1-2020

Transparency After Carpenter

Hannah Bloch-Wehba
Texas A&M University School of Law, hbw@law.tamu.edu

Transparency After *Carpenter*

Hannah Bloch-Wehba†

In his lecture at Washburn University School of Law, Professor Matthew Tokson observed that *Carpenter* continued, rather than altered, the existing course of Fourth Amendment jurisprudence. *Carpenter*'s refinement of Fourth Amendment protection is contiguous with previous decisions recognizing the potential privacy harm of new technologies. By recognizing that the government may conduct a Fourth Amendment "search" when it acquires particularly detailed, intrusive information from the coffers of third parties, the *Carpenter* Court, according to Professor Tokson, was attentive to the risk that the profusion of new technologies, and the decreasing costs of criminal investigation, pose to individual privacy.[1] Accordingly, Professor Tokson also concluded that courts applying *Carpenter* will likely recognize this general sensitivity to privacy intrusion and hold that a variety of new technologies—web history, pole cams, and smart homes—are equally entitled to Fourth Amendment protection.

The central observation of this invited response to Professor Tokson's lecture is twofold. First, I write to highlight the social, political, and economic factors at play in the *Carpenter* decision. The *Carpenter* Court recognized, in particular, that digital surveillance implicates the rights of more than just criminal suspects: it poses unique and unappreciated threats to public governance of policing. The decision, I argue, reflects longstanding preoccupations in Fourth Amendment decisions with protecting the "public"—particularly innocent third parties—from intrusive and baseless investigations.[2] In so doing, I situate Professor Tokson's piece alongside other scholarship exploring how Fourth Amendment doctrine protects a broader set of interests than simply those of the criminal defendant or suspect.[3]

---

† Assistant Professor of Law, Drexel University Thomas R. Kline School of Law.

1. Matthew Tokson, *The Next Wave of Fourth Amendment Challenges After* Carpenter, 59 WASHBURN L.J. 1 (2020).

2. *See* Shima Baradaran, *Rebalancing the Fourth Amendment*, 102 GEO. L.J. 1 (2013).

3. *See, e.g.*, David Gray, *Collective Standing under the Fourth Amendment*, 55 AM. CRIM. L. REV. 77 (2018); David Gray, *A Collective Right to Be Secure from Unreasonable Tracking*, 48 TEX. TECH L. REV. 189 (2015); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 119 (2008);

The second contribution is to highlight some practical obstacles to *Carpenter*'s approach of constraining intrusive digital searches. By subjecting (at least some of) those digital searches to the warrant requirement, the *Carpenter* court promoted values of transparency and anti-secrecy. Yet, digital search warrants are governed by a different set of rules than physical ones. Those rules are far more protective of law enforcement interests than their physical counterparts. A raft of secrecy-promoting practices in the digital context helps to ensure that digital searches are not subject to the same kinds of public scrutiny and debate as physical surveillance. This distinction has proven enduring despite *Carpenter*'s suggestion that the formal physical/digital divide should not dispose of constitutional questions. As a result, digital searches remain removed from some of the methods of democratic oversight and scrutiny that the Court may have intended to promote.

I. PRIVACY'S PUBLIC FACE

As Professor Tokson notes, in the decades preceding *Carpenter*, the prevailing rule was that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[4] This rule held regardless of whether the "third party" involved was an undercover informant,[5] a bank,[6] a FedEx worker,[7] a telephone company,[8] or the open sky.[9] Although the rule was not mechanically applied—as Professor Tokson points out, the Court made exceptions in cases concerning hospitals, hotel rooms, and pervasive location tracking[10]—its importance grew in direct relation to the emergence of the digital economy.[11] Indeed, the

---

Thomas P. Crocker, *The Political Fourth Amendment*, 88 WASH. U. L. REV. 303, 337 (2010); Thomas K. Clancy, *What Value(s) Does the Fourth Amendment Serve?: The Fourth Amendment as a Collective Right*, 43 TEX. TECH. L. REV. 255, 277–78 (2010); *see also* Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139 (2016) (exploring how Fourth Amendment doctrine relies on understandings of "societal" or "collective" knowledge).

4. Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).

5. Hoffa v. United States, 385 U.S. 293 (1966).

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

7. United States v. Jacobsen, 466 U.S. 109 (1984).

8. Smith v. Maryland, 442 U.S. 735 (1979).

9. California v. Ciraolo, 476 U.S. 207 (1986).

10. *See* Tokson, *supra* note 1, at 9 (describing *Ferguson v. City of Charleston*, 121 S. Ct. 1281 (2000); *Stoner v. California*, 376 U.S. 483 (1964); and *United States v. Jones*, 565 U.S. 400 (2012)).

11. *See, e.g.*, United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (questioning the third-party doctrine's application in the "digital age"); Stephen E. Henderson, *After* United States v. Jones, *After the Fourth Amendment Third Party Doctrine*, 14 N.C. J.L. & TECH. 431, 435 (2013); Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 649 (2011); Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581 (2011); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101 (2008).

growing power of digital firms, and their control over a wealth of sensitive user data, prompted a profusion of scholarship critiquing the third-party doctrine as out-of-date and out-of-touch.

Concern about the third-party doctrine only grew as the business models of digital firms became more complex, more deeply embedded in daily life, and more intrusive.[12] In the modern age, companies' "business records" can comprise a detailed and encyclopedic dossier reflecting one's medical history, religious affiliation, political views, and intimate partnerships. Although this data is highly revelatory and its collection nearly ubiquitous, positive law has failed to comprehensively define, let alone address, intrusive practices in the private sector.[13]

In cases considering how the third-party doctrine applies to technology companies, courts have been reluctant to critique these business practices head-on. The Fourth Amendment is not an information privacy statute, and it clearly does not restrict the ways in which the private sector uses or gathers information.[14] Instead, as the appellate decisions on cell-site location tracking make plain, the fact that the records at issue were created and maintained for "legitimate business purposes" essentially disposed of the constitutional issue.[15]

The appellate decisions on cell-site location tracking that preceded *Carpenter* reflect this approach, uniformly holding that individuals lacked any expectation of privacy in their cell-site location information.[16] These

12. *See* Jack M. Balkin, Essay, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1169 (2017) ("[C]onsumer objects - including appliances, cars, and houses - collect information about you, listen to everything you are doing, and then report back to the corporation that manufactures and services them."); *see also* Natalie Ram et al., *Genealogy Databases and the Future of Criminal Investigation*, 360 SCIENCE 1078 (2018) (describing why, pursuant to the third party doctrine, the Fourth Amendment does not require a warrant for police to acquire genetic testing or matching information from direct-to-consumer databases).

13. *See generally* Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125 (2014); Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law* (U. of Colorado Law Legal Studies Research Paper No. 19-25 August 7, 2019), https://ssrn.com/abstract=3433922 [https://perma.cc/662K-WVMB].

14. *See* Kiel Brennan-Marquez, *Outsourced Law Enforcement*, 18 U. PA. J. CONST. L. 797, 797–98 (2016) (explaining that the Fourth Amendment does not apply to private searches conducted "without prodding, to assist the authorities").

15. Smith v. Maryland, 442 U.S. at 744 (1979); *see also* United States v. Carpenter, 819 F.3d 880, 887 (6th Cir. 2016) ("[T]he cell-site data—like mailing addresses, phone numbers, and IP addresses—are information that facilitate personal communications, rather than part of the content of those communications themselves."); In re United States for Historical Cell Site Data, 724 F.3d 600, 612 (5th Cir. 2013) ("[T]hese are the providers' own records of transactions to which it is a party."); *see also* United States v. Davis, 754 F.3d 1205, 1217 (11th Cir. 2014) (reasoning that cell phone users did not "voluntarily" disclose their cell-site location information), *rev'd en banc*, 785 F.3d 498, 511 (May 5, 2015) ("Davis can assert neither ownership nor possession of the third-party's business records he sought to suppress.").

16. *See, e.g.*, United States v. Graham, 824 F.3d 421, 430 (4th Cir. 2016) (en banc) ("As most cell phone users know all too well, proximity to a cell tower is necessary to complete these tasks."); In re United States for Historical Cell Site Data, 724 F.3d at 613 ("A cell service subscriber, like a telephone

decisions frequently invoked ideas about what members of society actually knew about the technology and business practices of cell phone service providers, asserting that cell phone users "know," "understand," or "are aware" that cell towers collect location information. These inquiries and assumptions about cell phone users' general understanding and knowledge are integral to Fourth Amendment doctrine, even if they appear unfounded on empirical evidence about consumer knowledge.[17] As Professor Tokson has previously written, knowledge plays a "central role" in Fourth Amendment doctrine.[18] If an individual "knowingly exposes" information to the public, she cannot have an expectation of privacy in that information; the government's acquisition or use of it is not a Fourth Amendment search.[19]

When courts determine whether an expectation of privacy is "reasonable," and thus whether a search occurred, they frequently look to what Professor Tokson has called "societal" or "collective knowledge."[20] But the approach propounded by the appellate courts is particularly notable because it emphasized not the general interests or knowledge of "society" at large, but rather those of cell phone users and subscribers.[21] As the Fifth Circuit described it in 2013,

> "[b]ecause a cell phone user makes a choice to get a phone, to select a particular service provider, and to make a call, and because he knows that the call conveys cell site information, the provider retains this information, and the provider will turn it over to the police if they have a court order, he voluntarily conveys his cell site data each time he makes a call."[22]

Thus, what a firm chooses to do, as a business matter, would constrain the constitutional rights of its customers. The problem with this traditional approach is that it is blind to actual inequalities in law, politics, and the market.[23] The obvious imbalance of power between the cell service

---

user, understands that his cell phone must send a signal to a nearby cell tower in order to wirelessly connect his call."); United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (en banc).

17. Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society"*, 42 DUKE L.J. 727, 743 (1993) ("[T]he Supreme Court has frequently refused to consider empirical information, or has given it short shrift."); Tokson, *supra* note 3, at 177 ("[T]he majority of cell phone users do not know that their cell phone provider collects their location data, and roughly 15% of users affirmatively believe that their data is not collected.").

18. Tokson, *supra* note 3, at 141.

19. Katz v. United States, 389 U.S. 347, 351–52 (1967).

20. Tokson, *supra* note 3, at 151–52.

21. *See also* Carpenter v. United States, 138 S. Ct. 2206, 2229 (2018) (Kennedy, J., dissenting) (emphasizing that cell phone customers lack "any meaningful interest" in and "any practical control" over location records).

22. In re United States for Historical Cell Site Data, 724 F.3d 600, 614 (5th Cir. 2015).

23. *See* K. Sabeel Rahman, *Domination, Democracy, and Constitutional Political Economy in the New Gilded Age: Towards a Fourth Wave of Legal Realism?*, 94 TEX. L. REV. 1329, 1335 (2016) ("The

provider and the consumer—an imbalance that anybody who has tried to negotiate a cell phone contract would recognize—was irrelevant.[24] This imbalance is not limited to retail interactions between consumers and providers; as Frank Pasquale has pointed out, big tech companies can lobby far more effectively than their competitors, and certainly enjoy higher status in the U.S. Congress than criminal defendants.[25] In short, this approach essentially deferred to the power of private enterprise, recognizing that the business and technological realities of how a service is structured can dramatically affect privacy and allowing those realities to, in turn, empower the government as well.[26]

The majority opinion in *Carpenter* steered in a different direction, emphasizing not the interests of individuals as cell phone subscribers, but rather the interests of society as a whole. The opinion opened with a reminder of the decision's importance to the general public, pointing out that the number of active cell phone service accounts in the United States exceeds the nation's population.[27] Rather than looking to the "terms of [Carpenter's] contracts"[28] with his cell service providers in order to determine whether Mr. Carpenter had a reasonable expectation of privacy in his location records, the Court recast the inquiry into social expectations more broadly. The opinion suggested that American *society* had a reasonable expectation that law enforcement could not—and would not—

problem with this approach to constitutionalism is that what looks on the surface like the fairness and equality of market ordering in effect overlooks, and thus perpetuates, underlying disparities in power, capacity, and opportunity that shape these transactions.").

24. *See* Scott Skinner-Thompson, *Reclaiming the Right to Future Tense*, L. & POL. ECON. BLOG (Sept. 4, 2019), https://lpeblog.org/2019/09/04/reclaiming-the-right-to-future-tense/ [https://perma.cc/Z59Y-9MBZ] ("Lengthy and unreadable adhesion contracts that force us to surrender any remaining claim to privacy . . . tak[e] advantage of the limited resources we have to consume much less contest these terms-of-service.").

25. FRANK PASQUALE, BLACK BOX SOCIETY 311 (2016).

26. *See, e.g.*, WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 51 (2018) ("Because design can allocate power to people and industries, it is inherently political . . . . To not address design is to sanction the power of creators to determine the context in which people make decisions."); SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 480–81 (2019) (asserting that U.S. scholars focus on "Fourth Amendment doctrine as it circumscribes the relationship *between individuals and the state* . . . [t]he problem is that even expanded protections from the state do not shield us from the assault on sanctuary wrought by instrumentarian power and animated by surveillance capitalism's economic imperatives"); *cf.* ELIZABETH ANDERSON, PRIVATE GOVERNMENT: HOW EMPLOYERS RULE OUR LIVES (AND WHY WE DON'T TALK ABOUT IT) 40 (2017) (describing most modern workplaces as "communist dictatorships" and asking, "Should we not subject these forms of government to at least as much critical scrutiny as we pay to the democratic state?").

27. Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018) ("There are 396 million cell phone service accounts in the United States—for a Nation of 326 million people.").

28. *Id.* at 2235 (Alito, J., dissenting).

"secretly monitor and catalogue every single movement" an individual made, regardless of what the market might support.[29]

By repeatedly highlighting the rights of the general public—rather than the interests and understandings of the public as cell phone subscribers—*Carpenter* foregrounded the important political and social interests implicated by digital surveillance.[30] Concern about the government's "near perfect surveillance" capabilities, the Court reasoned, rendered the location-tracking in *Carpenter* different from the government's acquisition of ordinary third-party records.[31] The constant acquisition of cell-site location information from 400 million mobile devices in the United States made it possible for law enforcement to "travel back in time" to investigate any suspect.[32] In the language of technology, the business model of cell service providers made it possible to investigate "at scale."[33] And the falling costs of cell phone location surveillance, which "is remarkably easy, cheap, and efficient compared to traditional investigative tools[,]" only aggravated the Court's concerns that it was not just Mr. Carpenter's privacy that was implicated in *Carpenter*, "but also everyone else's."[34]

While the Court readily admits in *Carpenter* that digital surveillance has become cheap and easy, precisely *because* it is enabled and empowered by the private sector, it fails to fully acknowledge the degree to which private sector and government surveillance are entwined and enmeshed.[35] Put another way, the Court's laissez-faire attitude toward private sector data collection has created a rich source of information for law enforcement, yet goes hand in hand with stringent limitations on government conduct.[36] Of course, as the Fourth Amendment does not apply to the private sector, this

29. *Id.* at 2217; *see also* Orin S. Kerr, *Implementing Carpenter*, 7 (U.S.C. Law Legal Studies Paper No. 18–29 Dec. 14, 2018), https://ssrn.com/abstract=3301257 [https://perma.cc/BVJ2-RZW7] ("*Carpenter* asks a different question: Has technology changed expectations of *what the police can do*?").

30. *See, e.g.*, Katherine Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 744 (2008); Neil Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 388–89 (2008).

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

32. *Id.*

33. *Cf.* Julie E. Cohen, *Scaling Trust and Other Fictions*, L. & POL. ECON. BLOG (May 29, 2019), https://lpeblog.org/2019/05/29/scaling-trust-and-other-fictions/#more-2442 [https://perma.cc/4U95-RY6G] (highlighting the challenge of "governing data-driven algorithmic processes that operate in real time, immanently, automatically, and at scale").

34. *Carpenter*, 138 S. Ct. at 2218–19.

35. *See id.*

36. *See id.* at 2217, 2219. In this way, the Court's approach—preserving individual liberty and "choice" in the area of privacy, while "in disregard of the legally constituted structural setting in which these choices take place"—runs parallel to its approach in other areas of constitutional law. *See generally* David Singh Grewal & Jedediah Purdy, *Law & Neoliberalism*, 77 L. & CONTEMP. PROBS. 1, 15 (2014).

line makes sense.[37] But the Court appears blind to the unique affordances that digital technology, and the profusion of private-sector data collection in particular, provide to law enforcement and government agencies.[38]

2. KNOWLEDGE IS POWER

Digital surveillance has proven to be both cheap and easy in more than one sense. *Carpenter* also expressed unease about the secrecy and surreptitious nature of warrantless digital surveillance.[39] Secrecy threatens to undermine the effectiveness of checks on law enforcement because the public lacks any real opportunity to mobilize against abusive practices. The *Carpenter* Court noted that the cost and physical limitations that had previously constrained law enforcement's ability to conduct long-term surveillance were falling by the wayside as digital technology evolved.[40] As Justice Sotomayor had noted in her *Jones* concurrence, digital tracking compounds these concerns because its surreptitious nature also lowers the costs of surveillance by avoiding public engagement, scandal, and backlash—interests that the private sector also largely shares.[41]

Not only is compelled disclosure low-cost in a financial sense—because it piggybacks on existing business practices by compelling the disclosure of information that would exist anyway[42]—but because it proceeds in secret, and avoids the kind of "community hostility" that has traditionally served as a check on law enforcement.[43] The classic view, as the Fifth Circuit had put it in 2013, was that the remedy for overbroad surveillance power was "in the market or the political process: in demanding that service providers do away with such records (or anonymize them) or in lobbying elected representatives to enact statutory protections."[44] But compelled disclosure of business records occurs behind closed doors, and resists the longstanding view that the "political process" will constrain law enforcement when it overreaches.

Blind faith in the political process also ignores the ways in which our institutions have been designed, or are in fact operating, to shield critical

37. *See Carpenter*, 138 S. Ct. at 2213.

38. *Id.* at 2220.

39. *Id.* at 2217–18; *see* United States v. Jones, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring).

40. *Carpenter*, 138 S. Ct. at 2217–18 ("[C]ell phone tracking is remarkably easy, cheap, and efficient . . . .").

41. *Jones*, 565 U.S. at 415–16 (Sotomayor, J., concurring). *But see* Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 99 (2018) (arguing that the private sector constrains government surveillance through litigiousness, proceduralism, and policy mobilization).

42. *See generally* ZUBOFF, *supra* note 26.

43. Illinois v. Lidster, 540 U.S. 419, 424–25 (2004); *Jones*, 565 U.S. at 415–16 (Sotomayor, J., concurring).

44. In re United States for Historical Cell Site Data, 724 F.3d 600, 615 (2013).

information about compelled disclosure from the public. The disparities between compelled disclosure and search warrant practice in federal courts illustrate how key documents about digital surveillance are systematically kept out of the public eye. The Stored Communications Act does not require that law enforcement notify the target of an electronic search warrant.[45] In other words, the decision of whether the target will be notified rests entirely with the communications service providers.[46] But service providers are often bound by court orders commanding them not to notify the target of a search.[47] And local rules often presumptively embed secrecy into their frameworks and procedures for docketing electronic surveillance materials.[48] In contrast, while applications and orders for "compelled disclosure" have long been cloaked in secrecy, search warrants have historically been public.[49] In federal court, applications for search warrants are filed with the court clerk and routinely unsealed after a search has been executed.[50] The rules governing physical searches require that the target of a search warrant must be given notice of a search.[51]

The result is that, as *Carpenter* suggested, the "compelled disclosure" framework is far less transparent than physical searches. In recent months, several litigants have sought to change that. In a current case pending before the D.C. Circuit, the Reporters Committee for Freedom of the Press ("RCFP") and journalist Jason Leopold are seeking to unseal key documents—including docket numbers, applications for surveillance, and court orders authorizing surveillance—with respect to investigations that have already concluded.[52] The Northern District of California recently denied a similar application to unseal key information about electronic surveillance dockets, applications, and orders, reasoning that the kind of transparency the petitioners sought would require the investment of "significant manpower and public resources."[53] And in the Ninth Circuit,

45. 18 U.S.C. § 2703(b)(1)(A) (2019). *See, e.g.*, In re United States, 665 F. Supp. 2d 1210, 1221–22 (D. Or. 2009) (concluding that, "when the property to be seized is in the possession of a third party," the Stored Communications Act and Fourth Amendment require only notice to the third party); Memorandum from Chief Justice Lamberth (D.C. Cir.), In re Search Warrant for Email Account, 946 F. Supp. 2d 67 (D.D.C. 2013), http://images.politico.com/global/2013/05/20/lamberthrosen.html [https://perma.cc/R62J-FL5J].

46. *See, e.g.*, Office of Legal Education, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 133 (2009), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf [https://perma.cc/B2MC-VWZG].

47. *See* 18 U.S.C. § 2705(b) (2019) (setting out requirements for separate nondisclosure order).

48. Hannah Bloch-Wehba, *Exposing Secret Searches: A First Amendment Right of Access to Electronic Surveillance Orders*, 93 WASH. L. REV. 145, 162–64 (2018).

49. *Id.*

50. *See id.* at 168–69 (discussing First Amendment right of access to search warrant materials).

51. FED. R. CRIM. P. 41; *see also* Jonathan Witmer-Rich, *The Rapid Rise of Delayed Notice Searches, and the Fourth Amendment "Rule Requiring Notice"*, 41 PEPP. L. REV. 509, 571 (2014).

52. Leopold v. United States, No. 18-5276 (D.C. Cir. argued Sept. 17, 2019).

53. *In re* Granick, 388 F. Supp. 3d 1107, 1120–21 (2019).

the American Civil Liberties Union and the Electronic Frontier Foundation are seeking access to a judicial opinion that reportedly concerns the Department of Justice's effort to hold Facebook in contempt of court after it refused to provide technical assistance in wiretapping its Messenger service.[54] In that case, although the dispute has been widely reported, not even the docket number is known to the public.[55]

At first glance, concerns about secrecy appear to be no more than a minor theme in *Carpenter*. But the disparities between digital and physical search warrant practice only underscore the importance of the *Carpenter* Court's effort to adopt a common, privacy-oriented approach to defining a "search."[56] Against this background, the Court's imposition of the warrant requirement does more to vindicate public values than it might initially appear. By rejecting the notion that the warrant requirement "simply does not apply when the Government acquires records using compulsory process,"[57] the Court also called into question the longstanding formal distinction between the procedural requirements of "compelled disclosure" and those of a "traditional search," opening additional avenues for democratic oversight.[58]

The Court's re-envisioning of the line between "compelled disclosure" and a "traditional search" thus not only elevates the substantive standard for digital surveillance, but also has the potential to promote new forms of transparency for law enforcement, and to align practice for digital and physical searches. Yet, these changes have proven to be slow. Consider the case brought by the RCFP and Jason Leopold, which aptly illustrates how some courts have remained convinced, even after *Carpenter*, that compelled disclosure is qualitatively different than "traditional searches." The district court reasoned that digital search warrants are "functionally unlike" their physical counterparts, because of differences in the method of execution, and the potential for a recipient to move to quash before a search is executed.[59] The opinion also inaptly describes the Electronic Communications Privacy Act as a "statutory framework that broadly

54. *EFF, ACLU v. DOJ - Facebook Messenger unsealing*, ELEC. FRONTIER FOUND., https://www.eff.org/cases/eff-aclu-v-doj-facebook-messenger-unsealing [https://perma.cc/MGX7-V8VU] (last visited Dec. 1, 2019).

55. *Id.*

56. *See* Tokson, *supra* note 1 at 5–6 (describing how the Court's "focus on the privacy harms caused by pervasive digital surveillance suggests that it is these harms, rather than the extent of consumer disclosure to third parties, that will primarily determine the scope of the Fourth Amendment going forward").

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

58. In re Leopold, 300 F. Supp. 3d 61, 88 (D.D.C. 2018).

59. *See In re Leopold*, 300 F. Supp. 3d at 88–89.

prioritizes law enforcement's need for secrecy over the public's interest in transparency."[60]

If anything about *Carpenter* is clear, it is the Court's rejection of the notion that "digital is different," that digital searches are by definition less intrusive (or more consensual) than physical ones, or that as a categorical matter, a separate set of rules ought to apply to compelled disclosure. Yet, the RCFP case helps to explain why *Carpenter* alone will not discipline digital searches to public opinion. Widespread secrecy prevents judges from understanding new technologies of surveillance, impedes lawmakers from acting on new privacy threats, and keeps social movements from coalescing and advocating for change. Despite *Carpenter*'s "blockbuster" victory for privacy, democratic institutions remain ill-equipped to monitor, scrutinize, and oversee demands for compelled disclosure or digital searches more generally.

III. CONCLUSION

I agree with Professor Tokson that *Carpenter*'s shift away from the formulaic inquiry into whether an individual has formally or voluntarily yielded a privacy interest is cause for celebration. I also agree that *Carpenter*'s emphasis on privacy should suggest that the use of pole cams, and compelled disclosure of web histories and smart home data are "searches" in the constitutional sense.

But as technology companies continue to routinely gather, repackage, and sell information to law enforcement, the appetite for third-party surveillance will continue to grow. Consider one example from last year, when *Forbes* reported that the FBI had obtained a "reverse search warrant" compelling Google to disclose "all users of its services who'd been within the vicinity" of several robberies in Portland, Maine.[61] The story was particularly concerning in light of an Associated Press report that Google continued to track users' location even after they had turned tracking off.[62]

On one level, the Google case illustrates how *Carpenter*'s logic has been applied in new settings—the FBI did, after all, obtain a search warrant to compel disclosure of the information. But on a deeper level, the case also illustrates the continuing dependency of law enforcement on the wealth of

60. *Id.* at 87.

61. Thomas Brewster, *To Catch A Robber, The FBI Attempted An Unprecedented Grab For Google Location Data*, FORBES (Aug. 15, 2018), https://www.forbes.com/sites/thomasbrewster/2018/08/15/to-catch-a-robber-the-fbi-attempted-an-unprecendeted-grab-for-google-location-data/#24fc80e3741d [https://perma.cc/V6FN-VL5J].

62. Ryan Nakashima, *Google Tracks Your Movements, Like it or Not*, ASSOCIATED PRESS (Aug. 13, 2018), https://apnews.com/828aefab64d4411bac257a07c1af0ecb [https://perma.cc/RJ5H-YCRA].

information generated and held by private enterprise. As *Carpenter* suggested, warrantless surveillance threatens to become undemocratic when law enforcement operates "at scale" and behind closed doors.

Yet, *Carpenter* does little to address law enforcement's appetite for this information, an issue that will certainly remain problematic in the years to come. The warrant requirement seems like quaint protection against a surveillance economy that presents law enforcement with an all-you-can-eat buffet of particularly detailed information. In this context, legislative constraints, democratic oversight, and transparency will prove particularly essential for a proportionate response to warrantless surveillance at scale.