THE YALE LAW JOURNAL FORUM
APRIL 1, 2019

Fourth Amendment Reasonableness After *Carpenter*

Alan Z. Rozenshtein

ABSTRACT. In *Carpenter v. United States*, the Supreme Court held not only that the Fourth Amendment applies when the government collects certain categories of third-party data, but also that for such collection no process short of a warrant is constitutional. This Essay argues that a categorical warrant requirement for electronic surveillance is a mistake, and that, when faced with warrantless electronic surveillance, courts should consider whether such surveillance is nevertheless reasonableness, especially where it is legislatively authorized and subject to judicial oversight.

INTRODUCTION

Carpenter v. United States[1] is one of this generation's most important Fourth Amendment opinions.[2] Commentators have highlighted—and overwhelmingly praised—the opinion's limitation of the third-party doctrine.[3] But just as important as the decision's effect on the *scope* of the Fourth Amendment—under what circumstances the amendment applies—is its impact on the amendment's

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

2. *See, e.g.*, ORIN S. KERR, *Implementing* Carpenter, *in* THE DIGITAL FOURTH AMENDMENT (forthcoming) (manuscript at 1), https://papers.ssrn.com/abstract_id=3301257; Susan Freiwald & Stephen Wm. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 206 (2018); Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. (forthcoming 2019), https://osf.io/preprints/lawarxiv/bsedj [https://perma.cc/2EFF-UGJ3].

3. *See, e.g.*, Lindsey Barrett, *Model(ing) Privacy: Empirical Approaches to Privacy Law & Governance*, 35 SANTA CLARA HIGH TECH. L.J. 1, 7 (2018) ("*Carpenter* provided a rare glimmer of hope for those who wish to see a Fourth Amendment that fully grapples with the breadth and depth of technological change . . . ."); Danielle Keats Citron, *A Poor Mother's Right to Privacy: A Review*, 98 B.U. L. REV. 1139, 1163 (2018); Elizabeth De Armond, *Tactful Inattention: Erving Goffman, Privacy in the Digital Age, and the Virtue of Averting One's Eyes*, 92 ST. JOHN'S L. REV. 283, 294-96 (2018).

content. The Supreme Court didn't just hold that government acquisition of cell-site location information is subject to the Fourth Amendment. It also held that, even if congressionally authorized, any process short of obtaining a warrant—and thus any level of suspicion less than probable cause—would be unconstitutional. This Essay argues that *Carpenter*'s embrace of a categorical warrant requirement was a mistake,[4] and that the Court missed the opportunity (one it will inevitably have to take up in the future) to decide when legislatively authorized warrantless electronic surveillance is reasonable.

I. *CARPENTER* AND THE STORED COMMUNICATION ACT

Unlike many Fourth Amendment cases, *Carpenter* is not about a generic police practice, but rather a specific law: the Stored Communications Act (SCA).[5] The heart of the SCA is 18 U.S.C. § 2703, which sets out the procedures law enforcement must follow when it compels third parties to disclose user data.[6] Congress passed the SCA against a background assumption that electronic data held by third parties was not covered by the Fourth Amendment because of the third-party doctrine, which provides that government acquisition of a person's data (especially noncontent data) from a third party is generally outside the scope of the Fourth Amendment.[7] Thus, although the SCA is often framed as a grant of power to law enforcement, its main impetus was the opposite: Congress was chiefly concerned about digital privacy, and thus went to great lengths to specify workable, privacy-protecting rules governing law enforcement's ability to access certain categories of digital information.[8]

---

4. The term "warrant requirement" can refer to two different things: (1) the requirements, like particularity and probable cause, for issuing a valid warrant; and (2) the requirement that the government obtain a warrant before conducting a search. I use "warrant requirement" in the second sense.

5. 18 U.S.C. §§ 2701-12 (2018). The SCA was passed as Title II of the Electronic Communications Privacy Act of 1986. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.). For an overview of the SCA, see generally Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004).

6. 18 U.S.C. § 2703 (2018).

7. Specifically, the third-party doctrine holds that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," and therefore government acquisition of such information is not a search under (and thus is not regulated by) the Fourth Amendment. Smith v. Maryland, 442 U.S. 735, 742-44 (1979). The doctrine has operated as a key impediment to Fourth Amendment protection for digital data, much of which is generated and held by private businesses for their own business purposes. *See* DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 102-10 (2011).

8. *See* 14 S. REP. NO. 99-541, at 1 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3358 (noting that the SCA was passed "to update and clarify Federal privacy protections and standards in

The SCA provides different levels of protection depending on how sensitive Congress deemed certain categories of information. For example, the SCA requires law enforcement to secure a warrant (and thus establish probable cause) before acquiring the contents of certain categories of emails.[9] On the other end of the spectrum, Congress viewed user names, addresses, and billing information as relatively nonsensitive and thus the SCA lets law enforcement acquire such information with a mere subpoena.[10]

Section 2703's main innovation is to recognize a category of information between these two poles—information that is not so sensitive as to require a warrant, but sensitive enough that the government must do more than merely issue a subpoena for its production. Specifically, sections 2703(c) and 2703(d) provide that the government may acquire a noncontent "record or other information" about a user if it gets a court order (known as a "D order") based on "specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought[] are relevant and material to an ongoing criminal investigation."[11]

In *Carpenter*, the government had used an otherwise-valid D order to obtain Timothy Carpenter's cell-site location information (CSLI) from his cell-phone provider.[12] To ensure consistent service, cell phones continuously connect to nearby cell towers, and cell phone providers record this CSLI for their own business purposes.[13] CSLI can provide fairly detailed information on where a particular cell phone—and by inference its owner—has been, and is therefore very useful to law enforcement for criminal investigations. In Carpenter's case, the government obtained two orders, which together provided over a hundred

light of dramatic changes in new computer and telecommunications technologies"); *see also* Christopher J. Borchert et al., *Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act*, 13 DUKE L. & TECH. REV. 36, 40-41 (2015).

9. *See* 18 U.S.C. § 2703(a). For historical reasons, the SCA provides different levels of protection to emails depending on how long they have been in storage, *see* Kerr, *supra* note 5 at 30-32. Nevertheless, the latest caselaw suggests that the Fourth Amendment requires warrants for the compelled disclosure of email contents, *see* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010), and thus the SCA's distinction between emails based on their age is a dead letter, *see* 2 WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 4.4(c) (4th ed. 2018).

10. *Id.* § 2703(c)(2). The standard for subpoenas is very low. For example, grand jury subpoenas for the production of documents—formally issued by grand juries but in practice controlled entirely by prosecutors—are generally valid as long as they are neither "unreasonable [n]or oppressive." FED. R. CRIM. P. 17(c)(2); *see also* 3 LAFAVE ET AL., *supra* note 9, § 8.7(a).

11. 18 U.S.C. § 2703(d). The "specific and articulable facts" standard derives from *Terry v. Ohio*, 392 U.S. 1, 21 (1968). *See* United States v. Perrine, 518 F.3d 1196, 1202 (10th Cir. 2008).

12. 138 S. Ct. 2206, 2212 (2018).

13. *Id.* at 2211-12.

location points a day for more than a hundred days.[14] The government used this information to place Carpenter at the scene of a number of armed robberies, for which he was convicted and sentenced to over one hundred years in prison.

Carpenter challenged his conviction on the grounds that it was unconstitutional for the government to use a D order — rather than a warrant — to acquire his CSLI. The Court of Appeals affirmed Carpenter's conviction, relying (as had the other circuits that had considered the issue) on the third-party doctrine.[15] Since the CSLI was noncontent data (that is, data about Carpenter's cell phone, rather than the data Carpenter's cell phone transmitted) and acquired from a third party (Carpenter's cell-phone provider), the Court of Appeals held that the Fourth Amendment did not apply, and thus the D order was constitutional.[16]

The Supreme Court reversed. Most of the Court's opinion — and the portion of the opinion that has received the most public and scholarly commentary — focused on the question of whether acquisition of CSLI from a third party could in fact constitute a search within the meaning of the Fourth Amendment. The Court held that, because the amount of CSLI the government acquired exposed a vast amount of private information, Carpenter had a "reasonable expectation of privacy" in that information, and thus the Fourth Amendment applied.[17] Although the Court did not overrule the third-party doctrine, it substantially limited its scope, so much so that one commentator takes the decision as "declar[ing] the third-party doctrine to be almost dead."[18]

Although the Court (and the four separate dissents) focused on the issue of Fourth Amendment coverage — was the government's acquisition of Carpenter's CSLI a "search"? — that did not resolve the issue of whether the government acted unlawfully; the Court still needed to decide whether the search was "unreasonable." Without much analysis, the Court applied the traditional warrant requirement, whereby "warrantless searches are typically unreasonable where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing."[19] Because the SCA allows for D orders on a showing of less than probable cause, D orders cannot qualify as warrants. And because none of the traditional warrant exceptions — namely exigency — applied, the Court held the government's acquisition of CSLI to be unlawful. The Court thus found the SCA to be unconstitutional to the extent that it permits the government to collect

14. *Id.* at 2212.

15. *Id.* at 2213.

16. United States v. Carpenter, 819 F.3d 880, 886-89 (6th Cir. 2016), *rev'd*, 138 S. Ct. 2206 (2018).

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

18. Ohm, *supra* note 2, at 8.

19. *Carpenter*, 138 S. Ct. at 2221 (internal quotation marks omitted) (quoting Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 652-53 (1995)).

certain categories of noncontent data (like a large amount of CSLI) with less than probable cause. But should it have?

II. FOUR MODELS OF THE FOURTH AMENDMENT

As Christopher Slobogin has pointed out, a useful way to think about the Fourth Amendment is to imagine a world in which the amendment didn't exist, decide on core principles of investigative criminal procedure that we can all agree on, and then (with the least possible unsettling of precedent) identify how to bring Fourth Amendment doctrine in line with those principles.[20] We would

20. *See* Christopher Slobogin, *The World Without a Fourth Amendment*, 39 UCLA L. REV. 1, 3-4 (1991). Such an approach is decidedly nonoriginalist, and to some may thus be a dubious methodological choice. But it is nonetheless a defensible one. Even if we can agree on what the Fourth Amendment meant—that is, we can resolve the question of constitutional interpretation—it's unclear to what extent the original understanding helps with construction: the task of applying that original understanding to modern problems of government access to third-party data. *See generally* Lawrence B. Solum, *Originalism and Constitutional Construction*, 82 FORDHAM L. REV. 453 (2013) (discussing the relationship between interpretation and construction in constitutional originalism). Given the enormous differences between 1791 and now, which part of the original understanding should we emphasize, especially when different parts cut in different directions? For example, we know the Framers hated general warrants, but was their concern about giving police untrammeled discretion to physically search their homes and persons (in which case warrantless collection of CSLI from third parties should pose no Fourth Amendment concern)? Or were they instead concerned more generally about broad discretion by the government to investigate crime (in which case collection of CSLI should trigger Fourth Amendment protections)? Moreover, the constitutional understanding of the Framers depended on a very different role for the constitutional guarantees in the Bill of Rights, and thus a very different idea of remedies. *See* Jamal Greene, *The Supreme Court, 2017 Term—Foreword: Rights as Trumps?*, 132 HARV. L. REV. 28, 109-13 (2018). The further we get from the core police practices of 1791, the more general our use of the Fourth Amendment will be—to the point that originalism provides no more definite answers than does a more general balancing of privacy versus security. This is evidenced by *Carpenter* itself, where Justice Thomas, the Supreme Court's most committed originalist, came to conclusions opposite those drawn by prominent Fourth Amendment originalists and historians like Laura Donohue and William Cuddihy. *See* Ohm, *supra* note 2, at 52-53; *see also* Lawrence Rosenthal, *An Empirical Inquiry into the Use of Originalism: Fourth Amendment Jurisprudence During the Career of Justice Scalia*, 70 HASTINGS L.J. 75, 118 n.194 (2018) ("We have no way of knowing whether the Framing-era understandings that Justices Thomas, Alito, and Gorsuch invoked were critically dependent on the technological limitations of the era, which effectively constrained the volume of information about the activities of an investigative target that could be obtained from third parties.").

The Court seems to have realized the difficulty with Fourth Amendment originalism, at least in the context of new technology. As Paul Ohm notes, the "majority opinion engages in almost no historical analysis, beyond an obligatory acknowledgement of the role the opposition to general warrants and writs of assistance played in sparking the American Revolution." Ohm, *supra* note 2, at 53. Thus, whatever its theoretical interest, originalism is not, and is unlikely to soon become, a major driver of Fourth Amendment jurisprudence. *See* Rosenthal,

need to decide: (1) what sorts of government actions the rules cover, (2) what the rules require of those actions, and (3) what to do when the rules are violated. This nicely maps to how Fourth Amendment doctrine is generally divided: scope, requirements, and remedy. For our purposes, we can put the issue of remedy to the side and focus on scope and requirements. In particular, consider four different approaches: (1) minimal, (2) maximal, (3) selective, and (4) regulatory.

Law-and-order types might support a *minimal* criminal procedure with narrow scope and few requirements — a world in which rules of criminal procedure apply infrequently and are quite permissive even when they do apply. There aren't many defenders of this position in the judiciary (and almost none in the academy), and it is thus an unlikely model for Fourth Amendment jurisprudence.

Civil libertarians want the opposite: they want a *maximal* criminal procedure that combines broad scope and a lot of requirements — a world in which the rules of criminal investigations apply to most police activities and impose substantial restrictions on them. The vast majority of academic commentary on the Fourth Amendment takes this view to one degree or another — for example, by criticizing the third-party doctrine[21] or celebrating (and urging the reinvigoration of) the warrant requirement.[22]

The maximal approach has two disadvantages, however. The first is that a maximalist push for civil liberties will, at some point, detract from social welfare, since civil liberties must, at some point, be traded off for public safety.[23] The second is that, whatever its normative merits, the maximal position is a political nonstarter — not just in terms of electoral politics, but also in the judicial politics underlying constitutional law. A variety of factors — from the small-c conservativism of the federal bench, to its demographic makeup (many judges are former federal prosecutors),[24] to the United States' exceptionalism in both crime and

supra at 80 (noting "difficulties in applying original meaning in contemporary constitutional adjudication" of Fourth Amendment issues).

21. *See, e.g.*, SOLOVE, *supra* note 7, at 102-10; *see also* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563-64 (2009) (describing common criticisms of the third-party doctrine).

22. *See, e.g.*, Oren Bar-Gill & Barry Friedman, *Taking Warrants Seriously*, 106 NW. U. L. REV. 1609 (2012); David Gray, *Fourth Amendment Remedies as Rights: The Warrant Requirement*, 96 B.U. L. REV. 425 (2016).

23. *See* Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 163-64 & n.360 (2018).

24. *See* Editorial, *The Homogenous Federal Bench*, N.Y. TIMES (Feb. 6, 2014), https://www.nytimes.com/2014/02/07/opinion/the-homogeneous-federal-bench.html [https://perma.cc/VZ4K-SULW].

punishment[25] — mean that our criminal procedure is highly unlikely to settle into a civil-libertarian equilibrium. As the history of the Fourth Amendment shows, in the long run criminal procedure must meet criminal justice halfway.[26]

This brings us to the *selective* approach: a narrow-scope, high-requirements position that captures much of contemporary Fourth Amendment doctrine. Constitutional rules of criminal procedure apply only to certain narrow categories of government actions, but, where the rules apply, they impose substantial limitations on government practices, primarily through the requirement of ex ante judicial authorization supported by individualized, probable cause. The selective approach thus supports the once-dominant and still influential warrant requirement.[27]

A key flaw with the selective approach is that it withholds Fourth Amendment protections from large categories of police practices that clearly deserve it.[28] Under current doctrine, the Fourth Amendment doesn't apply when the police physically track our movements through the streets.[29] But why not? Clearly such surveillance infringes on privacy, raises the specter of government abuse, and can chill liberty. An ideal code of criminal procedure should, therefore, at least *regulate* (even if it ultimately allows) such conduct.

---

25. *See* Kevin R. Reitz, *American Exceptionalism in Crime and Punishment: Broadly Defined*, *in* AMERICAN EXCEPTIONALISM IN CRIME AND PUNISHMENT 1 (Kevin R. Reitz ed., 2017).

26. This is a claim about how law is, not how it ought to be (except to the extent that it's pointless to demand of a doctrine something it cannot accomplish). As a recent strand of constitutional history has emphasized, the Supreme Court rarely gets too far in front of public opinion and settled practice. *See generally* BARRY FRIEDMAN, THE WILL OF THE PEOPLE: HOW PUBLIC OPINION HAS INFLUENCED THE SUPREME COURT AND SHAPED THE MEANING OF THE CONSTITUTION (2009); MICHAEL J. KLARMAN, FROM JIM CROW TO CIVIL RIGHTS: THE SUPREME COURT AND THE STRUGGLE FOR RACIAL EQUALITY (2006). In the Fourth Amendment context, the Supreme Court "frequently draws on the official practice of regulated government actors today as a source of constitutional meaning." Aziz Z. Huq, *Fourth Amendment Gloss*, 113 NW. U. L. REV. 701, 703 (2019). Even the Warren Court, which most dramatically expanded the scope of constitutional criminal procedure, ultimately (and almost unanimously) acquiesced to the long-standing practice of stop and frisk, even if it added some level of procedural protection. *See* Terry v. Ohio, 392 U.S. 1, 20 (1968).

27. *See* Tracey Maclin, *The Central Meaning of the Fourth Amendment*, 35 WM. & MARY L. REV. 197, 202-07 (1993).

28. It also fits awkwardly with the text of the Fourth Amendment. As Akhil Amar notes, any common-sense understanding of "search" would include much activity that current Fourth Amendment doctrine excludes from that category. Akhil Reed Amar, Terry *and Fourth Amendment First Principles*, 72 ST. JOHN'S L. REV. 1097, 1100-02 (1998) [hereinafter Amar, *Terry*]. Earlier, Amar made the case that the warrant requirement is similarly atextual. *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 762-93 (1994).

29. *See* 1 WAYNE R. LAFAVE, SEARCH & SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.7(g) (5th ed. 2018).

So why have courts largely adopted the selective model? It's unlikely that the Justices on the Supreme Court actually think that detailed public surveillance doesn't implicate Fourth Amendment values.[30] Rather, courts are selective in where they apply the Fourth Amendment because they perceive any broad-scope position as incompatible with the realities of modern policing — as long as courts impose the high requirements of individualized, probable cause in all cases in which the Fourth Amendment applies.[31] As Anthony Amsterdam recognized in his famous lectures on the Fourth Amendment, an "all-or-nothing approach to the amendment puts extraordinary strains upon the process of drawing its outer boundary lines."[32]

This dynamic is apparent in how lower courts have applied *Carpenter*: generally cabining *Carpenter*'s cabining of the third-party doctrine.[33] *Carpenter*'s holding only applies to a particular set of records: more than seven days of reasonably precise CSLI.[34] Thus, courts not wanting to subject third-party surveillance to the Fourth Amendment's requirements could choose to read *Carpenter* narrowly. For example, one district court has held that *Carpenter* did not apply to grand jury subpoenas sent to an internet service provider (ISP) and an email provider for subscriber information associated with an ISP account and an email address: "The privacy interest in this type of identifying data . . . simply does not rise to the level of the evidence in *Carpenter* such that it would require law enforcement to obtain a search warrant."[35] Courts have similarly found *Carpenter*

30. *See, e.g.*, United States v. Jones, 565 U.S. 400, 414-17 (2012) (Sotomayor, J., concurring); *id.* at 430-31 (Alito, J., concurring in the judgment); *see also id.* at 412 (majority opinion).

31. *See* Christopher Slobogin, *The Liberal Assault on the Fourth Amendment*, 4 OHIO ST. J. CRIM. L. 603, 605 (2007).

32. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 388 (1974); *see also* Slobogin, *supra* note 31, at 607 ("[T]he consequence of the Court's rigid adherence to the probable cause standard for searches has been judicial reluctance to apply the latter term even to government actions that clearly involve looking for evidence of crime.").

33. This paragraph is based on a review of the roughly 200 federal and state opinions available on Westlaw (published and unpublished) that cite *Carpenter* as of early 2019. Of those that apply *Carpenter* to criminal-procedure fact patterns, the majority involve a backlog of two types of cases that are not relevant to this Essay: (1) good-faith issues for CSLI collected before *Carpenter* was issued, *see, e.g.*, United States v. Curtis, 901 F.3d 846, 848-49 (7th Cir. 2018); United States v. Goldstein, 914 F.3d 200, 201–02 (3d Cir. 2019); and (2) straightforward applications of *Carpenter* to similar fact patterns, *see, e.g.*, United States v. Curtis, 901 F.3d 846, 848 (7th Cir. 2018); United States v. Woods, 336 F. Supp. 3d 817, 828-29 (E.D. Mich. 2018). Although such cases make up the bulk of *Carpenter* citations, their proportion will decline in the future since the pre-*Carpenter* CSLI cases are a fixed pile and police departments will begin getting warrants for CSLI.

34. Carpenter v. United States, 138 S. Ct. 2206, 2217 n.3 (2018).

35. United States v. Tolbert, 326 F. Supp. 3d 1211, 1225 (D.N.M. 2018). Other courts have held the same. *See, e.g.*, United States v. Contreras, 905 F.3d 853 (5th Cir. 2018); United States v.

inapplicable to fixed video monitoring,[36] location-revealing bank records,[37] and online-shopping histories.[38] Other courts have emphasized that *Carpenter* only discussed historical, rather than real-time, collection of CSLI.[39] Still others have emphasized *Carpenter*'s seven-day timeframe as a potential lower bound for when Fourth Amendment protections kick in.[40]

The stakes for this jurisprudential choice are high, especially when applied to emerging "data driven," "big data," and "predictive" policing.[41] Because these investigative practices rely on accumulating and analyzing large data sets, they cannot operate if the government is required to establish probable cause that a particular individual is tied to a particular offense before the government can collect or analyze that person's data. But if the Fourth Amendment doesn't apply at all to such programs—for example, because, under the third-party doctrine, individuals have no privacy interests in data generated by others about them—then highly intrusive and privacy-threatening government activity will go unchecked. If courts have to choose between hamstringing police and allowing privacy intrusions to go unchecked, they will likely choose the latter. But the public loses out either way.

Gregory, No. 8:18CR139, 2018 WL 6427871, at *2 (D. Neb. Dec. 7, 2018); United States v. Streett, No. CR 14-3609 JB, 2018 WL 6182439, at *63 (D.N.M. Nov. 27, 2018); United States v. Monroe, 350 F. Supp. 3d 43, 48–49 (D.R.I. 2018); Cryer v. Idaho Dep't of Labor, No. 1:16-cv-00526-BLW, 2018 WL 3636529, at *1 n.1 (D. Idaho July 30, 2018).

36. *See, e.g.*, United States v. Kubasiak, No. 18-cr-120-pp, 2018 WL 4846761 (E.D. Wis. Oct. 5, 2018); United States v. Kay, No. 17-cr-16, 2018 WL 3995902 (E.D. Wis. Aug. 21, 2018).

37. *See* United States v. Frei, No. 3:17-cr-00032, 2019 WL 189826, at *1-3 (M.D. Tenn. Jan. 14, 2019).

38. *See* United States v. Schaefer, No. 3:17-CR-00400-HZ, 2019 WL 267711, at *5 (D. Or. Jan. 17, 2019).

39. *See, e.g.*, People v. Robinson, No. 337755, 2018 WL 6579355, at *4 n.3 (Mich. Ct. App. Dec. 13, 2018) (unpublished opinion); Andres v. State, 254 So. 3d 283, 297 n.7 (Fla. 2018). Notably, the federal government has conceded in at least one instance that *Carpenter* does indeed apply to real-time CSLI. *See* United States v. Hammond, No. 3:18-CR-5 RLM-MGG, 2018 WL 5292223, at *2 (N.D. Ind. Oct. 24, 2018).

40. *See* Sims v. State, No. PD-0941-17, 2019 WL 208631, at *8 (Tex. Crim. App. Jan. 16, 2019) (finding that the defendant "did not have a legitimate expectation of privacy in his physical movements or his location as reflected in the less than three hours of real-time CSLI records accessed by police by pinging his phone less than five times").

41. *See generally* ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2017); BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION 211-81 (2017); Kiel Brennan-Marquez, *Plausible Cause: Explanatory Standards in the Age of Powerful Machines*, 70 VAND. L. REV. 1249 (2017); Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35 (2014); Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871 (2016).

Fortunately, this choice—between a selective, narrow-scope criminal procedure and a maximal, broad-scope one—is false. Both alternatives assume that, whenever the rules of criminal procedure are implicated (that is, whenever there is a "search" under the Fourth Amendment), the full warrant requirement—ex-ante authorization by an independent magistrate, supported by probable cause—applies.

But this need not be the case. A *regulatory* model of criminal procedure would have criminal procedure rules apply to almost all government investigatory conduct, but would tailor the requirements to the invasiveness of the government action, the public-safety interests at stake, and the costs and benefits of different levels of ex-ante authorization and predication.[42] Criminal procedure would then be no different than any other of the many regulatory domains in which government action must always meet some minimal bar of evidence, logic, and reasoned elaboration.[43] Doctrinally, this view emphasizes that "[t]he touchstone of the Fourth Amendment is reasonableness," and that reasonableness is ultimately a question of balancing: "assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[44]

Such a response to *Carpenter* would fully accept not just the letter but also the spirit of the case: that the third-party doctrine, by making a reasonable expectation of privacy (and thus Fourth Amendment coverage) rise and fall based on the mere fact of third-party access, is hopelessly flawed and should be broadly cut back, if not abandoned entirely. Whatever the ultimate ground(s) of the Fourth Amendment—privacy, security, liberty, etc.—the third-party doctrine is both so over- and under-inclusive that its drawbacks outweigh its doctrinal benefits.

Without the third-party doctrine, courts would have to decide whether people have reasonable expectations of privacy in the many categories and vast quantities of digital information that are currently excluded from the Fourth Amendment. Freed from the concern that finding government activity a search would require the onerous imposition of the full warrant requirement, courts would almost certainly widely expand Fourth Amendment coverage. This would finally bring Fourth Amendment doctrine in line with general intuitions of what

---

42. Notably, such an approach has been advocated in these pages by no less than the intelligence community's former chief lawyer. *See* Robert S. Litt, *The Fourth Amendment in the Information Age*, 126 YALE L.J.F. 8, 13-14 (2016).

43. In administrative law, for example, arbitrary and capricious review operates in this fashion. *See, e.g.*, RICHARD J. PIERCE, JR. & KRISTIN E. HICKMAN, ADMINISTRATIVE LAW TREATISE § 11.1 (6th ed. 2018).

44. United States v. Knights, 534 U.S. 112, 118-19 (2001) (internal quotation marks omitted) (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

deserves Fourth Amendment regulation: not just physical intrusions like searches of homes and persons, but also digital intrusions of information—location, communication, etc.—held by third parties.

What would a post-*Carpenter*, reasonableness-centered, regulatory jurisprudence look like? The Seventh Circuit provided a hint in *Naperville Smart Meter Awareness v. City of Naperville*.[45] Plaintiffs, a civil-society group, sued Naperville, Illinois to prevent it from installing electricity "smart meters." Smart meters, unlike ordinary electricity meters, collect vast quantities of granular information on domestic electricity consumption, which can "reveal[] . . . the happenings inside a home."[46] The plaintiffs argued that the city's collection of such data would violate the Fourth Amendment's prohibition on unreasonable searches. Naperville responded that the third-party doctrine applied, since residents entered a "'voluntary relationship' to purchase electricity" and thus "sacrifice[d] their expectation of privacy in smart-meter data."[47] In rejecting the city's third-party-doctrine argument, the Seventh Circuit relied on *Carpenter*:

> [I]n this context, a choice to share data imposed by fiat is no choice at all. If a person does not—in any meaningful sense—"voluntarily 'assume the risk' of turning over a comprehensive dossier of physical movements" by choosing to use a cell phone, it also goes that a home occupant does not assume the risk of near constant monitoring by choosing to have electricity in her home.[48]

But what sort of Fourth Amendment protection would be called for? Crucially, the court did not follow *Carpenter* in assuming that only a warrant would render the government search "reasonable" under the Fourth Amendment. Instead, the court analyzed the data-collection program under a reasonableness balancing test. It concluded, based on the minimal intrusiveness of the smart-meter program, the noninvestigatory purpose of the program, and the substantial government interest in electrical-grid modernization, that the government action, while a warrantless search, was constitutional.[49]

Naperville is a start, but more doctrinal work needs to be done to combine *Carpenter*'s cutting back on the third-party doctrine with a reasonableness test that looks beyond the warrant requirement. Courts will need to extend

---

45. 900 F.3d 521 (7th Cir. 2018).

46. *Id.* at 524; *see also* Sonia K. McNeil, Note, *Privacy and the Modern Grid*, 25 HARV. J.L. & TECH. 199, 200-01 (2011).

47. *City of Naperville*, 900 F.3d at 527.

48. *Id.* at 527 (quoting Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (citations omitted)).

49. *Id.* at 528-29.

Naperville's reasonableness approach to surveillance conducted for the "ordinary enterprise of investigating crimes."[50] It remains to be seen whether lower courts will be able to read *Carpenter* creatively to do so[51] or whether the Supreme Court will itself have to clarify the stringency of the warrant requirement.

III. REASONS FOR REASONABLENESS

The intuition behind reasonableness balancing is, well, that it's reasonable. After all, how else could we approach complicated policy areas like law enforcement and government surveillance than by pragmatically trying to balance costs and benefits? Nevertheless, my proposal is, like all others of its type, subject to the "traditional critique of reasonableness": (1) that it is insufficiently protective of privacy and security; and (2) that, as compared to the "rule" requiring warrants, the reasonableness-balancing "standard" is too difficult to administer.[52]

A. Reasonableness Can Protect Fourth Amendment Values

The longstanding concern with departing from a strict warrant requirement is that the results undermine the Fourth Amendment's protections of security and privacy. For example, in *Terry v. Ohio* the Supreme Court held that, although a stop and frisk is a search and seizure within the scope of the Fourth Amendment, the police can conduct them with less than probable cause.[53] *Terry* has been widely criticized as both a betrayal of the Fourth Amendment's core

50. City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000) (declining to permit a generalized police narcotics checkpoint without individualized suspicion).

51. If I were to write a lower court opinion applying *Carpenter* that tried to avoid the warrant requirement, I would lean on two passages in the majority opinion. First, *Carpenter* reaffirms the baseline reasonableness requirement, whereby the "ultimate measure of the constitutionality of a governmental search is 'reasonableness'" and where "warrantless searches are *typically*" – and thus not necessarily – "unreasonable where 'a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing.'" *Carpenter*, 138 S. Ct. at 2221 (quoting Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 652-53 (1995)). Second, the opinion emphasizes (as the Chief Justice did in *Riley v. California*, 134 S. Ct. 2473, 2494 (2014)), that exigent circumstances may still permit warrantless (though presumably still probable-cause-supported) acquisitions of CSLI. *Carpenter*, 138 S. Ct. at 2222. Still, the best reading of *Carpenter* is that the case embraces the warrant requirement.

52. Cynthia Lee, *Reasonableness with Teeth: The Future of Fourth Amendment Reasonableness Analysis*, 81 MISS. L.J. 1133 (2012); *see also* Richard S. Frase, *What Were They Thinking? Fourth Amendment Unreasonableness in* Atwater v. City of Lago Vista, 71 FORDHAM L. REV. 329 (2002).

53. 392 U.S. 1, 20-24 (1968).

values[54] and an invitation to programmatic police harassment that falls disproportionality on racial minorities without providing substantial public-safety benefits.[55] And the Supreme Court's administrative and special-needs cases—where the Court explicitly engages in freestanding reasonableness balancing—have been similarly criticized, with commentators characterizing them as using highly deferential rational basis review in which the government interest—however attenuated or invented after the fact—inevitably trumps individual privacy and security.[56] Even defenders of reasonableness balancing concede that the Supreme Court has failed to specify precisely what constitutes "reasonableness"[57] for a warrantless search.

That the task is challenging, however, does not mean it is impossible. A growing movement, the "new administrativist turn,"[58] looks to administrative law and theory as a model for regulating government investigations and surveillance. For example, Daphna Renan proposes using cost-benefit analysis to measure "programmatic efficacy."[59] Barry Friedman and Maria Ponomarenko suggest that local police departments promulgate rules through notice and comment before acting.[60] Slobogin argues for a general "proportionality principle" for law-

54. *See* Lawrence Rosenthal, *Pragmatism, Originalism, Race, and the Case Against* Terry v. Ohio, 43 TEX. TECH. L. REV. 299, 300 & n.7 (2010) (collecting articles critical of *Terry*).

55. These criticisms have been made most recently and powerfully in the context of stop-and-frisk programs in major cities like New York, which a federal court held had violated the Fourth and Fourteenth Amendment rights of minorities. *See* Floyd v. City of New York, 959 F. Supp. 2d. 540 (S.D.N.Y. 2013); *see also* Aziz Z. Huq, *The Consequences of Disparate Policing: Evaluating Stop and Frisk as a Modality of Urban Policing*, 101 MINN. L. REV. 2397 (2017); Tracey L. Meares, *Programming Errors: Understanding the Constitutionality of Stop-and-Frisk as a Program, Not an Incident*, 82 U. CHI. L. REV. 159 (2015).

56. *See* Lee, *supra* note 52, at 1147-48.

57. *See* Amar, *Terry*, *supra* note 28, at 1099-1100; *see also* Christopher Slobogin, *Let's Not Bury* Terry*: A Call for Rejuvenation of the Proportionality Principle*, 72 ST. JOHN'S L. REV. 1053, 1054-55 (1998) (praising *Terry* but criticizing the Court for using the case's balancing formula as a "smoke screen for an ad hoc agenda").

58. Andrew Manuel Crespo, *Systemic Facts: Toward Institutional Awareness in Criminal Courts*, 129 HARV. L. REV. 2049, 2059 (2016).

59. Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1112-26 (2016); *see also* Cass R. Sunstein, *Beyond Cheneyism and Snowdenism*, 83 U. CHI. L. REV. 271 (2016) (exploring applications of cost-benefit analysis to national security surveillance programs).

60. Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 1827, 1834 (2015); *see also* Christopher Slobogin, *Policing as Administration*, 165 U. PA. L. REV. 91, 91 (2016) (arguing that police agencies should engage in "notice-and-comment rulemaking or a similar democratically oriented process" when they create policies aimed at "largely innocent categories of actors").

enforcement activities,[61] and, in the case of broad surveillance programs, appropriate levels of democratic participation.[62]

Matters should be substantially easier where the Fourth Amendment activity is pursuant to legislative authorization, as was the case with the SCA and the CSLI acquisition in *Carpenter*. In such cases, courts should at least seriously consider whether the legislature's judgment can shed useful light on the difficult tradeoffs inherent in any surveillance scheme. Legislatures have several structural advantages when it comes to surveillance policymaking: Congress can legislate more comprehensively, it has access to better information and expertise, and, most importantly, its representative nature means that it enjoys a legitimacy that the courts do not, at least when it comes to making tradeoffs between otherwise reasonable policy choices. As Judge Wilkinson has observed with respect to the SCA's treatment of CSLI: "Faced with a term literally crying out for balance between the competing interests of individual privacy and societal security, it is appropriate to accord some degree of deference to legislation weighing the utility of a particular investigative method against the degree of intrusion on individuals' privacy interests."[63]

None of this is to suggest that courts should uncritically let legislatures preempt the field of criminal procedure.[64] Nor does it suggest that a court, after performing reasonableness balancing, could never conclude that a warrant is in fact necessary.[65] But we should recognize that the judiciary has no monopoly on reasonableness. We should also recognize the need to incentivize legislatures (not to mention law-enforcement and surveillance agencies themselves) to develop detailed and binding regulations in contexts where the Fourth

---

61. *See* Slobogin, *supra* note 20; *see also* Greene, *supra* note 20, at 124-27 (arguing that "[p]roportionality jurisdictions tend to engage . . . weighty questions directly rather than load them onto a definitional frame that cannot bear their weight"); Vicki C. Jackson, *Constitutional Law in an Age of Proportionality*, 124 YALE L.J. 3094, 3130-36 (2015) (suggesting that "some form of more individualized proportionality analysis may produce decisions that are both better reasoned and more protective of rights than the 'categorical approach' employed by the U.S. [Supreme] Court.").

62. *See* Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721 (2014).

63. United States v. Graham, 824 F.3d 421, 439 (4th Cir. 2016) (en banc) (Wilkinson, J., concurring).

64. *See* Orin S. Kerr, *The Effect of Legislation on Fourth Amendment Protection*, 115 MICH. L. REV. 1117 (2017).

65. This is especially true where a court concludes that the digital search is functionally equivalent to an analog search that falls squarely within the warrant requirement. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that, notwithstanding the SCA, "[t]he government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause.").

Amendment does apply, and not, as is currently the case, only where the Fourth Amendment doesn't apply.[66] The less deference the political branches can expect regarding what constitutes reasonableness under the Fourth Amendment, the less they'll try to bring their representative processes to bear on the issue.

Given all this, it's notable how cursory—dismissive, even—was the Supreme Court's treatment of the SCA. In a single paragraph, the Court disparaged the applicable legal standard—whether the CSLI was "relevant and material to an ongoing investigation"—as "fall[ing] well short of the probable cause required for a warrant."[67] The Court read the standard expansively, such that "law enforcement need only show that the cell-site evidence might be pertinent to an ongoing investigation—a gigantic departure from the probable cause rule."[68]

The Court's insistence on portraying the legislative standard as meaningless led it to a mischaracterization. The court "decline[d] to grant the state unrestricted access to a wireless carrier's database of physical location information."[69] But D orders permit no such thing: as noted above, the D-order standard is drawn from the intermediate requirements of *Terry*, and provides far greater protection than a mere grand-jury subpoena, which can issue with essentially no suspicion at all.[70]

A useful case study of how courts can analyze the constitutionality of complex, legislatively authorized surveillance programs can be found in section 702 of the Foreign Intelligence Surveillance Act (FISA).[71] Section 702, which has been reauthorized by Congress multiple times over the past decade, allows the government to conduct warrantless domestic surveillance of electronic communications on "persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[72] Critically, section 702 does not require the government to obtain a warrant before engaging in such collection;

---

66. *See* Kerr, *supra* note 64, at 1148.

67. Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

68. *Id.* (internal quotations omitted).

69. *Id.* at 2223. It also led to the majority mischaracterizing the CSLI collected in the case as more accurate than it actually was. *See* Kerr, *supra* note 2, at 10-15. Because the majority was operating under a warrant-requirement paradigm (narrow-scope/high-requirements), if it wanted to find D orders for CSLI unconstitutional, it needed to clear the high bar of finding that the D orders were searches. And the more the majority could portray the government conduct as invasive, the easier it was to establish that it was a search.

70. *See supra* note 10. This is a serious error, given the settled interpretative canon that statutes are to be interpreted so as to minimize, rather than exacerbate, constitutional difficulties. *See* I.N.S. v. St. Cyr, 533 U.S. 289, 299-300 (2001).

71. *See* FISA Amendments Act of 2008, Pub. L. No. 110-261, sec. 101, § 702, 122 Stat. 2436, 2438-48 (codified as amended at 50 U.S.C. § 1881a (2018)).

72. 50 U.S.C. § 1881a(a).

rather, the program sets up a complex system of ex ante judicial oversight (of targeting and minimization procedures) and ex post internal oversight (through multiple layers of compliance review, both within the intelligence agency itself and from the Department of Justice) to minimize incidental impacts on the privacy of U.S. persons.[73] There is no question that interception of information under section 702 is a "search" under the Fourth Amendment. But those courts that have evaluated the constitutionality of the program have upheld it on the grounds that its institutional features render it reasonable.[74] The future of law-enforcement electronic surveillance lies in FISA-like regulatory regimes that innovatively combine judicial oversight with rigorous internal compliance mechanisms, not slavish adherence to a judicially constructed, one-size-fits-all warrant requirement.

FISA is hardly uncontroversial, and civil libertarians may view my argument—that domestic, law-enforcement electronic investigations use foreign-intelligence surveillance as a model—as taking surveillance law in precisely the wrong direction.[75] But the realistic alternative is not a maximal Fourth Amendment, but rather the limping along of the selective one. In other words, either *Carpenter*'s rigid emphasis on the warrant requirement will have to give way to some less demanding requirement, or the third-party doctrine will live on to the extent law enforcement needs it to, as courts cabin the effect of *Carpenter*.

B. Reasonableness Is Administrable

As Jamal Greene notes, "[t]he most significant theoretical concern with importing proportionality jurisprudence into U.S. courts stems from the nature of the Supreme Court as an apex court within a system of highly decentralized constitutional jurisdiction."[76] In particular, "[i]nsofar as proportionality"—or, in the Fourth Amendment context, reasonableness review—"relies heavily on case-by-case adjudication, it gives less guidance to other courts, public officials, and

---

73. For detailed analyses of how the (notoriously complex) section 702 program operates as well as policy evaluations, see 1 DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS 2d ch. 17 (2012); and PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2014).

74. *See, e.g.*, United States v. Mohamud, 843 F.3d 420, 443-44 (9th Cir. 2016).

75. Laura Donohue has leveled some of the most comprehensive legal critiques of section 702. *See, e.g.*, LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE: PRIVACY AND SURVEILLANCE IN A DIGITAL AGE (2016); Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117 (2015). For a response, see Joel Brenner, Book Review, 9 J. NAT'L SEC. L. & POL'Y 631 (2018).

76. Greene, *supra* note 20, at 93-94.

citizens than does a categorical approach"—that is, a strict warrant requirement.[77] This in turn can raise rule-of-law fears, as the "freewheeling 'reasonableness' standard . . . suffers from the concerns about official arbitrariness that rules are meant to combat."[78]

This is an important critique of any reasonableness-focused interpretation of the Fourth Amendment, but (as Greene notes) it is not fatal. First, the increased decision costs associated with reasonableness (as with standards generally) may nevertheless be smaller than the accuracy costs associated with categorical rules.[79] Given the manifest lack of fit between a blanket warrant requirement and modern data-driven police and surveillance practices, any administrability costs of a reasonableness regime seem to be dwarfed by the accuracy costs of continuing to abide by a strict warrant requirement—both in terms of the practices that will be unnecessarily precluded, and those practices that should be covered by the Fourth Amendment but will not be.

Second, the inadministrability of a reasonableness standard is exaggerated. Standards, including in the Fourth Amendment context, do not remain open-ended and amorphous for long; as they are fleshed out, they naturally become more codified and rule-like.[80] And even where some residual uncertainty remains, it is hardly fatal. For example, the probable-cause standard is famously vague,[81] yet its backers include some of the most diehard supporters of the warrant requirement.

No doubt a full description of what constitutes "reasonableness" for digital searches under the Fourth Amendment will be a complicated, sometimes messy, affair. But a warrant-requirement jurisprudence will be just as complex, as evidenced by the complicated series of tests courts currently use to decide whether a particular government action counts as a "search."[82] Digital searches are not

---

77. *Id.* at 94.

78. Carol S. Steiker, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820, 855 (1994).

79. *See* Greene, *supra* note 20, at 94; *see also* Slobogin, *supra* note 20, at 70-71 (noting that "even seemingly 'bright-line' rules usually become blurred as the police and the adversarial process test their outer limits"); Jackson, *supra* note 61, at 3155 (noting that "[e]ven if 'categorical' rules would result in fewer errors . . . a standard may result in fewer 'serious' errors").

80. *See* Slobogin, *supra* note 20, at 74. *See generally* Frederick Schauer, *The Convergence of Rules and Standards*, 2003 N.Z. L. REV. 303 (suggesting that the distinction between rules and standards tends to collapse in practice).

81. *See, e.g.*, Illinois v. Gates, 462 U.S. 213, 232 (1983) ("[P]robable cause is a fluid concept . . . not readily, or even usefully, reduced to a neat set of legal rules.").

82. Anyone who has struggled to learn, teach, or apply *Katz*'s reasonable-expectation-of-privacy standard to the broad variety of real-world policing scenarios will appreciate why Fourth Amendment doctrine is so frequently characterized as "'a mess,' 'an embarrassment,' and 'a mass of contradictions.'" Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 479 (2011).

exempt from this problem. For example, leading Fourth Amendment scholar Orin Kerr devotes dozens of pages to operationalizing *Carpenter*'s holding on scope to the many varieties of real-world electronic investigations.[83] This is an invaluable service to lower courts, and I generally agree with Kerr's conclusions, insofar as they assume the continuation of the selective (narrow-scope/high-requirement) paradigm for electronic surveillance.

But Kerr's method does not strike me as substantially less complicated than Fourth Amendment doctrine would be under a regulatory (high-scope/variable-requirement) paradigm. As Slobogin notes, "even seemingly 'bright-line' rules usually become blurred as the police and the adversarial process test their outer limits. The grail of 'rule-oriented' jurisprudence is as mythical as King Arthur's."[84] And crucially, doctrinal work to flesh out the reasonableness requirement would more directly engage with what I take to be the heart of the Fourth Amendment: an optimization of the inevitable tradeoffs between privacy and security. That is, the question of "reasonableness."

CONCLUSION

If the Supreme Court is serious (as I hope it is) about rolling back the third-party doctrine—if, in other words, it means *Carpenter* to be the beginning of a Fourth Amendment revolution, not just a one-off case—it will sooner or later have to repudiate *Carpenter*'s suggestion that warrants (and thus individualized, probable cause) are required for all electronic surveillance. In the meantime, a critical research agenda in Fourth Amendment scholarship must be to develop an account of what substitutes for warrants are reasonable in a digital age.

Visiting Assistant Professor of Law, University of Minnesota Law School. *For helpful comments I thank Richard Frase, Jill Hasday, Aziz Huq, Orin Kerr, Anna Lvovsky, Justin Murray, Shava Nerad, Shalev Roisman, Christopher Slobogin, and participants in the Public Law Workshop at the University of Minnesota Law School. For terrific research assistance I thank Sam Cleveland and Paul Dimick. And for excellent editorial work I thank the editors of the* Yale Law Journal.

83. *See* Kerr, *supra* note 2.

84. Slobogin, *supra* note 20, at 71.