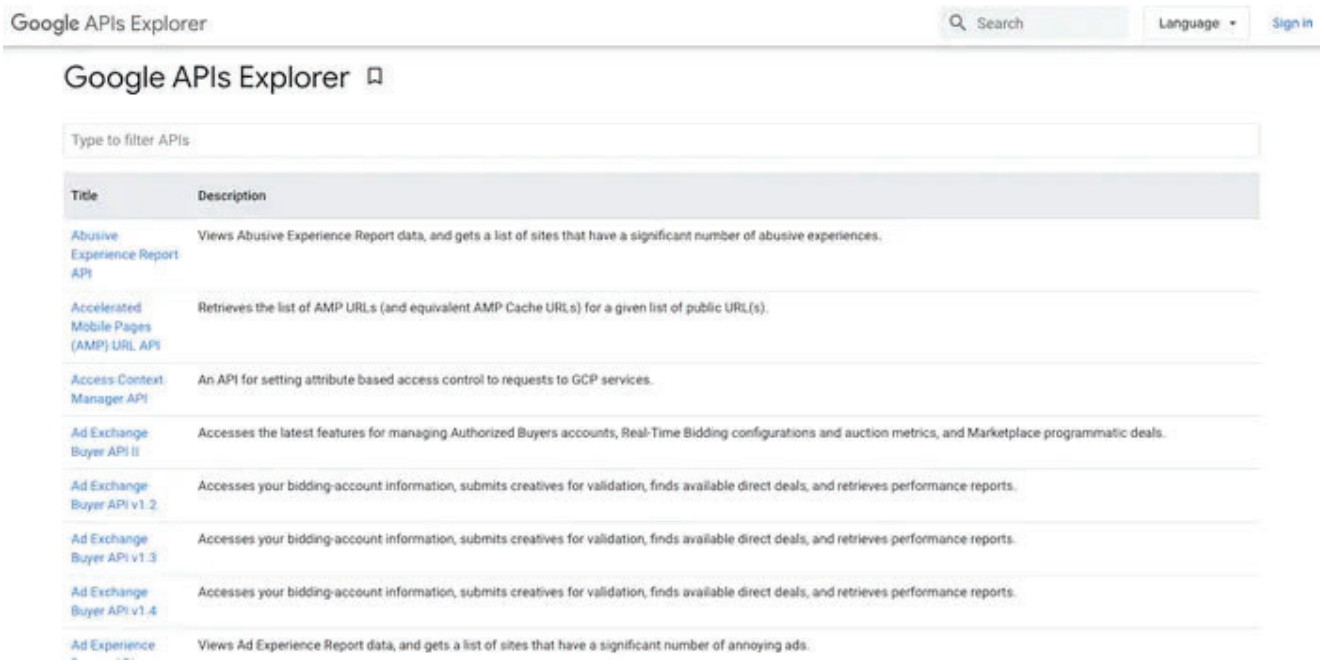
APIs are a core component of most modern software, so we are surrounded by them. Here are a few examples of APIs in common use:

> Facebook makes its social graph and marketing data available to third-party developers via its pair of Graph and Marketing APIs. The Graph API lets programs read and write to the Facebook social graph with access to pages, users, posts, and more. Likewise, the Marketing API gives access to Facebook ad campaigns, custom audiences, and reports.



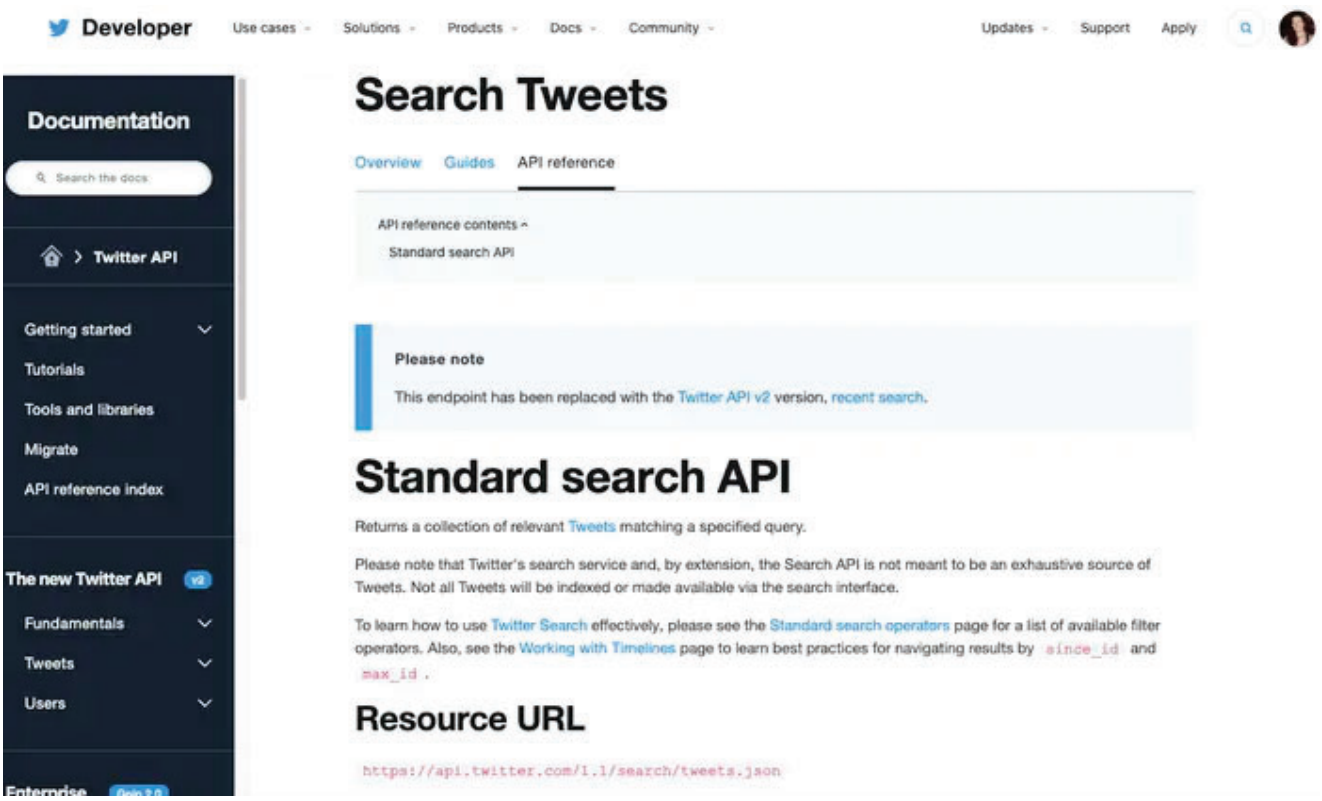
Developers can use Facebook's APIs for a variety of purposes.
Grace Eliza Goodwin/Insider

> Google maintains dozens of public APIs that allow developers of third-party applications and web services to access Google services. You can see a list of them at Google's API Explorer.



you can view Google's public APIs on its API Explorer site.
Grace Eliza Goodwin/Insider

Twitter offers a web-based Twitter API that lets developers create tweets, search for published tweets, and even favorite tweets programmatically.



Twitter's API helps developers automate processes like favoriting tweets.
Grace Eliza Goodwin/Insider

Dave Johnson

Dave Johnson is a technology journalist who writes about consumer tech and how the industry is transforming the speculative world of science fiction into modern-day real life. Dave grew up in New Jersey before entering the Air Force to operate satellites, teach space operations, and do space launch planning. He then spent eight years as a content lead on the Windows team at Microsoft. As a photographer, Dave has photographed wolves in their natural environment; he's also a scuba instructor and co-host of several podcasts. Dave is the author of more than two dozen books and has contributed to many sites and publications including CNET, Forbes, PC World, How To Geek, and Insider.

Mobility Data Specification

Information Briefing

October 31, 2018

Introduction

Similar to a common language, the Mobility Data Specification (MDS) gives cities an elegant and cost effective tool to actively manage private mobility providers and the public right-of-way. MDS allows cities to collect valuable insights through a shared data vocabulary and to communicate directly with product companies in real time using code. Today, it enables cities to manage dockless scooters, bikes, taxis, and buses. Tomorrow, that could be autonomous cars, drones, and whatever else the future may hold.

Standard Data Sharing

In Los Angeles, permitted shared use mobility providers (like scooters and bikes) must provide real-time information about how many of their vehicles are in use at any given time, where vehicles are at all times, and the physical condition that vehicles are in. Additional information includes:

- Parking Verification
- Operating Cost
- Customer Cost
- Vehicle Utilization
- Percent Battery Charge
- Start Trip Data
- End Trip Data

Applications

The MDS is based on a set of Application Programming Interfaces (API). APIs are the underpinning of the modern mobile internet. APIs help get data to and from your mobile device to the backend system of a mobile service you might be using.

In Los Angeles, mobility providers are required to share data with LADOT. The MDS defines the API that LADOT will use in order to pull this data from mobility service companies.

The MDS also defines a number of other APIs that mobility service companies will support so that, in the very near future, LADOT can actively manage

Mobility Data Specification

mobility services that are in the public right-of-way. For instance, if a vehicle is parked outside of a proper parking area, LADOT's Agency APIs will be able to communicate in real-time with the mobility service provider and their customer about the proper parking area and may prevent a user from ending their trip until the vehicle is parked in an appropriate designated area. This active management of shared vehicles, for instance, helps ensure safe passage for all who are using the public right-of-way.

First Principles

Open-Source: allows any city or company to run MDS and related products as a service within their city free from any royalties or license fees.

Competition: fosters a competitive market for companies to develop products as a service in cities by creating a single platform where everyone is invited to participate and build.

Data and Privacy: adheres to best practices for privacy standards, commits to data collection transparency, and--above all else--protects citizen privacy.

Harmony: encourages consistent regulation so that providers can offer low cost, homogeneous services across municipal borders.

Sustainability: prepares cities for regulating transportation services that are low-emission, resilient, and ultimately better for the environment

Contributors

MDS is an open source project that involves contributions from cities, agencies, and mobility service providers. Contributors include:

- *The City of Los Angeles*
- *The City of Santa Monica*
- *The City of Austin*
- *San Francisco Metropolitan Transit Authority (SFMTA)*
- *Seattle Department of Transportation*
- *Harvard Kennedy School*
- *Bird*
- *Spin*
- *Lime*

For more info:
github.com/CityOfLosAngeles/ /mobility-data-specification
urbanmobilityla.com
ladot.io

LADOT

Implementing *Carpenter*

Orin S. Kerr*

THE DIGITAL FOURTH AMENDMENT
(Oxford University Press, forthcoming)

Abstract

In its June 2018 decision in *Carpenter v. United States,* the Supreme Court held that cell phone users have Fourth Amendment rights in their historical cell-site location records. *Carpenter* takes the Fourth Amendment in a new direction, adding new protections for non-content third-party business records. *Carpenter* prompts fundamental questions of what the Fourth Amendment means in the digital age. The Court is embarking on a new path. But what the new Fourth Amendment will look like, and what its limits may be, remain unclear.

This article is a discussion draft of two chapters from a book project, *The Digital Fourth Amendment*, forthcoming from Oxford University Press. The book argues that computers and the Internet should trigger new Fourth Amendment rules for the digital age. The facts of the digital world are different from the physical world, and new rules are needed to restore the role of the Fourth Amendment. The Supreme Court has already begun creating a Digital Fourth Amendment in *Carpenter* and its 2014 decision in *Riley v. California*. This book develops the rationale for the new rules based on the theory of equilibrium-adjustment, and it offers a comprehensive picture of how the Fourth Amendment should apply to a wide range of doctrines.

The two chapters presented here offer a way to implement *Carpenter*. They develop and apply a test for *Carpenter* searches that is faithful to the decision, true to the theory of equilibrium-adjustment on which it rests, and yet also provides as much of the clarity that Fourth Amendment law demands as possible. Chapter 6, *The Carpenter Shift*, starts by explaining why *Carpenter* represents a departure from traditional Fourth Amendment principles based on a premature but explicit application of equilibrium-adjustment principles. It then argues that *Carpenter* should apply to Internet records when three requirements are met: The records exist because of the digital age, they are created without meaningful voluntary choice, and they tend to reveal the privacies of life. Chapter 7, *Implementing Carpenter*, explains that any records that satisfies these criteria should be protected. Courts should reject a mosaic theory that would limit *Carpenter* to long-term monitoring or case-by-case approaches that look to whether privacy invasions actually occurred. The Chapter ends by identifying specific examples of Internet records that should trigger *Carpenter* -- and examples that should not.

---

* Frances R. and John J. Duggan Distinguished Professor, University of Southern California Gould School of Law. This 12/19/18 draft is posted with the permission of Oxford University Press. Special thanks to Daniel Solove, Paul Ohm, Victoria Schwartz, and the law faculties at UC Hastings College of Law and Pepperdine University for comments on an earlier draft. Comments are very welcome. Please help me improve the chapters by sending your comments to orin@orinkerr.com.

TABLE OF CONTENTS

Chapter 6:
The *Carpenter* Shift

The Supreme Court's June 2018 ruling in *Carpenter v. United States*[1] is a blockbuster for the Digital Fourth Amendment. Before *Carpenter*, Fourth Amendment protections were tied to places and things. They depended on where the information was coming from – on what the government learned about happenings in a location or item – echoing the textual focus of the Fourth Amendment on protecting "persons, houses, papers, and effects." *Carpenter* embarks on a new path. To ensure that digital technology does not hand the government too much power, *Carpenter* adds protection to information because of what it may reveal.

My views on *Carpenter* are mixed. On one hand, the Court's instincts are right. *Carpenter* is a resounding win for the theory of equilibrium-adjustment. The Court was trying to do what this book argues they should: Adjust Fourth Amendment rules for the digital age to restore the earlier balance of government power. The Justices feared that the digital age alters the fundamental balance of the Fourth Amendment because so many private records are now easily accessible to the government outside of places or things. The Court countered that change by introducing Fourth Amendment protection for at least some of those records to restore the prior balance. It was pure equilibrium-adjustment.

But there's a catch: the Court's decision was premature. The Court's case for equilibrium-adjustment portrayed the records as more precise, comprehensive, and all-encompassing than they are. This creates a puzzle. If you take the technology in *Carpenter* as it actually exists, the case for equilibrium-adjustment in that case was weak. But if you accept *Carpenter's* factual presentation as true, the case for equilibrium-adjustment was much stronger. More importantly for us, by presenting the facts as they did, the Court laid the groundwork for the similar treatment of digital technologies present and future that genuinely raise the concerns the Justices expressed in *Carpenter*. *Carpenter* sends an unmistakable message, premature but urgent: Some kinds of Internet

[1] 138 S.Ct. 2206 (2018).

metadata now must be protected to restore limits on access to metadata otherwise reduced by digital technology.

The challenge is how to do that. Detaching the Fourth Amendment from its traditional focus on places and things requires a new Fourth Amendment theory of information transfers. That's hard for a very practical reason: It requires line-drawing where no obvious lines exist. Chapter 1 showed how the Fourth Amendment requires certainty. The police need to know what they can legally can do, and the citizen needs to know what the police legally *can't* do. To help them both, the law must be clear.

Carpenter poses a major challenge for the digital Fourth Amendment because information transfers are hard to regulate using bright lines divorced from places or things. Computers and the Internet store and transmit extraordinary quantities of information. What information should be protected, collected how, and obtained by the government when? *Carpenter* hints at a middle ground that the decision does not fully develop. The law now must protect some information but not all of it, separating out certain kinds of information and subjecting it to special treatment based on the new powers of the digital age. This is no easy task.

A footnote in *Carpenter* recognized the difficult issues but put them aside for another day. "We do not begin to claim all the answers today," the Chief Justice acknowledged, in light of "the manifold situations that may be presented by this new technology."[2] Not having all the answers, the Court decided "no more than the case before us."[3] Hard questions await. The digital age is about connection. It is about using digital services that help us do things and that necessarily keep records of how they do it. When the government wants those records, what rules apply?

We know from Chapter 5 that contents of communications are protected, but what about the non-content records? What about IP addresses kept by an Internet service provider? Or account logs of how an app was used? Or lists of websites a user visited? Or records of when a messaging service was used by one person to contact another? Courts must find a way to implement *Carpenter* for Internet data that is true to the language in the decision, faithful to the principles of equilibrium-

[2] *Id.* at 2220 n.4.
[3] *Id.*

adjustment on which it rests, and yet also provides the clear rules that the Fourth Amendment demands.

This Chapter offers a set of principles to implement *Carpenter.* It argues that non-content Internet records should be protected under the Fourth Amendment when three requirements are met. All three requirements must be satisfied for a category of records to gain Fourth Amendment protection. Here are the three requirements:

First, *Carpenter* applies only to collection of information made widely possible by surveillance methods of the digital age. Traditional forms of surveillance that predate the digital age are categorically exempt. To trigger a search, the government must collect non-content records that are made available because of the "seismic shift" of the digital world.

Second, records must not be the product of a user's meaningful voluntary choice. *Carpenter* applies to records that are necessarily created when a person uses core technologies of the digital age. However, it does not apply to records that a user might choose to create beyond what participation in modern Internet life requires.

Third, the records must be of a type that tends to reveal an intimate portrait of a person's life beyond the legitimate interests of criminal investigations. The records will reveal personal information typically beyond state interference such as our personal associations, religious beliefs, sexual preferences, and political views. This aspect of *Carpenter* reflects its focus on protecting the innocent from surveillance and exposure of embarrassing or unpopular facts.

The Traditional Place-or-Thing-Based Fourth Amendment

It helps to begin by recognizing the novelty of *Carpenter's* method. Fourth Amendment searches traditionally have focused on places and things. Knowing how the Fourth Amendment applies required identifying the place or thing from which the information was obtained instead of the nature of the information collected there. If the government revealed information from inside a place or thing the Fourth Amendment protects, it is a search. Think of the interior of houses, inside pockets, inside the trunks of cars, and inside packages. On the other hand, if the government collected the information from a place or thing the Fourth Amendment doesn't protect, no search occurred. Examples would include information found in public or otherwise exposed to public view.

The source of the information determines how the Fourth Amendment applies.

Arizona v. Hicks shows how this traditional approach works.[4] An officer entered an apartment after shots were fired from inside. After looking around for the shooter, the officer noticed expensive stereo equipment in the otherwise squalid apartment. The officer guessed that the equipment might be stolen, so he moved a turntable enough to see the serial numbers on its bottom so he could check the number with databases of stolen property. The officer's hunch was right. The equipment was stolen. When charges against Hicks followed, he argued that the police had searched his apartment improperly by moving the stereo equipment to find the serial numbers and learn that the equipment was stolen.

The Supreme Court agreed. Moving the turntable just a few inches was a search, the Court held, because it "exposed to view concealed portions of the apartment or its contents."[5] The equipment was in Hicks's apartment. That apartment was his place that was entitled to constitutional protection. And that was the whole case. "It matters not," the Court explained, "that the search uncovered nothing of any great personal value." "A search is a search," the Court declared, "even if it happens to disclose nothing but the bottom of a turntable."[6]

We see the same focus on location in cases on high-technology surveillance. In two cases in the 1980s, officers wanted to know where narcotics suspects had set up their drug labs. After radio beepers were secretly installed in property controlled by the suspects, the officers tracked the location of the beepers to learn where the suspects were going. In the first case, *United States v. Knotts*,[7] the officers tracked the property when it was in the suspect's car traveling over public roads. In the second case, *United States v. Karo*,[8] the officers tracked the property after it was carried into the suspect's cabin.

The Supreme Court treated the two cases differently because the beepers revealed information from different places. The entrance of the property into the cabin triggered a search, *Karo* held, because it revealed information "about the interior of the premises," namely "that the beeper

[4] 480 U.S. 321 (1987).
[5] *Id.* at 325.
[6] *Id.*
[7] 460 U.S. 276 (1983).
[8] 468 U.S. 705 (1984).

was inside the house."[9] The monitoring over public roads did not trigger a search in *Knotts*, however, as it merely gathered information about what happened in "public places."[10] The place searched – the origin of the information revealed – was the key.

It's true that the Supreme Court famously said, in *Katz v. United States,* that "the Fourth Amendment protects people, not places"[11] Based on that statement, you might think that the reasonable expectation of privacy test introduced in Justice Harlan's *Katz* concurrence effectively ended any place-based doctrine. But it didn't. A quick explanation of why is helpful.

The question in *Katz* was whether Katz's Fourth Amendment rights were implicated when the government used a microphone taped to a public phone booth to listen to phone calls he was making inside it. The parties' briefs focused on whether a public phone booth was a Fourth-Amendment-protected space like a home (Katz's view) or an unprotected space like an open field (the defendant's view). Justice Stewart's majority opinion churlishly corrected the litigants for focusing the analysis solely on place. To have Fourth Amendment rights, *Katz* explained, more than the place mattered. To have Fourth Amendment rights, a person in a protected space must also make efforts to hide his activity from outside observation. Some personal effort was required. Ergo, "The Fourth Amendment protects people, not places."

But it was still the place that mattered most in *Katz*, as Justice Harlan's concurrence later adopted by the Court made clear. Justice Harlan dismissed the famous statement that the Fourth Amendment protects people instead of places: "The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a 'place.'"[12] Katz had Fourth Amendment rights in a public phone booth, Justice Harlan explained, because, "like a home" and "unlike a field," a phone booth was "an area" where a person could have Fourth Amendment rights. As Justice Harlan put it, a phone booth was a place where a person's expectation of privacy could be "be one that society is prepared to recognize as reasonable." The place controlled the scope of the Fourth Amendment. The key question was

[9] *Id.* at 715.
[10] *Knotts*, 460 U.S. at 276.
[11] Katz v. United States, 389 U.S. 347, 351 (1967).
[12] *Id.* at 361 (Harlan, J., concurring).

whether a person had a reasonable expectation of privacy in a particular place or thing: Whether that place was sufficiently home-like to merit Fourth Amendment rights.

The Fourth Amendment's focus on places and things is no modern invention. It's right there in the text. The constitutional text recognizes a right of the people to be secure against unreasonable searches and seizures "in their persons, houses, papers, and effects."[13] The scope of the right is textually limited to these four places or things. One of the four is a physical place – "houses." The other three are things – "persons," "papers," and "effects." The cases applying *Katz* have remained surprisingly loyal to that textual focus. It's easy to assume that the *Katz* reasonable expectation of privacy test was a departure from the text. Neither the majority nor Justice Harlan focused on text or history in their Katz opinions. But the Supreme Court's application of *Katz* has closely traced the Fourth Amendment's focus on places and things. That location focus is the heart of what the Fourth Amendment protects.

Carpenter's New Expectation of Privacy Test

Or at least all of this was true until June 22, 2018, when the Supreme Court handed down *Carpenter v. United States*.[14] *Carpenter* signals a major break from the traditional understanding. For the first time, the Fourth Amendment is no longer about places and things. *Carpenter* signals a new kind of expectation of privacy test, one that focuses on how much the government can learn about a person regardless of the place or thing from which the information came.

A close look at *Carpenter* reveals its departure. Recall from Chapter 3 that *Carpenter* is the case involving a string of robberies. A member of the group agreed to cooperate with the government and told the investigators the cell phone numbers of every participant. The government obtained the cell-site records for the group's cell phones. The records showed that Timothy Carpenter and his co-conspirators consistently were in the general neighborhood of the robberies around the time the crimes occurred. The legal question was whether the government violated the Fourth Amendment by obtaining Carpenter's cell-site

[13] U.S. Const. Amend. IV.
[14] 138 S.Ct. 2206 (2018).

records using a court order under a federal privacy law, the Stored Communications Act, that requires judicial approval but uses a standard less than the Fourth Amendment's traditional probable cause hurdle.

The Sixth Circuit Court of Appeals held that the Fourth Amendment was not violated because Carpenter was not searched.[15] The cell-site records were created by the cellular service providers to deliver their customer's calls, and the records were stored by providers for their own business purposes. In short, the records were the companies' records, not the phone owner's. This is the traditional place-and-thing-based Fourth Amendment in action. The records were generated by the companies and stored by them on the company's computers for the company's purposes. The companies, not the users, had Fourth Amendment rights in them.

The Supreme Court disagreed, and in a novel way. Writing for the majority, Chief Justice Roberts started with an interesting fact about life "[p]rior to the digital age."[16] Back then, it was difficult and costly for the police to track a person's physical movements over time. Societal expectations about what the police could do generally ruled out detailed location tracking. But technological change has now made that tracking easy. Thanks to the widespread use of cell phones, tracking records are now available that did not exist before. And the records were not only available, but easily accessible. Obtaining them was "remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense."[17]

That brings us to *Carpenter*'s key move. According to the Court, the technological change from difficult-and-rare location tracking to easy-and-common location tracking "contravene[d] that expectation" from the past. The ability of today's technology eliminated the expectation of privacy that existed before. Note the shift. Before *Carpenter*, the *Katz* test was about places and things. The law asked whether government action violated a reasonable expectation of privacy in a particular place or thing. *Carpenter* asks a different question: Has technology changed expectations of *what the police can do*?

---

[15] *See* United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016) (Kethledge, J.)
[16] *Carpenter*, 138 S.Ct. at 2217.
[17] *Id.* at 2218.

If the police can easily take investigative steps that far exceed their powers in the past, the thinking runs, that newfound ability violates a reasonable expectation of privacy. The question isn't what government action violates a person's reasonable expectation of privacy in persons, houses, papers, and effects. Instead, the question is whether technological change has rendered obsolete a past expectation of a practical limit on government power. In *Carpenter*, the reasonable expectation of privacy test does not ask whether the place or thing is home-like. Instead, it asks about whether a prior limit on government power has been lifted.

It's worth speculating about why the Court reformulated the *Katz* concept in this way. I think the reason is that equilibrium-adjustment forced the change. Chapter 3 explained how *Carpenter* is premised on the theory of equilibrium adjustment.[18] When technology expands government power in a transformative way, courts change the Fourth Amendment rules to restore preexisting limits on that power. Before the digital age, people could keep much of their private information private by keeping it in places and things that they controlled. Places and things like their homes, their offices, their rented safe deposit boxes, and the like. A Fourth Amendment limited to a person's places and things still gave people significant control over their private information.

Carpenter reflects the majority's fear that digital technology has displaced that assumption. Third-party network providers in the ordinary course of business now keep and store detailed records of what their users do. If those records reveal deeply personal facts about individuals, then the computer age signals a major shift in where private records are stored and who can control them. Thanks to digital technologies like cell phones, the government has a new way to collect location information without accessing information from the suspect's place or thing. The information is now collected and stored automatically by cellular providers, far from cell phone users and largely unbeknownst to them. The sensitive records have moved. A majority of the Justices felt they needed a new way for the Fourth Amendment to protect private information wherever it went.

Carpenter's reformulation of the *Katz* test likely seemed the most direct way to conduct the equilibrium-adjustment that restored the prior

[18] [Author's Note: For those unfamiliar with equilibrium-adjustment, see Orin S. Kerr, *An Equilibrium–Adjustment Theory of the Fourth Amendment*, 125 Harv. L. Rev 476 (2011).]

balance. Forget about context and just look at the words in isolation: The phrase "reasonable expectation of privacy" seems to echo life experience. If technology expands government power so much that equilibrium-adjustment demands new limits, you can squeeze that into the *Katz* test by expressing the new power in an expectation-based way.

In particular, you just need to assume that people reasonably expect the police to do what technology lets the police easily do. Before the digital age, nobody would have expected the government to have invasive tracking power. Today, though, the police have an ability they previously lacked. As a result, the new technology violates past expectations of government power. Gathering cell site records violates a reasonable expectation that the government couldn't violate privacy the way it now does. New powers mean new practices, and new practices means new expectations of those practices. And voila: The *Katz* test restores the expectation of privacy that technology took away.

To be fair, my presenting the Court's reformulation of *Katz* as entirely new is a slight exaggeration. But only a slight one. *Carpenter* based its test on the concurring opinions in *United States v. Jones*[19] in 2012, and particularly Justice Alito's concurrence in that case. Investigators in *Jones* had secretly installed a GPS device on a car that and monitored its location for 28 days. Justice Alito's concurrence was mostly devoted to disagreeing with the majority's view that the installation of the GPS device was a search.[20] At the end, however, Justice Alito added a single paragraph explaining why the long-term monitoring of the GPS device was a search. That explanation later became the main authority for *Carpenter*.

A search occurred in *Jones*, Justice Alito argued, because "a reasonable person would not have anticipated"[21] the police to engage in long-term monitoring for a routine criminal case. Sure, people would expect the police to engage in "relatively short-term monitoring" of location, such as what happened – and was deemed no search – in the *Knotts* beeper-over-public-roads case. But 28 days of location monitoring was more than people traditionally expected from the police, at least in cases that were not "extraordinary." By exceeding expectations of how the police investigated routine criminal cases, Alito reasoned, the

[19] United States v. Jones, 565 U.S. 400 (2012).
[20] *See id.* at 419-27 (Alito, J., concurring).
[21] Id. at 430 (Alito, J., concurring).

government's 28 days of monitoring violated a reasonable expectation of privacy and was a search.[22]

In *Carpenter*, Chief Justice Roberts cited and relied on Justice Alito's framework from *Jones*, elevating the idea of focusing on past expectations of police practices from a mere concurring opinion (that itself cited no authority) to a majority opinion that is now binding authority.[23] The Chief Justice also subtly changed the focus. Justice Alito's brief analysis in *Jones* appeared to hinge on a case-by-case expectation. It considered whether a reasonable person traditionally would have expected the police to engage in the long-term and detailed monitoring that happened in *Jones* in a *Jones*-like case.

Carpenter works at a higher level of generality. It asks, did the police traditionally have easy access to detailed location tracking records? And do they have that access today? The trigger for the search was not the details of what the police learned about Carpenter in that particular case. Instead, the trigger was the broader technological shift that enabled the police to learn a lot about everyone who used a cell phone – that is, everyone. It's as if the technology violated a reasonable expectation of privacy rather than the government that used it.

Whether you credit Chief Justice Roberts in *Carpenter* or Justice Alito in *Jones* for introducing the idea, the Court has now adopted a new approach to the expectation of privacy test that focuses on changes in police powers. When technology enables surveillance that could not occur before, the new surveillance becomes a search. To avoid a dramatic increase in government power, the new surveillance tools that digital technology creates are to be slotted into the legal box of searches that require a warrant.

The Wrong Facts, But at Least a Plausible Case on the Wrong Facts

This brings us to the oddest part about *Carpenter*. The Court presented government access to historical cell-site information as a "seismic shift" in government power. But the record in the case suggests otherwise. The record suggests that access to cell-site information is more an incremental increase in government power than a radical

[22] *Id.*at 430-31 (Alito, J., concurring).

[23] *Carpenter*, 138 S.Ct at 2215 (referring to the *Jones* concurrences as setting out views to which "five Justices agreed"); *Id.* at 217-18 (relying extensively on the *Jones* concurrences).

transformation. This means that the Court's case for equilibrium-adjustment was a bit, well, made up. Perhaps this creativity will prove prescient someday. But today it makes the equilibrium-adjustment in *Carpenter* more preventive than necessary. The Court jumped into equilibrium-adjustment based on fears of new government powers rather than proof of it.

The gap between the facts of the case and the Court's description of the technology explains my conflicted views of the opinion. On one hand, I think *Carpenter* was wrongly decided based on its facts. Historical cell-site records don't shift government power in a transformative way. Given the practical and conceptual challenges of developing a new theory of the Fourth Amendment outside the context of protected places or things, the Court should have waited to see if that technological future came to pass and if that equilibrium-adjustment was truly needed. The better approach would have been to follow existing law and allow legislatures to continue to provide the privacy protection that was felt appropriate and to debate if more or less privacy was helpful.

On the other hand, *Carpenter* seems quite plausible if you assume the Court's vision of the technology is true. Equally importantly, there are other digital technologies that raise the dynamic that *Carpenter* imagined in cell site records. By taking a leap when the facts didn't support it, the Court necessarily created a new framework for equilibrium-adjustment for other aspects of Internet surveillance that may more directly raise the kinds of concerns that animated the case. The Court applied the right theory to the wrong facts, suggesting but not developing a theory that may prove more attuned to other facts that better support its framework.

Let me spend a few pages explaining why I see a big gap between what the record showed and how the Court described historical cell-site information. Start with the record. After Carpenter and his gang committed the string of robberies, one of Carpenter's conspirators flipped and cooperated with the investigators.[24] He told them about Carpenter's involvement in the robberies and gave them Carpenter's cell phone number. Investigators went to court and obtained a court order for the cell phone location records for that number, as required under a federal privacy law called the Stored Communications Act.[25]

---

[24] *Carpenter*, 138 S.Ct. at 2212.
[25] 18 U.S.C. 2701 *et se*

According to testimony offered at trial, the records revealed the location of Carpenter's phone within a half-mile to two miles whenever a call was made or ended.[26] The government then used the records, together with other evidence, to help show the jury that Carpenter and his conspirators were in the general neighborhood of four of the nine robberies around the time they happened.[27]

But how much did the records actually reveal? Here's where the gap emerges. The evidence in *Carpenter* indicated that the records didn't pinpoint precisely where the phone was located. The half-mile-to-two-mile imprecision meant that the records could provide rough neighborhood information. You might know the phone was somewhere in the west side of town, for example, but that's it. Plus, the records only existed for particular times when a call was started or ended from that phone. If no calls were made, no records existed of the phone's location. And of course the records didn't say who was using the phone at the time. For all these reasons, there was no evidence that the records revealed anything interesting or private beyond the phone being in the general neighborhood of several robberies around the time they occurred.

Admittedly, the government obtained *a lot* of individual location records. The string of robberies had spanned two years.[28] The government presumably wanted to show Carpenter's involvement in all of them. The court authorized the disclosure of Carpenter's records for a 152-day period from his cell provider and for a 7-day period from another provider on whose network his phone was "roaming." The first provider produced 127 days of records of the 152 days sought, and the second added another two days of the seven sought.[29]

When combined, the records included 12,898 location entries.[30] Put together, the providers gave the government records for about 80% of the days in the period ordered, and about 100 records per day – averaging about one record every 15 minutes – for those 80% of the days on which records were available. That's a large number of records. But remember that the records themselves only showed the phone's location to about half a mile to two miles from a particular tower.

---

[26] See id. at 2225 (Kennedy, J., dissenting).

[27] See id. at 2226

[28] Trial transcript, United States v. Carpenter, Eastern District of Michigan, (Closing argument of the prosecutor at p. 41).

[29] These figures are found at *Carpenter*, 138 S.Ct. at 2212.

[30] *See id.*

Contrast this with how *Carpenter* describes historical cell site records. The records permit "absolute surveillance,"[31] the Court says. Everyone has "effectively been tailed every moment of every day for five years,"[32] the current retention period of records of major cell phone providers. "[W]hen the Government tracks the location of a cell phone," the Court states, "it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user." [33]

Carpenter presents the surveillance as not just absolute and perfect but also profoundly invasive of privacy. The records are "deeply revealing" [34] because of their "depth, breadth, and comprehensive reach" and because they are "continually logged."[35] The records are a "detailed chronicle of a person's physical presence" at "every moment" for years. The resulting records are "all-encompassing," "detailed, encyclopedic, and effortlessly compiled," [36] an "exhaustive chronicle" [37] of everyone's location that reveals not only the places everyone went "but through them [their] familial, political, professional, religious, and sexual associations."[38]

In short, *Carpenter* presents historical cell site records as the 2018 equivalent of Big Brother in George Orwell's dystopian novel *1984*.[39] In Orwell's novel, every citizen is under constant and inescapable surveillance from telescreens that act as security cameras for the state. Everyone is warned: Big Brother Is Watching You. *Carpenter* envisions access to historical cell site records as similar. The records and surveillance are "absolute," "near perfect," "deeply revealing," "encyclopedic," "all-encompassing," and "exhaustive."

As I understand the record in *Carpenter,* however, this isn't actually true. Because the records were precise only to a range of about a half-mile to two miles, and records were only generated at some times (and

[31] *Id.* at 2218.
[32] *Id.*
[33] *Id.*
[34] *Id.* at 2223.
[35] *Id.*at 2218.
[36] *Id.*at 2216.
[37] *Id.*at 2219.
[38] Carpenter, 138 S.Ct. at 2217 (quoting Unitd States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).
[39] George Orwell, 1984 (London: Secker and Warburg, 1949).

available only on certain days), the records were not the transformative Big Brother that the Court portrays.

What explains that gap? Chief Justice Roberts addresses it briefly, although not in my view persuasively. First, he suggests that the cell site records were still invasive even if other information had to be added to them to make them meaningful.[40] Indeed, the Chief Justice notes, the government thought the records "accurate enough to highlight it during the closing argument"[41] of Carpenter's trial.

But this is weak. The primary evidence against Carpenter was the direct testimony of several of his conspirators about precisely what Carpenter did and said.[42] It was that evidence, not the cell site records, that mattered. The prosecutor did mention the cell site records in the closing argument.[43] But it was only an afterthought. When you read the transcript, the cell-site records are mentioned only briefly near the end of the closing argument as some "extra corroborating evidence."[44] It was a side show, not the main event.

Second, the Chief Justice argues that technology is changing to make the technological picture he drew more accurate. "While the records in this case reflect the state of technology at the start of the decade," he writes, "the accuracy of CSLI is rapidly approaching GPS-level precision."[45] New technology has given cell phone providers "the capability to pinpoint a phone's location within 50 meters," he wrote, citing a brief filed by a coalition of civil liberties groups.[46]

This was more aspirational than real, however. The civil liberties brief relied on 2012 congressional testimony by a leading computer science professor, Matthew Blaze.[47] Blaze is certainly an expert on cell-site surveillance. But the cited part of his testimony was about trends in

---

[40] *See id.* at 2218.

[41] *Id*. at 2218.

[42] Trial transcript, United States v. Carpenter, Eastern District of Michigan, (Closing argument of the prosecutor at p. 41).

[43] *See id.* at [].

[44] *Id.* at 54.

[45] *Carpenter*, 128 S.Ct. at 2219.

[46] *See id.* (citing Brief for Electronic Frontier Foundation et al. as Amici Curiae).

[47] *See* Brief for Electronic Frontier Foundation et al. as Amici Curiae at 12 (citing Matthew Blaze, Testimony Before the House Committee on the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security Hearing on ECPA, Part 2: Geolocation Privacy and Surveillance, April 25, 2012, available at https://judiciary.house.gov/wp-content/uploads/2016/02/Blaze-Testimony.pdf).

technological capability, not the actual practice of cell phone providers that retain historical cell-site records.[48] I am unaware of any actual case, then or now, in which investigators obtained historical cell-site records that featured the kind of precision the Court described. Both then and now, historical cell site records typically indicate the rough neighborhood of a cell phone, not the phone's precise location.

To be sure, Chief Justice Roberts faced a hard problem in describing the invasiveness of the records in *Carpenter*. The first problem, alluded to in the opinion, is that cell-site technology is still evolving. Ongoing technological change makes the significance of cell site records something of a moving target. In my view, that counseled in favor of delay in deciding how the Fourth Amendment applies. It's hard for a court to engage in equilibrium-adjustment successfully before a technology stabilizes.[49]

A second problem the Chief Justice faced is the difficulty of measuring the intrusiveness of records held in the ordinary course of business by private companies. Private companies can do what they want. How many records exist, and how much detail they show, is a business choice beyond the Supreme Court's control. At one extreme, a cell phone provider could decide to keep no historical cell-site records. If the government came a year later seeking records, the provider would just say none exist and that would be the end of it. At the other extreme, the provider could decide to keep very detailed records of every connection. How much the records reveal would depend on each company's policies, each technology, and even each user. Perhaps the Chief Justice imagined a worst-case scenario for privacy because it could not control the business choices that could limit that worst-case scenario.

Whatever the reason, *Carpenter* presents access to historical cell-site records as a "seismic shift" in technology that demands equilibrium-adjustment. The question going forward is how courts should follow *Carpenter*'s framework for equilibrium-adjustment for other records. Now a search occurs when the government learns enough information about a person in a way that upsets traditional expectations of police power. It doesn't matter where the government gets the record – whether it obtains the record on its own or by accessing the records held by a third

---

[48] See https://judiciary.house.gov/wp-content/uploads/2016/02/Blaze-Testimony.pdf

[49] *See* Kerr, *Equilibrium-Adjustment*, 125 Harv. L. Rev. at 539-42.

party service provider. Some kind of *information transfer*, defined *somehow*, now becomes a search because of the kind of information it is. We need a theory of Fourth Amendment sensitive information that explains when an information transfer to the government has crossed the line from non-search to a search. The remainder of this chapter tries to develop and apply that theory.

Step 1: The New Records of the Digital Age

The first requirement for a *Carpenter* search should be that the records collected are available because of digital technology. The records must be of a kind and nature that generally could not be collected in a pre-digital age. Pre-digital records and their modern equivalents are exempt, sort of like a constitutional grandfather clause. Only new kinds of records that the digital age has enabled can trigger the new search doctrine.

This limit originates in *Carpenter* itself. According to the Chief Justice, "seismic shifts in digital technology" have "made possible" access to "an entirely different species"[51] of data that "do[] not fit neatly under existing precedents."[52] This created "new concerns wrought by digital technology" that were inconsistent with viewing the cell-site records as simply a new form of an old record that should be treated like the old records. Only the new records exceed society's expectation from "[p]rior to the digital age" about what "law enforcement agents and others" would or could do. "There is a world of difference," the Court concluded, "between the limited types of personal information" at issue before the digital age and the "exhaustive chronicle"[53] of information the new technologies can provide.

Carpenter therefore leaves untouched what it calls "conventional surveillance techniques and tools."[54] Pre-digital technologies such as security cameras are merely examples of "garden-variety"[55] surveillance familiar from the past that are exempt. Old forms of surveillance that

[50] *Carpenter*, 138 S.Ct. at 2219.
[51] Id. at 2222.
[52] Id. at 2214.
[53] Id. at 2219.
[54] Id .at 2220.
[55] Id. at 2219.

existed before the digital age, and that haven't since been transformed, are exempt. *Carpenter* simply does not apply to "conventional" and "garden-variety" information gathering. It is solely about using the new tools of the digital age. *Carpenter* therefore does not disturb the traditional third-party doctrine cases of *Smith* and *Miller*, involving access to numbers dialed from a telephone (in 1979) and access to bank records (in 1976), at least on their facts. *Carpenter* only regulates new law enforcement capacities that did not exist or were rare before the digital age.

The idea of limiting *Carpenter* to new surveillance data of the digital age may seem odd at first. If the goal is to distinguish police practices that invade privacy from those that don't, distinguishing between digital and pre-digital practices seems an imperfect line. Many longstanding investigative practices invade privacy, often more than newer techniques. For example, it's surely invasive for the police to obtain all of your bank records so they can examine your financial transactions and learn what you bought and from whom. In 1976, in *United States v. Miller*,[56] the Supreme Court ruled this was not a search under the third-party doctrine. *Carpenter* carefully notes that it "do[es] not disturb"[57] this result. It's fair to ask why: Why should the law leave traditional surveillance practices unregulated by the Fourth Amendment if they invade privacy more than digital surveillance practices that Carpenter now makes a search?

There are two reasons. A doctrinal reason is that *Carpenter* is premised on exactly this distinction. *Carpenter* extended Fourth Amendment protection to digital records when their pre-digital equivalents were not protected on the theory that digital records are categorically different. If you accept that premise, you can't then reason that pre-digital equivalents should be protected on the theory that the pre-digital records are fundamentally the same. If differences justify a departure, similarities can't also justify a fusing. The advent of the digital world requires new rules for the new world without changing the old. You don't get *Carpenter* without that distinction.

It's worth noting that Timothy Carpenter himself benefited from this divide. The cell-site records obtained in his case were too imprecise

[56] 425 U.S. 435 (1976).
[57] *Carpenter*, 138 S.Ct. at 2219.

to reveal anything particularly private about him.[58] But this made no difference, as the records belonged to "an entirely different species" of records that caused a "seismic shift" in police power. A search occurred because the records were on one side of that seismic shift even if they did not reveal anything particularly invasive in his case. The flip side of that should also be true: Collection of traditional kinds of records should be categorically exempt from *Carpenter*.

The second reason for limiting *Carpenter* to new digital records is consistency with the theory of equilibrium-adjustment. As Chapter 5 explained, the original Fourth Amendment drew a dividing line between inside spaces like homes that were protected and outside spaces like open fields that were not. The first major communications network, the postal network, effectively replicated this distinction over a network. This permitted courts to draw information equivalents. The inside of letters and packages was the network equivalent of indoor protected space (and therefore opening letters and packages was a search) while outside envelope information was the network equivalent of delivery information in public (and therefore accessing it was not a search).

The traditional telephone network of the twentieth century replicated the same function. As a result, the same information equivalents could be drawn. The contents of calls was the network equivalent of private spaces (protected), and collecting metadata for phone calls was the network equivalent of observation in public space (unprotected). And that was the law before *Carpenter*. Drawing information equivalents turned the traditional Fourth Amendment distinction between inside and outside in physical space into the simple rule that contents are protected while metadata are not protected in network space.[59] In a pre-digital world, those equivalents held.

Carpenter reflects the understanding that digital technologies and the Internet are different. Digital networks work like any network in some ways, of course. They send and receive communications, substituting for in-person transaction, just like the traditional postal network and telephone network. But *Carpenter* reflects a judicial belief that digitization means "a new phenomenon"[60] – the effective creation of

[58] This point was emphasized in Justice Kennedy's dissent, and also in Judge Kethledge's opinion for the Sixth Circuit below.

[59] See Chapter 5.

[60] *Carpenter*, 138 S.Ct. at 2216.

some "unique"[61] kinds of new records – and that those new records must be treated differently. Although the new records are the network equivalent of traditional eyewitness testimony in some sense, the reality that everything can be recorded and stored means that third party providers "are not your typical witnesses."[62] "Unlike the nosy neighbor who keeps an eye on comings and goings," the new witnesses of the Internet are "ever alert, and their memory is nearly infallible."[63]

From this perspective, a new approach is needed limited to the new records of the digital world to best maintain the original balance that existed before the Internet age. Functional translation worked for the postal network and the early telephone network because they did not dramatically transform what records existed. But the digital age is an inflection point that changes what records are available and therefore what powers investigators have to collect those records. Courts must try to restore the old levels of power by separating out the new kinds of records and subjecting them to Fourth Amendment regulation.

At the same time, the pre-digital records that remain the network equivalent of public surveillance should still be unprotected. Those records are still of a kind that existed and was collected before the transformation of the digital era. Leaving these traditional forms of surveillance as non-searches is essential to maintaining the traditional balance of government power. This results in *Carpenter*'s first limit: The new records get the new treatment, while the old records and their equivalents remain unprotected.

Applying this distinction will require some hard judgment calls. We need to identify recurring features of different kinds of records and classify them as akin to traditional records or as part of a new digital category. Technology won't always make that easy. New technologies do not neatly fall into categories. The legal test requires a technological essentialism that the technology can resist. Different companies may offer different versions of the same functionality that make different kinds of records available. The Internet changes rapidly, with new services and new apps and new capabilities appearing (and disappearing) regularly. Identifying a set of records and understanding its characteristics as similar

[61] Id. at 2217.
[62] Id. at 2219.
[63] Id.

to or different from a preexisting set of records necessarily involves identifying points on a continuum.

Step 2: The Records Must Be Created Without Meaningful Voluntary Choice

The second requirement is that *Carpenter* applies to records created without the subject's meaningful voluntary choice. This is plainly met when the government conducts the surveillance or orders a third party provider to do it. In *Jones*, for example, Jones had no meaningful choice about whether the government would track his location with the GPS secretly attached to his car. The requirement is also met when the government collects third-party records that are inescapably created through use of broadly-used services. On the other hand, *Carpenter* should not apply to records that are generated only because a user made a voluntary decision to allow a third-party to generate that record.

This requirement again comes from *Carpenter* itself. Remember that the government's main argument relied on the third-party doctrine. In the government's view, the third-party doctrine applied because Carpenter voluntarily disclosed his location information to his cell phone provider. Carpenter knowingly used the phone. Carpenter therefore must have known he was sharing the location information needed to make the phone work. According to the government, the voluntary disclosure of the defendant's location to his phone provider made the provider an eyewitness to his location.

The Court disagreed. There was no voluntary disclosure in a "meaningful sense,"[64] Chief Justice Roberts reasoned, because cell-site location tracking was inescapable. The records were created automatically whenever the phone was used. And cell phones had become "such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society."[65] "Apart from disconnecting the phone from the network," the Chief Justice explained, "there is no way to avoid leaving behind a trail of location data."[66]

[64] Id. at 2220.
[65] Id. (quoting Riley, 573 U.S. at [].)
[66] Id.

This passage implies that *Carpenter* has a compulsion requirement. The third-party doctrine applies when you volunteer your information to someone. But participating in modern society requires using a cell phone, and that gives you no real choice whether to disclose your location. For *Carpenter* to apply, this passage suggests, the records must not be created by a person's meaningful voluntary choice.

The key word is "meaningful," and it's worth pondering what the Court had in mind. *Carpenter*'s notion of voluntariness appears to be a normative judgment rather than a fact. *Carpenter* asks a philosophical question: What uses of digital technology are "indispensable to participation in modern society"? To answer that, you need to know three things. First, what does modern society look like; second, what does it mean to participate in that society; and third, what technologies are needed to achieve that participation. If people can't help but generate a record to participate in modern life, then creating the record is not voluntary in the Court's "meaningful" sense. This is a judgment call, obviously, not mechanically turning a crank to produce the answer.

Carpenter's compulsion requirement can be understood as a modern translation of traditional Fourth Amendment principles. The traditional Fourth Amendment rule in physical space is that you have rights inside private spaces as long as you protect them from outside view. This is the core of the two-part *Katz* test. To have Fourth Amendment rights in a place, Justice Harlan explained, the space needed to be one that the Fourth Amendment protects and a person also had to take acts that showed an "intention to keep" the space "to himself."[67] Exposing your protected information "to the plain view of outsiders,"[68] such as by opening the door and letting anyone in, eliminated protection.

A compulsion requirement acts as an equilibrium-adjustment of that rule for a world of shared information. Some amount of sharing is inevitable in a networked world. *Carpenter* treats the inevitable sharing as a baseline and protects it. To draw an analogy, the Court treats the digital space like a world where technology requires our virtual homes to have a front window that you can't cover. As a matter of technology, you can't stop the neighbors from peering in that window. *Carpenter*'s compulsion requirement works like a legal rule that the government can't look in that

[67] Katz, 389 U.S. at 361 (Harlan, J., concurring).
[68] Id.

window. If the technology requires the window, the law has to step in and add new protections to limit government snooping.

The flip side is that if a person volunteers to reveal information about himself to others, beyond what the technology requires, that information is still unprotected. Opting to share your Internet records with others today is like leaving your front door open to your neighbors in the past. You can leave the front door open if you want. Or you can close it, as most do. As long as you have a choice – a choice beyond what the Court deems essential to participation in modern life – what you decide to expose is on you.

Step 3: The Records Must Tend to Reveal "The Privacies Of Life"

The next challenge is to identify the kinds of digital records that trigger its framework. Not all digital records count, because not all records contain personal information. Here's the question: What do the new records need to reveal, or what information do they need to communicate, for government acquisition of those records to be a basis for a *Carpenter* search?

The *Carpenter* opinion and the theory of equilibrium-adjustment again provide the answer. The records must be of a kind that tends to reveal an intimate portrait of a person's life typically beyond legitimate state interest. This reflects *Carpenter*'s focus on protecting the innocent. The goal is to keep investigators from using the powers of the digital age to have unlimited access to embarrassing personal information about us – information such as personal associations, religious beliefs or sexual preferences – that ordinarily has no relevance to a criminal investigation. *Carpenter* prevents that dystopian result by regulating government access to the records likely to reveal such facts.

This limit originates first from a close reading of the *Carpenter* opinion. Obtaining historical cell-site records violates a reasonable expectation of privacy, Chief Justice Roberts reasons, because such records provide "an intimate window into a person's life."[69] Quoting from Justice Sotomayor's concurrence in *Jones*, the Chief Justice notes that comprehensive location records not only revealed physical location but also could reveal a person's "familial, political, professional, religious,

[69] Carpenter, 138 S.Ct. at 2217.

and sexual associations."[70] Such records deserve special Fourth Amendment protection, the Chief states, because they "hold for many Americans the 'privacies of life.'"[71]

This is pretty stirring language. But what does it mean? We can gain additional insight into these quotations by studying their sources. The first source is Justice Sotomayor's opinion in *Jones*, with its language that unlimited location monitoring could reveal a person's "familial, political, professional, religious, and sexual associations."[72] This language reflected a broader fear Justice Sotomayor pressed in her concurrence about how unlimited GPS monitoring could invade and chill associational freedoms. Governments that can track everyone with no Fourth Amendment oversight can easily learn a great deal of highly personal and potentially embarrassing facts about a person that, put simply, are none of the government's business.

Justice Sotomayor in *Jones* cited a 2009 case under the New York state constitution, *People v. Weaver*,[73] that had made the point explicit. Unlimited GPS monitoring could reveal "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar, and on and on."[74] Note the common theme. The driving concern was that the government would have untrammeled ability to learn about our most personal associations and intimate facts -- our sexually-transmitted diseases, our mental illnesses, our sexual preferences, and our religious beliefs – that it could have no legitimate interest in learning.

The second quoted language cited in the Chief Justice's opinion is the "privacies of life." That phrase originated in an 1886 ruling, *Boyd v. United States*.[75] *Boyd* held that the Fourth Amendment's protections inspired from cases of forced government entry into homes also applied to government orders compelling a person to hand over his records. The Fourth Amendment's principles extend beyond direct government entry,

---

[70] Id at 2217 (quoting Jones, 565 U.S. at 415 (Sotomayor, J., concurring)).

[71] Id. at 2217 (quoting Riley, 134 S.Ct., at 2494–2495) (quoting Boyd, 116 U.S., at 630).

[72] Jones, 565 U.S. at 415 (Sotomayor, J., concurring)

[73] 12 N.Y.3d 433 (2009).

[74] People v. Weaver, 12 N.Y.3d 433, 441-442, 882 N.Y.S.2d 357, 909 N.E.2d 1195, 1199 (2009)

[75] 116 US 616 (1886).

the Court reasoned: "[T]hey apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life."[76] The Court breathed new life into the phrase in the 2014 cell-phone search case, *Riley v. California*.[77] In *Riley*, the Chief Justice invoked the privacies of life in light of both the astonishing volume and personal quality of information on a cell phone: "With all they contain and all they may reveal," the Chief intoned, cell phones "hold for many Americans 'the privacies of life.'"

Like *Carpenter*, *Riley* also echoed and cited Justice Sotomayor's *Jones* concurrence for the personal nature of the information revealed. "[C]ertain types of data" often found on a cell phone, *Riley* concluded, are "qualitatively different." *Riley* expressed particular concern about the web browsing records likely to be on a phone: "An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns — perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD."[78]

These passages and their sources from *Carpenter* reflect a specific focus. In *Carpenter*, and in the earlier opinions in *Riley* and *Jones* on which it relied, the Justices focused on limiting government access to records that revealed associational freedoms and intimate facts outside any legitimate government interest. The "privacies of life" that *Carpenter* honors maintains the confidentiality of the "private interests and concerns" central to our identities. They are truths about us, such as our sexual preferences, our medical conditions, and our religious beliefs, that in most cases the state has no legitimate interest in learning. These truths do not reveal evidence of crime. They are just private facts about private people leading quiet lives free from criminal conduct.

It seems no coincidence that these records and the facts they reveal are the kinds of records that have often received special constitutional status under the Fourteenth Amendment. Start with records that might reveal political or religious views. In *NAACP v. Alabama*,[79] the Supreme Court imposed special limits under the Fourteenth Amendment on government efforts to compel expressive groups to reveal their members

[76] Id. at 630.
[77] 134 S. Ct. 2473 (2014).
[78] Id. at 2490.
[79] 357 U.S. 449 (1958).

to the government. According to the Court, expressive groups involved in "political, economic, religious or cultural matters," have a special "immunity from state scrutiny of membership lists" based on "the right of the members to pursue their lawful private interests privately and to associate freely with others in so doing."

Concerns about medical records echo that treatment. In *Whalen v. Roe*,[80] the Supreme Court suggested that there may be a Fourteenth Amendment constitutional right to "avoid[] disclosure of personal matters" that may be implicated by government efforts that disclose medical records. Some lower courts have run with this idea, concluding that "there can be no question that an employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection" under this right.[81] Such information, the Third Circuit has stated, is "within the private enclave" where a person "may lead a private life."[82]

Concerns that surveillance might reveal sexual preferences also echo constitutional concerns outside search and seizure law. Consider *Lawrence v. Texas*,[83] which invalidated sodomy laws under the Fourteenth Amendment. The opening paragraph of *Lawrence* celebrated the Constitution's role in protecting "spheres of our lives and existence, outside the home, where the State should not be a dominant presence."[84] "Liberty," Justice Kennedy wrote for the Court, "presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct."[85] A person's "right to liberty under the Due Process Clause gives them the full right to engage in their conduct without intervention of the government."[86]

I am not suggesting that Due Process protection is needed to trigger *Carpenter*. The Due Process clause deals with different history, different text, and different context than the Fourth Amendment. But *Carpenter*'s focus on records that echo Due Process concerns reflects its specific focus on limiting the government to protect the innocent.

---

[80] 429 U.S. 589 (1977)
[81] United States v. Westinghouse Elec. Corp., 638 F. 2d 570, 577 (3d Cir. 1980).
[82] Id. (quoting United States v. Grunewald, 233 F.2d 556, 581-82 (2d Cir. 1956) (Frank, J., dissenting)).
[83] 539 U.S. 558 (2003).
[84] Id. at 562.
[85] Id. at 562.
[86] Id. at 578.

Carpenter imposes Fourth Amendment limits on gathering types of records for which illegitimate uses are particularly likely. To prevent abuses, *Carpenter* enshrouds the full set of records in Fourth Amendment protection and limits access to circumstances in which the government can provide probable cause to believe the records will be evidence of crime.

The notion that *Carpenter* should be limited to records of innocent personal facts outside legitimate state interest also echoes equilibrium-adjustment. Equilibrium-adjustment tries to avoid dystopia. Too much government power is harmful because it leads to abuse. It enables the police to pursue personal vendettas, target the politically unpopular, and otherwise use investigative powers in bad faith in ways that cause great civil liberties harms. These concerns are at their apex when records are likely to contain embarrassing facts outside any legitimate state interest. The incentive to abuse unlimited access to such records is high. Limiting *Carpenter*'s scope to records that reveal an intimate portrait of a person's life focuses on the records most subject to abuse and in the greatest need of a countering adjustment.

Chapter 7:
Implementing *Carpenter*

The previous chapter pinpointed three requirements needed to trigger *Carpenter* searches. But we're not done yet. These requirements are about the general category of record that *Carpenter* covers. Some kinds of records qualify for *Carpenter* treatment and others do not. That's an important first step, but implementing *Carpenter* requires addressing another big question: How can you identify, in a particular case, whether a particular government collection of those records is a search?

This is a hard problem. Fourth Amendment law traditionally looks to when a protected place or thing has been opened, or at least when information from inside that place or thing has been retrieved. That makes identifying the search relatively easy. You just look at whether the information from inside was obtained. Divorcing Fourth Amendment law from places or things means bestowing protection on some body of data. That prompts a new question: When the law protects a body of data, when does a transfer of that data to the government trigger the Fourth Amendment? Put another way, how do you measure when privacy has been invaded?

Consider three possible tests. The first test, what I call the Subjective Approach, would focus on when the government learned the kind of private information that *Carpenter* safeguards. If courts adopt it, a search would occur the moment the government learns a private fact about a person that is among the type *Carpenter* regulates. The government's realization of the private fact triggers a search.

A second approach, what I call the Mosaic Theory, would focus instead on whether the quantity of records obtained are ordinarily sufficient to reveal the kinds of private information that animated *Carpenter*. The mosaic theory would identify general rules for how much surveillance is enough. Under this approach, a search occurs when an

information transfer to the government includes a large quantity of *Carpenter*-protected information.

The third approach, what I call the Source Rule, would ask only whether any information revealed to the government was dependent or relied on use of a technology that *Carpenter* covers. This is a bright-line rule that looks to the source of the information obtained. If the government learned any fact sourced from any *Carpenter*-covered record, then that information transfer is a search.

All three approaches are facially plausible ways to measure whether a particular information transfer should trigger *Carpenter*. But I think only the Source Rule can work. The significance of information is always contextual. A fact may be meaningless or profound based on what else is known. This reality makes the Source Rule the only way to know in advance what the law requires. Fourth Amendment rules must be clear, both so the police can follow the law and so subjects of unlawful searches can obtain legal remedies for violations. The Source Rule is not perfect, as it over-protects records to provide the needed clarity. But no approach is perfect, and the Source Rule is the best of the choices.

The last part of the chapter applies the test to a few important examples of Internet metadata that should or shouldn't trigger a search under my framework. On one hand, government collection of records concerning who a person e-mailed and texted, and what websites a person visited, should trigger a search. On the other hand, basic subscriber records, records of voice call numbers dialed, and assigned IP addresses should not be a search. These results are true to the *Carpenter* decision itself, to the theory of equilibrium-adjustment that animated it, and – as much as possible – to the need for clear rules that can guide the police.

Against the Subjective Approach

To figure out when a *Carpenter* invasion of privacy has occurred, we need to look closely at each of the three options. Let's start with the Subjective Approach. At first blush, it has intuitive appeal. If access to records counts as a search because it paints an intimate portrait of a person's life, why not say a search occurs when the portrait has been painted? Just watch what the government knows. When it learns something invasive, a search has occurred.

It sounds simple at first. But it's not. It rests on a judgment that is surprisingly difficult to predict or identify. Information is not an on/off switch. Whether an information transfer tells us a particular private fact about a person is not readily answerable in the abstract. It's not like you either know something private about someone or you don't. Instead, information is more like water. It's cumulative. It has degrees. It always depends on what else we know and how much certainty is enough to really "know" something.

Fourth Amendment doctrine can't readily rely on such a standard. Under the Subjective Approach, it would be difficult for law enforcement to identify ahead of time when an information transfer revealed a private fact that made the transfer a search. "Searches" could come and go depending on subjective judgments about what facts are known at particular times. And subjects of searches would have no way to know whether they were searched. The Subjective Approach would be too unpredictable, too vague, and too random to apply.

The best way to demonstrate these flaws is with an example. Or rather, a series of examples. I'll start with a simple example based on *Carpenter*. I'll then vary the problem by first taking away facts and then adding new ones back in. My hope is that the string of examples will show you why the Subjective Approach is too contingent to work.

Here's the hypothetical: Imagine an investigation into a criminal suspect named Bob Fitzsimmons, a suspect who has a cell phone reachable at (626) 657-0253. The government wants historical cell-site records over a one week period when Bob was a suspect in crime. Every time Bob makes or ends a phone call, his cell phone provider creates and stores a record of what cell site was used to route the call. A typical person makes about five cell phone calls a day, so let's say Bob's seven-day database contains seventy entries (the typical ten entries per day).[87] The first five entries in the database looks like this:

[87] See Amanda Lenhart, Cell Phones and American adults, Pew Research Center (2010) available at http://www.pewinternet.org/2010/09/02/cell-phones-and-american-adults/ ("The average adult cell phone owner makes and receives around 5 voice calls a day.").

Bob Fitzsimmons Cell-Site Location Records
(626) 657-0253

Time	Physical Location
June 5, 2018 3:32pm	1200 Monaco Parkway, Bakertown, CA
June 5, 2018 3:43pm	1200 Monaco Parkway, Bakertown, CA
June 5, 2018 6:19pm	67 Spruce Street, Smithville, CA
June 5, 2018 6:52pm	422 Main Street, Smithville CA
June 5, 2018 8:45pm	1200 Monaco Parkway, Bakertown, CA

Imagine the government obtains an order compelling the phone company to hand over the full set of seventy entries. *Carpenter* tells us that a search has occurred, and the Fourth Amendment requires a warrant, because obtaining the records violated Fitzsimmons's "reasonable expectation of privacy in the whole of his physical movements."[88]

Now let's tinker with the hypothetical. Assume the police don't need the entire seven-day database. They only want to know a few facts about his whereabouts at that time. To get what they need, but to avoid drawing an intimate portrait of Fitzsimmons's life, investigators might ask for less information. Let's strip down how much information the government learns and ask whether the facts still amount to a *Carpenter* search.

Let's start by making the data less precise. Call this Scenario 2. Instead of seeking a warrant for the entire database, investigators tell the phone company that they only want to know the towns where the phone was located over the seven-day period. Instead of sending the government the list of seventy entries with exact dates, times, and cell-site locations, the company responds with only this limited information:

[88] *Carpenter*, 138 S.Ct. at 2219.

Bob Fitzsimmons's Cell-Site Location, June 5th to 12th
(626) 657-0253

Physical Location of Phone
Bakertown, CA
Smithville, CA
Holderson, CA
Los Angeles, CA
Long Beach, CA

Is this still a search? On one hand, the government has learned much less than it knew before. The seventy entries have become five. The precise time and locations have been replaced with just a list of towns over a week-long window. The government probably can't reconstruct the intimate details of Fitzsimmons's life with this data. On the other hand, the government still has learned some location information using detailed tracking technology. It has learned all of the towns where the phone was located in that time. Ask yourself: In Scenario 2, has a search occurred?

Now let's consider Scenario 3. As with Scenario 2, the government only wants to know what towns the phone was in over the week. But there's one difference: This time, the government doesn't know who used the phone with number (626) 657-0253. It's a burner phone – a disposable phone with no registration information – and the government doesn't yet have a known suspect. The phone is believed to have been used in a crime, but the government doesn't know who the suspect is and may want the location records just to find out. The government gets a court order, and the cell company responds with this database:

Cell-Site Location Records
(626) 657-0253

Physical Location of Phone (June 5th to June 12th)
Bakertown, CA
Smithville, CA
Holderson, CA
Los Angeles, CA
Long Beach, CA

This is almost the same information as in Scenario 2. But this time, there is no name. Scenario 2 lost precision and detail, and Scenario 3 adds the loss of identity. Does it matter that the information is no longer linked to a particular person? *Someone* was in those towns over those five days. Do you see a Fourth Amendment search?

Let's strip down the data one more time with Scenario 4 before we start to build up the information again. Scenario 4 is like Scenario 3, but with a twist: The cops don't want to know where the phone was located. They just want to know if whoever used that phone number was in the same area as the known phone of a possible suspect, Sally McAdams, at a particular date and time when the police think a crime occurred.

In Scenario 4, the government obtains an order requiring the provider to answer a yes/no question: "On June 5th, from 3-4pm, was the phone associated with the number (626) 657-0253 within a 1-mile radius of the phone registered to Sally McAdams?" An employee of the cell-phone company complies with the order by looking through the cell-site database and responding with one word: "No."

Again, has a search occurred? On one hand, we started with the same database of seventy entries that would have been a search of Fitzsimmons, at least as long as not knowing his identity did not make the difference. And it was paired to another database, that of the entries for McAdams' phone, which, if the government knew it, would have been a Fourth Amendment search of McAdams, too.

On the other hand, now the government is seeing only a tiny slice of the information from that database. The query of the database only covers one hour of the one-week period. Only two entries were made over that hour. And all the government learns from the query is that, *wherever* that phone was, and *if* there were any database entries for that

window, it was not within a mile of another phone -- wherever *that* phone was located. Do you still see a search?

Now let's start to add new information in and see what changes. The government is conducting an investigation, and it will likely have other sources of information beyond the cell-site records. Those additional sources can give new meaning to the cell-site records collected. So here's Scenario 5. Let's go back to Scenario 3, in which the government gets a list of towns in which that phone number was recorded as having been located over the one-week period. At this point, the government doesn't know who is using the phone. But imagine that the day after getting the company's list, an investigator asks a criminal informant if he knows who uses the phone number (626) 657-0253. "Sure," the informant responds. "That's Bob's number. Bob Fitzsimmons."

Does the informant's answer make a Fourth Amendment difference? The list of towns from Scenario 3 now has a name attached to it. You don't yet know if the informant's answer is correct or useful. Maybe the name can be researched to link it to an identity and maybe it can't be. (What if the answer was only the first name and not the last?) But the new information makes that the de-identified information from Scenario 3 more meaningful. It is now potentially personalized again to become the records of Scenario 2. Has a search occurred?

One last hypothetical. Scenario 6 is the same scenario as 5, but now an investigator also goes online and googles the name "Bob Fitzsimmons." He googles the towns listed where the phone was located. The investigator learns that Bakertown, Smithville, and Holderson are small towns in rural California about an hour apart. These three towns are known for very specific things. There is nothing in Bakertown except for a church run by a non-traditional Christian denomination. Smithville is known for having three strip clubs and little else. And Holderson is famous for having a quack physician who specializes in the treatment of an embarrassing sexually-transmitted disease.

Add one more detail. The investigator's googling also reveals postings on a public Internet message board about California tourism from a "Bobby FitzS." In a string of messages posted on June 1st, "Bobby" writes that he lives in Los Angeles and works in Long Beach. He is planning a trip to rural California and wants to know of good places to stay in Jonesburg, a large town that happens to be not far from

Smithville, "to try to get right with the Lord, get some medical attention, and have some fun."

You can see where I'm going with this. The new information, found on a public message board, makes the cell-site records much more revealing in context. Records that may not be revealing in isolation start to paint a picture when combined. We can't be sure that "Bobby FitzS" is the Bob Fitzsimmons mentioned by the informant. But it seems plausible. And combining the list of towns that the phone company provided with informant's tip with the googling starts to suggest that we know what Bob Fitzsimmons was up to on the week starting June 5th. We can't be sure. But it's a decent guess that he spent some time at home, some time at work, and also went on a trip to that church, a strip club, and the doctor who treats an embarrassing sexually-transmitted disease.

The key lesson is that the invasiveness of information is contingent on what else is known. We find information invasive when it supports a conclusion about a person. At an intuitive level, the sense of invasiveness occurs when learning fact *A* implies sensitive fact *B*. But whether *A* implies *B* often depends on whether we also know *C*. *A* might seem meaningless (or damning) today but damning (or meaningless) tomorrow. It all depends what else we know. And of course what we "know" is just our current belief. That can change, too, as we reassess what we know or learn new facts and reach new conclusions. As Fourth Amendment thresholds like probable cause and reasonable suspicion suggest, investigators don't really *know* facts about suspects. They just have reasons to believe things about them to various degrees of certainty.

These problems provide good reasons not to adopt the Subjective Approach. If a search occurs when the government learns an invasive fact, then there needs to be very close attention to what the government knows over time. Courts would need standards for exactly how much information is enough to make a possible fact 'learned.' Is a hunch that turns out to be right enough? What if the government should have realized the existence of a fact but didn't? What if different officers knew different facts that could have combined to see a fact but the officers never spoke or the information was never combined? Courts would also need standards for how the Fourth Amendment applies as new information is added and the government's state of knowledge changes. Whether a search has occurred might flip between "yes" and "no" multiple times as the government's known facts change.

That standard would be too unpredictable. It's hard to know whether new fact *A* implies sensitive fact *B* until the new fact is introduced and appreciated. The government couldn't know whether obtaining a record amounted to a search until after the record was obtained. And that would give the government every incentive to deny the implications of what it learns or avoid combining knowledge, making the factual picture particularly difficult to reconstruct in litigation

The Subjective Approach might have one benefit. It could encourage investigators to get less information to avoid learning about the privacies of life. It's an admirable goal. After all, it's better for the police to avoid learning private information it has no legitimate interest in knowing that could only be abused. But the desirability of the goal cannot overcome the challenges of reaching it elaborated on above. If you can't know when private information would be learned, you can't avoid learning it. The Subjective Approach is to unpredictable, too vague, and too random too implement. It sounds good in theory, but it would be awfully difficult to implement in practice.

Against the Mosaic Theory

The next possible way to identify *Carpenter* privacy invasions is through what I have called the Mosaic Theory.[89] The idea of the mosaic theory is to treat short-term or limited records collection differently than long-term or broad records collection. Limited collection is not a search, but surveillance that goes on too long crosses a line and triggers the Fourth Amendment. Like the Subjective Approach, the Mosaic Theory sounds good in theory. But it won't work either, and for similar reasons.

Let's start with the case for the mosaic theory. If the problem identified in *Carpenter* is that digital technology allows the government to conduct large-scale surveillance easily and cheaply, the thinking runs, a search should occur only when the government actually engaged in large-scale surveillance. Short-term or narrow evidence collection that is akin to traditional surveillance should not be a search. On the other hand, long-term or broad collection that far exceeds traditional expectations crosses a line and is ruled a search. The idea is rooted in equilibrium-

[89] *See generally* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311 (2012).

adjustment: Regulate the new scope of surveillance that digital technology allows. Because broad surveillance can create a mosaic of a person's life, only the broad surveillance should trigger the Fourth Amendment.

The mosaic theory was introduced by *Jones* before *Jones*. In 2010, the federal appellate court in Washington, DC, decided the case under the name *United States v. Maynard.*[90] Under Supreme Court precedent from the 1980s, monitoring the location of a car in public was not a search.[91] But according to the DC Circuit, monitoring and analysis over 28 days was different. It was so detailed and comprehensive, and went on for so long, that it allowed the government to create a mosaic of the driver's life.[92] It provided the kind of invasive look that otherwise would be obtained from a home search.[93] As a result, the collection and analysis of GPS data over 28 days was an aggregated search. The mosaic theory was born.

At the Supreme Court, Justice Alito's concurrence in *Jones* then echoed the lower court's theory, focusing on expectations of government investigations. People expect the government to engage in short-term surveillance, Justice Alito reasoned.[94] But long-term surveillance exceeds societal expectations. Although this part of Justice Alito's *Jones* concurrence was a key basis for *Carpenter*, the majority in *Carpenter* reserved the question of whether short-term surveillance avoids a search: "It is sufficient for our purposes today," the Chief Justice wrote in a footnote, "to hold that accessing seven days of CSLI constitutes a Fourth Amendment search."[95] *Carpenter* thus leaves a big question unanswered: If the massive scale of digital surveillance justifies new Fourth

[90] 615 F.3d 544 (D.C. Cir.), aff'd sub nom. United States v. Jones, 132 S. Ct. 945 (2012).

[91] United States v. Knotts, 460 U.S. 276, 281-82 (1983).

[92] *See Maynard*, 615 F.3d at

[93] *See id.* at

[94] 132 S.Ct. 945 (2012) (Alito, J., concurring in the judgment) ("For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.").

[95] Carpenter, 138 S.Ct at 2217 n.3 ("We need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.")

Amendment regulation, is it only digital surveillance on a massive scale that counts?

In my view, the Supreme Court should reject the mosaic theory as a way of identifying *Carpenter* privacy invasions. The idea is well-meaning. It is rooted, properly, in equilibrium-adjustment. But the mosaic theory creates more headaches than it solves. If data is protected sometimes, someone has to answer *when*.

Trying to answer the question tends to refute the theory. Once you say that the search inquiry depends on how evidence is aggregated and analyzed, you need to draw lines about what kind of aggregation and analysis counts. Filling in the blanks to create the bright-line rules that the Fourth Amendment demands would require courts to draw sharp and arbitrary lines that seem embarrassingly legislative. And even if courts tried, the effort would likely flop. By the time the rules would be announced, technological change would likely have made the rules obsolete.[96]

Consider the difficult and novel questions a court would have to answer under the mosaic theory. Most obviously, how long is long enough? How much information is enough? Is it a day? Or a week? Does it vary for different kinds of records?

And this is only the beginning. Can the government collect just under the constitutional line to avoid a search occurring, and then come back the next day and do it again? Or is there some sort of anti-circumvention principle that keeps the police from repeated sub-mosaic data access without triggering the Fourth Amendment? Imagine a search happens when records span five days. Investigators obtain records for 4 days and 23 hours – not a search. Five days later, the investigators get records for the next 4 days and 23 hours – again, not a search. Or should the two searches be grouped together, amounting to almost ten days, which *is* a search? What is the line for when orders need to be grouped versus treated separately?

Another puzzle is how to deal with partial records. If a record is created once a day that measures something occurring that minute, does getting five records over five days count as five minutes of surveillance or five days of surveillance? What if the device was turned off for four of the five days: Does collecting the one day of records count as one day or five

---

[96] I develop the argument in this section in much greater detail in my article, The Mosaic Theory of the Fourth Amendment, 111 Mich. L. Rev. 311 (2012).

days? That problem came up in *Carpenter*, where one of the orders was for seven days of cell-site records but the provider only retained data for two of the seven days. If there is a five-day time cut off, does obtaining two days of records in response to a seven-day production order suffice?

I can hear the response: Judges are in the business of making judgment calls. Judges are smart people, and they can draw these lines if they must. But the mosaic theory is unique because it forces courts to draw lines across multiple dimensions to figure out how much is too much. Courts would have to distinguish differences of degree rather than differences in kind. They would have to do so repeatedly, in case after case, to answer how endless variations change the formula. They have to make judgments about time, about numbers of events, and about how much the combination of time and numbers leads to a feeling that a line has been crossed. The enterprise would force courts to act more like legislators and number-crunchers than judges.

And even if they tried, it's hard to see them succeeding. The mosaic theory weighs the present invasiveness of new technologies. But technological change makes any judgment about invasiveness inherently time-bound. The technologies themselves change. A GPS device of 2005 is very different from a GPS device of 2015 and may be even more different from a GPS device of 2025. And the perceived invasiveness of a technology can change, too. In 1970, a tool that revealed the incoming phone number of a phone call might have been seen as a serious invasion of privacy; today it just a built in feature of all phones. By the time the Supreme Court settled the precise rules for how to apply the mosaic theory to a particular technology, the rules would likely be long out of date.

From a broad perspective, the problem with the Mosaic Theory resembles the problem with the Subjective Approach. Both approaches aim to identify on a case-by-case basis when the privacies of life are invaded. The Subjective Approach looks back, asking whether a past information transfer invaded the privacies of life. The Mosaic Theory looks forward, asking whether a future information transfer is likely to do so. Both methods try to pinpoint when an information transfer has caused a shift in government knowledge. But that is very hard to do, as the effects of technology on understanding are difficult to predict and implement as constitutional rules. The exercise ends up requiring arbitrary and likely-endless line-drawing.

Although *Carpenter* leaves the future of the mosaic theory open, the Court's 2014 opinion in *Riley v. California* teed up the proper grounds for its demise.[97] As explained in Chapter 4, *Riley* rejected the traditional rule that the cops can search all the property on a person at the time of their arrest. Searches of cell phones are different, the Court reasoned, as they are more invasive than physical searches.[98] The Court ended up adopting a bright line rule: Searches of cell phones require a warrant, even when found during an arrest. But before adopting a bright-line warrant rule, the Court considered and rejected an "analogue" test. Under the proposed analogue test, a search of a cell phone would have been permitted without a warrant incident to arrest as long as the government only obtained the same information as could have been obtained by a search of a "pre-digital counterpart" to a cell phone.[99]

The Court disagreed. Among other problems, "[a]n analogue test would launch courts on a difficult line-drawing expedition to determine which digital files are comparable to physical records."[100] The questions were obvious: "Is an e-mail equivalent to a letter? Is a voicemail equivalent to a phone message slip?"[101] Such a test offered no certainty: "It is not clear how officers could make these kinds of decisions before conducting a search, or how courts would apply the proposed rule after the fact."[102] The analogue test "would keep defendants and judges guessing for years to come."[103]

The same is true of the Mosaic Theory. It offers no clarity about how much surveillance is enough to trigger a search. The police need to know the rules to follow them, and they can't know them and can't follow them under the mosaic approach. The Court should reject the mosaic theory for the same reason it rejected the analogue test in *Riley*.

---

[97] 134 S.Ct. 2473 (2014).
[98] *See id.* at [].
[99] Id. at 2493.
[100] Id. at 2493.
[101] Id. at 2493.
[102] Id. at 2493.
[103] Id. at 2493.

That brings us finally to the Source Rule as a way to measure invasions of privacy for *Carpenter* searches. Under the Source Rule, government access to any information that owes its source to *Carpenter*-protected information is a search. The issue would be whether the government obtained compelled access to data that reveals any part of information covered by *Carpenter*. In the case of cell-site records, for example, access to any time period of a person's cell-site records would be a search. Learning if the phone was in the state of California on a particular date would be a search. Learning if a phone was in the same city as another phone at some point in the last year would be a search. Because all of these records derive from data that is covered by *Carpenter*, each individual piece is fully protected.

In my view, the Source Rule is the best approach to measure whether a *Carpenter* invasion of privacy has occurred. Assuming that the other conditions of *Carpenter* have been satisfied – that the government used a digital technology to obtain information that was unavailable before the digital age and that can reveal the privacies of life – then all of that information should receive protection. As long as the information reveals some fact about that person's records derived from the regulated technology, the revealing of information should count as a search. One datum is just as protected as the entire database. It's all protected.

The core reason to adopt the Source Rule is its clarity. The Source Rule avoids impossible line-drawing exercises over whether any particular information transfer is sufficient. Implementing *Carpenter* is hard enough already. After wading through the judgement calls of whether *Carpenter* should apply to the general kind of record at issue, it is simply too hard to add an additional case-by-case test for the privacy impact of any particular data transfer involving those records.

The only way out of the maddening complexities of the Subjective Approach and the Mosaic Theory is a prophylactic rule that would treat drawing from any protected records as a search. As in *Riley*, once you identify a digital technology that is vastly different from an earlier analog technology in what information it provides the government – and once you identify the capacity of that technology to provide an intimate picture of a person's life – you need a clear line that tells the police what the rules are.

In effect, the clarity of the Source Rule acts as a substitute for the traditional Fourth Amendment reliance on places and things. Under the traditional Fourth Amendment, any information from inside a Fourth Amendment place is protected. As *Arizona v. Hicks* put it, "[a] search is a search, even if it happens to disclose nothing but the bottom of a turntable."[104] That's a type of source rule, too. All information sourced from inside a protected place or thing is a search.

The Source Rule here operates as a similar bright line. It ensures that the difficult line-drawing exercises needed to implement *Carpenter* only require decisions for each type of record generally rather than for each information transfer individually. If the government enters a house, the reliance on protected places and things means you don't need a theory for what kinds of information in the house is protected. The Source Rule is similar. After you conclude that a type of record triggers *Carpenter*, the hard work is done.

There may be occasional hard questions even under a Source Rule, but they are rare. Consider the problem of records that are aggregated over multiple people. For example, a company with twenty employees could combine data drawn from the cell-site records of all of its employees. In such a case, it may be difficult to tell if a particular record can reveal anything about a particular person.

But that challenge seems modest. It can be addressed by the usual burden of proof in Fourth Amendment law. The defendant always has the burden of showing that he was the subject of a search.[105] When the government compels the production of aggregated or otherwise anonymized data, the defendant would just have the usual burden of showing that the record revealed any fact about him based on a *Carpenter*-regulated source.

The Source Rule isn't perfect. It has the major flaw of being over-inclusive. In some cases, government access to information will be a search in the digital context when accessing analogous information would not be a search in the analog context. This may seem jarring to some. But it's the least bad among the imperfect options. *Carpenter* requires equilibrium-adjustment for digital versions of analog surveillance. Once you take that step, you need either to treat equivalent information differently for digital and pre-digital facts or else find some

[104] 480 U.S. 321, 325 (1987).
[105] *See generally* Rakas v. Illinois, 439 U.S. 128, 130 n.1 (1978).

test that draws tricky lines for when the digital becomes sufficiently different that it triggers the new regime.

The Source Rule's being over-inclusive is a necessary price to pay to implement *Carpenter* in a predictable and manageable way. It allows courts to implement *Carpenter* by analyzing whether classes of records should be covered without evaluating whether individual information transfers should be covered.[106] This should reduce the morass of complex questions raised by *Carpenter* into something more manageable. Nothing here is easy. But the Source Rule brings the challenge of implementing *Carpenter* from seemingly-impossible to just really-hard. For all these reasons, courts should adopt the Source Rule and treat all information from *Carpenter*-covered sources equally.

My approach bears some resemblance to a proposal by Professors Danielle Citron and David Gray authored in the wake of *United States v. Jone*s called *The Right to Quantitative Privacy*.[107] Looking for a way to implement the then-new *Jones* concurrences, later adopted into law in *Carpenter* six years later, Citron and Gray argued that the clearest way to implement the *Jones* concurrences is through a "technology-centered approach."[108] Whether a search occurred, they argue, should depend on the technological capacity of the surveillance tool rather than how it was used in a particular case. The issue should be decided "as a general matter for that technology rather than on a case-by-case basis."[109]

Important differences exist between my approach and that of Citron and Gray. They wrote before *Carpenter* adopted and refined the *Jones* concurrences, and their test for what should trigger the *Carpenter*/*Jones* shift is different from mine. Despite these differences, we share the same view about how best to measure privacy invasion: The most administrable way to implement a test that treats digital surveillance as a search when analogous pre-digital surveillance is not a search is to treat the fruits of digital surveillance as categorically different. The test should rest on categories of surveillance rather than the impact of scope of particular information transfers.

---

[106] At least assuming the records have not been aggregated in a way that makes the but-for relationship between the person's data and the record difficult to determine.

[107] 98 Minn. L. Rev. 62 (2013).

[108] *See id.* at 126.

[109] *Id.* at 127.

Application to Messaging Services

It's time to apply the test. I'll start with how *Carpenter* should apply to Internet messaging services. One of the primary functions of the Internet is to facilitate messages. Think of e-mails, text messages, and Facebook messages. These are just some of the many examples of how we use the Internet to send and receive written communications. How should the Fourth Amendment apply?

The traditional Fourth Amendment rule is that contents of communications are protected but non-content metadata is not. As Chapter 5 showed, contents are the digital equivalent of inside surveillance that is protected inside a person's house or effects. Non-content metadata traditionally is not protected for the postal network and the telephone network. This is the network equivalent of physical observation, and it has been treated as unprotected under the Fourth Amendment just like physical observation has been treated as unprotected.

In my view, *Carpenter* requires a different rule for transaction metadata of Internet messages. The to/from information about using Internet messaging services – information such as what account you have e-mailed or when you sent a text – should be protected. When the government gets transactional records that reveal details of how a messaging service was used, that should ordinarily trigger a search that requires a warrant under *Carpenter*.

Let's run through the test to see why. First, Internet messaging metadata is a category of information not readily acquired in a pre-digital age. Of course, the government had pre-digital powers to identify to/from information of communications technologies. Under *Smith v. Maryland*, the government could obtain pen register records to find out the number that a particular account called.[110] Under *Ex Parte Jackson*, the government could observe the outside of postal mail.[111] And these forms of surveillance are the network equivalent of outside surveillance: The government could traditionally watch suspects in public.[112]

But taking *Carpenter* seriously, the government's power to conduct Internet surveillance of communications messaging metadata is

110

111

112

measurably different and should trigger constitutional protection. Internet messaging metadata is different because the Internet facilitates and stores communications on a scale never before seen. We use Internet messaging services far more than we ever made phone calls or sent letters. A typical person makes about five phone calls a day,[113] and they may receive a few pieces of personal mail on a daily basis. But messaging is orders of magnitude different from phone calls or postal mail.

Consider some numbers. In 2013, American adults from the ages of 18 to 24 sent and received an average of 128 text messages every day.[114] For today's teenagers, texting is like speaking. They do it constantly, back and forth, with all of their friends. E-mail accounts raise similar dynamics. People don't e-mail as often or instinctively as they text. But they usually keep the e-mails they send and receive. And that means their e-mail accounts can be a complete record over years. A 2012 study found that a typical Gmail account used by a person as their personal account contains 17,000 messages.[115] Because the Internet enables the transmission and storage of communications on a very different scale, access to the metadata of Internet messaging serves gives the government access to far more records than the pre-digital version.

Second, these records are created without meaningful voluntary choice in the *Carpenter* sense. Texting, e-mail, Facebook messages, and other Internet messaging services have become "indispensable to participation in modern society."[116] If participating in modern society includes having a cell phone, then it also includes communicating with others using messaging services. These days, if you meet someone new, you don't ask if they have a way to communicate by Internet message. You ask which ones they use, or you pick the age-appropriate service and know with confidence that they're in the circle of users, too. In modern life, it's how people communicate.

Finally, access to a record of who a person messaged – and who messaged them – tends to reveal an intimate portrait of a person's life that

[113] See Amanda Lenhart, Cell Phones and American adults, Pew Research Center (2010) available at http://www.pewinternet.org/2010/09/02/cell-phones-and-american-adults/ ("The average adult cell phone owner makes and receives around 5 voice calls a day.").

[114] https://www.textrequest.com/blog/how-many-texts-people-send-per-day/

[115] Mike Barton, How Much Is Your Gmail Account Worth?, WIRED (July 25, 2012), http://www.wired.com/insights/2012/07/gmail-account-worth.

[116] Carpenter, 138 S.Ct at 2220.

triggers *Carpenter*'s concerns. Knowing who a person texted and when shows their lifestyles. It details their relationships. Knowing who a person e-mailed reveals not only what organizations a person might be in communication with, but exactly who the person is on the other end of the message. This kind of transactional information would allow the government to gather a comprehensive picture of the person's associations and contacts akin to knowing their precise location. Under the source rule, the entirety of this Internet transactional metadata should be protected by the Fourth Amendment.

Application to Voice Calls

I think a different rule should apply to voice calls. Numbers dialed for phone calls should continue to be unprotected under *Smith v. Maryland*. In my view, voice call metadata should not trigger *Carpenter* because it fails the first test: The digital age has not substantially changed their nature. These records are the same traditional pre-digital records that the government traditionally has been permitted to access without constitutional limit. That should continue. *Carpenter* focuses on the new powers of the digital age. These records are not among them.

Some will find my distinction jarring. These days, what we think of as "phone calls" are simply Internet services that provide real time voice communications services. Even phone calls we make from landline phone calls and cell phones are really Internet communications that just seem like old-fashioned calls. And services like Skype and Facetime take the old-fashioned telephone functionality, add video, and otherwise work like any other Internet service. It might seem rather artificial to treat the metadata for these services differently than for text messages and e-mails. Given that they're all ways of sending communications over the Internet, shouldn't we treat them the same way?

I think the answer is that we should not. That's my answer because, to borrow from Holmes, the life of *Carpenter* is not logic but experience.[117] *Carpenter* requires distinguishing between old surveillance powers and new ones. The government's ability to obtain metadata of real-time voice communications – to/from and time information between two accounts over which a voice conversation in real time is held -- is

[117] Cf. Oliver Wendell Holmes, The Common Law 1 (1881) ("The life of the law has not been logic; it has been experience.")

conventional and longstanding. We use the phone today just like we used the phone in 1980. We make just a few phone calls a day, and knowing a call was made sheds little light on its content. The contents of phone calls themselves should be protected, of course. But the fact that someone from one account called another is a traditional non-search that should remain one.

The key distinction is social practice and storage. Text messages are like speaking and e-mails are stored forever, while calls are just calls. Collecting metadata for Internet text communications now gives the government transformative power; collecting metadata for Internet voice calls does not. Put another way, the Internet does not transform the nature of all metadata. It only transforms the nature of some metadata while leaving other metadata largely untouched. If this distinction seems like an odd line to draw, at least it is an odd line that is true to the animating principles of *Carpenter*.

Application to Websurfing

The next application to consider is how *Carpenter* should apply to government monitoring of websurfing. There are two issues to consider. First, if the government wants to monitor what websites a user is visiting, should the monitoring of websites visited be a search? Second, if the government wants to know what IP address a person is using while surfing the web should obtaining that record be a search? I think the answer should be "yes" for the first question and "no" for the second: Monitoring websites visited is a search but monitoring IP addresses assigned while doing so is not.

Let's apply the three-part test, starting with websites visited. First, records of websurfing habits are a new kind of record in the digital age. In the past, the police could always tail a suspect in person. But websurfing is new, as is the ability to track it. In the digital age, we think and therefore we Google. It's only a slight exaggeration to say that every thought turns into a website visit. We feel we are not being watched, so we feel free to explore the web based limited only by our imaginations. According to a 2015 study, the typical American spends over 2 hours a day online.[118] Much of that time is spent surfing the web. The

[118] https://www.quora.com/For-how-many-hours-per-day-does-the-average-US-Internet-subscriber-use-the-Internet

government's ability to track the websites a person visits through network surveillance is a new kind of power of the digital age.

The remaining two tests reach the same result. Websurfing is such a central part of using the Internet that it should be considered essential to participating in modern life just like sending written messages. Finally, obtaining websurfing records invades the privacies of life. If you can track what websites a person visits, you can reconstruct the kind of intimate picture of a person's life in far greater detail than merely knowing their physical location as in *Carpenter*. Websurfing records are a gold mine of the kind of intimate information such as personal interests, sexual preferences, and political beliefs that expose the privacies of life.

Courts should reach a different result when the government merely seeks to know the Internet Protocol (IP) address that a person was using when connected to the Internet. An IP address is like the Internet equivalent of a phone number. Whenever a person is connected to the Internet, he must have an IP address so data can be routed to him. IP addresses can change for a range of reasons, making the IP address that a particular person was using very useful to link network information to a person.

In my view, however, IP addresses that a person was assigned should not trigger *Carpenter*. A person's IP assigned address is the Internet network equivalent the person's home address or phone number. Knowing a person's IP address might reveal roughly where they are located or what company they are using to access the Internet. But that is the equivalent of knowing a person's phone number and being able to trace that to a person's home or business. It's a traditional kind of record that the Internet has not substantially changed.

Once again, there is a potentially odd consequence of my approach: It treats two forms of IP address surveillance differently. When the government wants to monitor the websites that a suspect is visiting, it might get that information by collecting the IP addresses of Internet traffic from that computer or account that is on the port associated with website traffic. That would typically reveal the domain name a person visited but not the particular webpage that was shown at that domain name. Under my approach, then, obtaining IP addresses that a person is visiting could be a search while obtaining the IP address that a person was assigned would not be.

But I think that is a sensible distinction. A person's assigned IP address does not reveal much about them. It changes over time, but in

ways that generally don't give a detailed picture of their lives. The IP addresses that a person visits while surfing the web is different. It creates an intimate portrait of what a person was doing and what they were thinking at particular times. As a result, monitoring the websites that an account was visiting should trigger *Carpenter*; monitoring the IP addresses that a person was assigned should not.

Application to Ride-Sharing Records

Another interesting application to consider is third-party records generated by services. Focus on just one example: Records of trips created using ride-sharing "apps" such as Uber and Lyft. It is common today to rely on such services to hail a car to travel from point A to point B. The services use the GPS and other locational information on our phones to link us with drivers. Taking a trip creates a record, retained by the provider and also available to us through our accounts, of exactly what we did. The record includes precisely when and where we were picked up, precisely what road we traveled, and precisely where and when we were dropped off. Here's the question: If the government wants a person's record of our trips, does that require a warrant?

I think the answer should be "no." Ride-sharing records fail at least one of the three tests, and maybe all three. First, ride-sharing trip records are not a new kind of record unique to the digital age. The digital age has made it easier to connect riders with drivers. But the basic kind of record -- where a person was picked up, what path a person took, and where they were dropped off – is not new. Taxicab drivers in the past routinely kept records of their pick-ups and drop-offs for billing and accounting purposes.

It's true that ride-sharing records can provide some new information. They can relay with precision that a driver may not recall about exactly what road was taken. But that extra information is not transformative. While origins and destinations can be revealing, the particular road that the driver took to get there is usually just whatever road the driver's GPS app recommended.

Although I need not reach it, ride-sharing apps also may fail the remaining two tests. Calling an Uber or a Lyft is a voluntary act that a person chooses to take. Travel is essential to participating in modern life, but there are many ways to travel without creating ride-sharing records. You can take a taxi. You can ride the bus. You can drive your own car,

if you have one. Finally, ride-sharing records do not typically reveal the privacies of life. Permanent physical tracking reveals those privacies, *Carpenter* tells us, because it is pervasive. But ride-sharing records are merely occasional records of where we went, not continuous records of where we are.

The Law of Downstream Analysis

I want to end by recognizing an important corollary to my approach to *Carpenter*: Mere analysis cannot trigger a search. If the government collects records that are not protected, the Fourth Amendment does not regulate combining and querying databases of those records. As long as the inputs were not sourced from records that satisfy the three *Carpenter* requirements, downstream analysis cannot trigger a search in the output.

This corollary follows directly from the Source Rule. Analysis of data that is not sourced from records that satisfy the test cannot satisfy the Source Rule. If no protected records enter the database, the output of queries cannot be sourced from protected records. The government can create a database that contains a person's phone call metadata, assigned IP addresses, ride-sharing records, and any other unprotected information and can mine and analyze it endlessly without triggering a search.

This does not mean that downstream analysis is irrelevant to *Carpenter*. It should play an important role. When deciding whether *Carpenter* protects a type of record, the privacy implications of combining the record with other records and analyzing them together is relevant. In particular, whether a record tends to reveal the privacies of life should be analyzed in light of the realistic prospects that the data can be combined with other data.[119] The prospect of what can be revealed when a record is combined with other unprotected records may determine if one or both of the records is something *Carpenter* protects. Once a type of record is declared unprotected, the Fourth Amendment drops out. But downstream analysis is relevant to whether a particular record is a *Carpenter*-protected source.

---

[119] *Cf. Carpenter*, 138 S. Ct at 2218 ("[T]he Court has already rejected the proposition that inference insulates a search.") (quoting in part Kyllo, 533 U.S., at 36).

This approach can help solve the grouping problem that can arise when classifying records. Imagine a company keeps two kinds of records. Imagine that each kind of record, considered in isolation, fails some aspect of the three-part test (say, the privacies-of-life test). Also imagine that if the government can collect both records and analyze them together, combining the records might collectively yield information that on the whole satisfies the three-part test. This creates a puzzle for how to group records. Should courts treat the records separately, as unprotected records that can later be combined as mere downstream analysis? Or should courts treat the records together, viewing the prospect of downstream analysis as influencing how the three-part test may apply?

There may be no universal answer to that question. Under my approach, however, a court could treat the prospect of combining the two kinds of records downstream as a reason to view one or both of the records as protected. In that case, any information from one or either of the data sources would trigger *Carpenter* under the Source Rule. This doesn't answer everything, of course. Grouping two records from the same company may seem more plausible than grouping unrelated records from two different sources. But the analytic method addresses at least some of the important cases, and it frames the right questions for others.

United States Court of Appeals for the Ninth Circuit

Office of the Clerk
95 Seventh Street
San Francisco, CA 94103

Information Regarding Judgment and Post-Judgment Proceedings

Judgment

- This Court has filed and entered the attached judgment in your case. Fed. R. App. P. 36. Please note the filed date on the attached decision because all of the dates described below run from that date, not from the date you receive this notice.

Mandate (Fed. R. App. P. 41; 9th Cir. R. 41-1 & -2)

- The mandate will issue 7 days after the expiration of the time for filing a petition for rehearing or 7 days from the denial of a petition for rehearing, unless the Court directs otherwise. To file a motion to stay the mandate, file it electronically via the appellate ECF system or, if you are a pro se litigant or an attorney with an exemption from using appellate ECF, file one original motion on paper.

Petition for Panel Rehearing (Fed. R. App. P. 40; 9th Cir. R. 40-1)
Petition for Rehearing En Banc (Fed. R. App. P. 35; 9th Cir. R. 35-1 to -3)

(1) A. Purpose (Panel Rehearing):

- A party should seek panel rehearing only if one or more of the following grounds exist:
  - ► A material point of fact or law was overlooked in the decision;
  - ► A change in the law occurred after the case was submitted which appears to have been overlooked by the panel; or
  - ► An apparent conflict with another decision of the Court was not addressed in the opinion.
- Do not file a petition for panel rehearing merely to reargue the case.

B. Purpose (Rehearing En Banc)

- A party should seek en banc rehearing only if one or more of the following grounds exist:

- ► Consideration by the full Court is necessary to secure or maintain uniformity of the Court's decisions; or
- ► The proceeding involves a question of exceptional importance; or
- ► The opinion directly conflicts with an existing opinion by another court of appeals or the Supreme Court and substantially affects a rule of national application in which there is an overriding need for national uniformity.

(2) Deadlines for Filing:

- A petition for rehearing may be filed within 14 days after entry of judgment. Fed. R. App. P. 40(a)(1).
- If the United States or an agency or officer thereof is a party in a civil case, the time for filing a petition for rehearing is 45 days after entry of judgment. Fed. R. App. P. 40(a)(1).
- If the mandate has issued, the petition for rehearing should be accompanied by a motion to recall the mandate.
- *See* Advisory Note to 9th Cir. R. 40-1 (petitions must be received on the due date).
- An order to publish a previously unpublished memorandum disposition extends the time to file a petition for rehearing to 14 days after the date of the order of publication or, in all civil cases in which the United States or an agency or officer thereof is a party, 45 days after the date of the order of publication. 9th Cir. R. 40-2.

(3) Statement of Counsel

- A petition should contain an introduction stating that, in counsel's judgment, one or more of the situations described in the "purpose" section above exist. The points to be raised must be stated clearly.

(4) Form & Number of Copies (9th Cir. R. 40-1; Fed. R. App. P. 32(c)(2))

- The petition shall not exceed 15 pages unless it complies with the alternative length limitations of 4,200 words or 390 lines of text.
- The petition must be accompanied by a copy of the panel's decision being challenged.
- A response, when ordered by the Court, shall comply with the same length limitations as the petition.
- If a pro se litigant elects to file a form brief pursuant to Circuit Rule 28-1, a petition for panel rehearing or for rehearing en banc need not comply with Fed. R. App. P. 32.

- The petition or response must be accompanied by a Certificate of Compliance found at Form 11, available on our website at www.ca9.uscourts.gov under *Forms.*
- You may file a petition electronically via the appellate ECF system. No paper copies are required unless the Court orders otherwise. If you are a pro se litigant or an attorney exempted from using the appellate ECF system, file one original petition on paper. No additional paper copies are required unless the Court orders otherwise.

Bill of Costs (Fed. R. App. P. 39, 9th Cir. R. 39-1)

- The Bill of Costs must be filed within 14 days after entry of judgment.
- See Form 10 for additional information, available on our website at www.ca9.uscourts.gov under *Forms.*

Attorneys Fees

- Ninth Circuit Rule 39-1 describes the content and due dates for attorneys fees applications.
- All relevant forms are available on our website at www.ca9.uscourts.gov under *Forms* or by telephoning (415) 355-7806.

Petition for a Writ of Certiorari

- Please refer to the Rules of the United States Supreme Court at www.supremecourt.gov

Counsel Listing in Published Opinions

- Please check counsel listing on the attached decision.
- If there are any errors in a published opinion, please send an email or letter **in writing within 10 days** to:
  - ► Thomson Reuters; 610 Opperman Drive; PO Box 64526; Eagan, MN 55123 (Attn: Maria Evangelista (maria.b.evangelista@tr.com));
  - ► and electronically file a copy of the letter via the appellate ECF system by using "File Correspondence to Court," or if you are an attorney exempted from using the appellate ECF system, mail the Court one copy of the letter.

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 10. Bill of Costs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form10instructions.pdf

9th Cir. Case Number(s)

Case Name

The Clerk is requested to award costs to *(party name(s))*:

I swear under penalty of perjury that the copies for which costs are requested were actually and necessarily produced, and that the requested costs were actually expended.

Signature **Date**

*(use "*s/[typed name]*" to sign electronically-filed documents)*

COST TAXABLE	**REQUESTED** *(each column must be completed)*			
DOCUMENTS / FEE PAID	No. of Copies	Pages per Copy	Cost per Page	TOTAL COST
Excerpts of Record*			$	$
Principal Brief(s) *(Opening Brief; Answering Brief; 1st, 2nd , and/or 3rd Brief on Cross-Appeal; Intervenor Brief)*			$	$
Reply Brief / Cross-Appeal Reply Brief			$	$
Supplemental Brief(s)			$	$
Petition for Review Docket Fee / Petition for Writ of Mandamus Docket Fee / Appeal from Bankruptcy Appellate Panel Docket Fee				$
			TOTAL:	$

***Example:** Calculate 4 copies of 3 volumes of excerpts of record that total 500 pages [Vol. 1 (10 pgs.) + Vol. 2 (250 pgs.) + Vol. 3 (240 pgs.)] as:*
No. of Copies: 4; Pages per Copy: 500; Cost per Page: $.10 (or actual cost IF less than $.10);
TOTAL: 4 x 500 x $.10 = $200.

Feedback or questions about this form? Email us at forms@ca9.uscourts.gov