DEFINING THE PRIVACIES OF LIFE: LOWER COURT TRENDS IN THE WAKE OF *CARPENTER*

Tiffany Chen†

I. INTRODUCTION

When the Supreme Court announced its *Carpenter v. United States* decision in June 2018,[1] many scholars and journalists lauded the opinion as a groundbreaking victory for privacy. The decision "chose to bring the Fourth Amendment into the digital future and protect against growing technologically enhanced police surveillance powers," wrote Professor Andrew Ferguson.[2] *Slate* writer Mark Joseph Stern perceived *Carpenter* as a "far-reaching decision," even an "earthquake in Fourth Amendment law," one that could "dramatically . . . expand[] the scope of the Fourth Amendment" and "provide[] vital new protections to the vast majority of Americans."[3] Numerous other commentators similarly predicted that *Carpenter* would have wide-ranging consequences for digital privacy; American Civil Liberties Union staff attorney Nathan Freed Wessler, for example, remarked that this "groundbreaking update to privacy rights" "open[ed] the door to the protection of many other kinds of data generated by popular technologies."[4]

The last year,[5] however, has seen little of the "widespread implications" so anticipated by observers.[6] Thus far, lower courts have repeatedly

DOI: https://doi.org/10.15779/Z38RF5KG63

† J.D., 2021, University of California, Berkeley, School of Law.

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

2. Andrew Ferguson, *Future-Proofing the Fourth Amendment*, HARV. L. REV. BLOG (June 25, 2018), https://blog.harvardlawreview.org/future-proofing-the-fourth-amendment.

3. Mark Joseph Stern, *A Historic Victory for Privacy*, SLATE (June 22, 2018, 11:41 AM), https://slate.com/news-and-politics/2018/06/carpenter-v-united-states-supreme-court-rules-fourth-amendment-protects-cell-phone-location-records-in-an-opinion-by-chief-justice-john-roberts.html.

4. Nathan Freed Wessler, *The Supreme Court's Groundbreaking Privacy Victory for the Digital Age*, FREE FUTURE (June 22, 2018, 2:30 PM), https://www.aclu.org/blog/privacy-technology/location-tracking/supreme-courts-groundbreaking-privacy-victory-digital-age.

5. This Note was written in 2020, so "the last year" refers to the year 2019.

6. Megan L. Brown, Matthew J. Gardner, Kathleen E. Scott & Vesna K. Harasic-Yaksic, Carpenter v. United States*: The Supreme Court's Recent Decision Will Have Widespread Implications for the Collection of Digital Information by Law Enforcement*, WILEY REIN LLP NEWS & INSIGHTS (June 25, 2018), https://www.wiley.law/alert-Carpenter_v_United_States_The_Supreme_Courts_Recent_Decision_Will_Have_Widespread_Implications

emphasized *Carpenter*'s own admission that its "decision [wa]s a narrow one," and generally declined to extend the holding to data outside of the cell site location information (CSLI) discussed in *Carpenter*.

These lower courts were correct not to broaden *Carpenter* in the last year, because these cases' fact patterns have not yet presented digital technologies at their most invasive. However, as law enforcement's surveillance techniques become increasingly sophisticated and intrusive, courts should heed *Carpenter*'s warnings and find Fourth Amendment violations whenever a "seismic shift[] in digital technology" invades the "privacies of life."[7]

This Note will analyze the last year's post-*Carpenter* decisions and highlight emerging surveillance technologies that may lead to Fourth Amendment violations in the near future. Parts II and III will provide background for *Carpenter*, with Part II discussing the Fourth Amendment as applied to the digital age, and Part III describing the legal and factual lead-up to the decision. Part IV will summarize the *Carpenter* ruling itself. Part V will then analyze lower court decisions announced in the year since, covering cases on police use of telephone pole cameras, internet protocol (IP) addresses, Global Positioning System (GPS) devices, and home Internet of Things (IoT) devices. The penultimate Part VI will introduce a new law enforcement practice on the horizon—big data database tracking—and argue that courts should hold that this technique violates the Fourth Amendment. Finally, Part VII will conclude with some observations on other actors in the digital privacy space who may contribute to *Carpenter*'s broadening in the near future.

II. THE FOURTH AMENDMENT

The Fourth Amendment of the U.S. Constitution grants citizens "the right . . . to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[8] The Amendment further states that this right "shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[9] As the *Carpenter* Court noted, the Amendment was adopted for two key purposes: first, to "secure 'the privacies of life' against 'arbitrary power' "; and second, " 'to place obstacles in the way of a too permeating police surveillance.' "[10]

7. *Carpenter*, 138 S. Ct. at 2214.
8. U.S. CONST. amend. IV.
9. *Id.*
10. *Carpenter*, 138 S. Ct. at 2214 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886) and United States v. Di Re, 332 U.S. 581, 595 (1948)).

Courts' Fourth Amendment analyses generally rest upon the *Katz* standard, which asks "whether a person invoking its protection can claim . . . a 'reasonable' . . . 'expectation of privacy' that has been invaded by government action."[11] In order to constitute a Fourth Amendment violation under this test, an act must satisfy two elements. First, an aggrieved individual must demonstrate that they had a subjective expectation of privacy that was infringed by the act; second, this subjective expectation must be "one that society is prepared to recognize as 'reasonable.' "[12]

Of course, as Justice Scalia was quick to note in *Kyllo v. United States*, "in the case of the search of the interior of homes"—an activity that falls squarely within the "persons, houses, papers, and effects" language of the Fourth Amendment—"there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that . . . is acknowledged to be *reasonable*."[13] Thus, if the government action clearly constitutes an intrusion into citizens' homes and does not use technology "in general public use," then the conduct will, per *Kyllo*, be considered a search, and will not require a full *Katz* analysis.[14]

In the last couple of centuries, technological improvements have, as Professors Susan Freiwald and Stephen Smith observed, "inevitably present[ed] new tools for the criminally minded" and created novel questions for Fourth Amendment applicability.[15] As a result, the legislature and judiciary have repeatedly, to borrow Professor Orin Kerr's term, pursued "equilibrium-adjustment"[16]—i.e., readapted the law to address these new technologies, from telegraph messaging, to pole cameras, to GPS devices. The advent of location tracking devices in the late twentieth century—including CSLI collection, the basis of the Supreme Court's landmark *Carpenter* ruling—constituted one such development.

III. THE PATH TO *CARPENTER*

In the 1970s, a pair of Supreme Court cases—*United States v. Miller* and *Smith v. Maryland*—articulated the concept at the heart of *Carpenter*: the third

11. United States v. Knotts, 460 U.S. 276, 280 (1983) (quoting Smith v. Maryland, 442 U.S. 735, 740 (1979)).

12. Smith v. Maryland, 442 U.S. 735, 740 (1979) (quoting Katz v. United States, 389 U.S. 347, 361 (1967)).

13. Kyllo v. United States, 533 U.S. 27, 34 (2001).

14. *Id.* at 34, 40.

15. Susan Freiwald & Stephen Wm. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 205 (2018).

16. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 476 (2011).

party doctrine.[17] *Miller* concerned a criminal defendant's bank records; his banks had supplied law enforcement with these materials upon receiving grand jury subpoenas.[18] In light of the fact that "all of the documents obtained . . . contain[ed] only information voluntarily conveyed to the banks," the Court reasoned that the defendant had no legitimate expectation of privacy in his bank records.[19] To support this conclusion, the Court articulated a concise definition of the third party doctrine: "[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose."[20] Given this doctrine, then, the Court held that the government's actions did not constitute a search under the Fourth Amendment.[21]

The Court upheld this doctrine a few years later in *Smith*.[22] Here, the third party in question was a telephone company: law enforcement officials installed a pen register at the company's central offices without a warrant to track the numbers that a criminal suspect used to call a robbery victim.[23] Citing *Miller*, the Court again applied the third party doctrine and found that the police had not conducted a Fourth Amendment search.[24] "When [the defendant] used his phone," the Court observed, "[he] voluntarily conveyed numerical information to the telephone company and . . . assumed the risk that the company would reveal to police the numbers he dialed."[25]

Given this doctrine, one can understand why courts and law enforcement officials at first believed that warrantless retroactive CSLI collection did not violate the Fourth Amendment. After all, cell phone users did turn their location information over to third parties, i.e., their wireless carriers.[26] Thus, starting in the late 1990s, law enforcement agencies began compelling service providers to supply retroactive CSLI based on showings required by 18 U.S.C. § 2703(d) (a provision of the Stored Communications Act which, by

17. *See* United States v. Miller, 425 U.S. 435, 443 (1976); *Smith*, 442 U.S. at 744.
18. *Miller*, 425 U.S. 435, 437–38 (1976).
19. *Id.* at 442.
20. *Id.* at 443.
21. *Id.* at 446.
22. *See* Smith v. Maryland, 442 U.S. 735, 744 (1979).
23. *Id.* at 737–38.
24. *Id.* at 744.
25. *Id.*
26. *See id.*; United States v. Miller, 425 U.S. 435, 443 (1976).

this time, mandated a "specific and articulable facts" threshold far less stringent than the probable cause standard for warrants).[27]

By the late 2000s, however, several federal magistrate judges had begun to reject these orders; after all, neither Congress nor the Supreme Court had weighed in on the new CSLI surveillance regime.[28] On appeal, circuit courts did not split and instead uniformly found no reasonable expectation of privacy in CSLI records in light of the third party doctrine.[29]

These decisions carried on for several years, until, in 2017, the Supreme Court disregarded the lack of circuit split and granted *certiorari* to review a Sixth Circuit decision on the issue: *Carpenter v. United States*.[30]

IV. THE *CARPENTER* DECISION

In *Carpenter*, law enforcement obtained over one hundred days of defendant Carpenter's CSLI from his wireless carriers under the Stored Communications Act.[31] In total, the police gathered 12,898 location points recording Carpenter's movements, averaging 101 data points per day.[32] According to the government, these CSLI records "clinched the case"; at trial, an FBI agent produced maps showing Carpenter's cell phone close to four of his charged robberies.[33] Carpenter was eventually convicted of all but one of his firearm counts.[34]

On appeal, the Sixth Circuit stayed true to the circuit courts' previous decisions and affirmed Carpenter's sentence under the third party doctrine.[35] After all, the court explained, "any cellphone user who has seen her phone's signal strength fluctuate must know that, when she places or receives a call, her phone 'exposes' its location to the nearest cell tower."[36]

The Supreme Court granted certiorari for the case and disagreed with the Sixth Circuit. "Technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes," the Court noted, and judges must continue to adjust Fourth Amendment readings so as

27. Freiwald & Smith, *supra* note 15, at 212.
28. *Id.*
29. *Id.* at 215–16. *See* Smith v. Maryland, 442 U.S. 735, 744 (1979); *Miller*, 425 U.S. at 443.
30. Freiwald & Smith, *supra* note 15, at 216.
31. Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).
32. *Id.*
33. *Id.* at 2213.
34. *Id.*
35. *Id.*
36. United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016).

not to leave citizens " 'at the mercy of advancing technology.' "[37] Here, CSLI collection represented a "seismic shift[] in digital technology," one that gave law enforcement "detailed, encyclopedic, and effortlessly compiled" information that effectively amounted to "tireless and absolute surveillance."[38] The data disclosed in this case, the Court warned, "provide[d] an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations' "—i.e., the same "privacies of life" that the Fourth Amendment was originally adopted to protect.[39] Also, the Court carefully pointed out, this information was not truly voluntarily given; cell phones were now "indispensable to participation in modern society," and "apart from disconnecting the phone from the network, there [wa]s no way to avoid leaving behind a trail of location data."[40] Given the uniquely intrusive nature of CSLI, then, the Court refused to extend the third party doctrine to this novel technology and held that accessing seven or more days of CSLI records constituted a Fourth Amendment search.[41]

Importantly, however, the Court tempered this finding with a caveat. "[O]ur decision today," it emphasized, "is a narrow one."[42] The majority was careful to list the types of data that the decision did *not* address: real-time CSLI; "tower dumps" showing specific cell sites' data over a given time period; "conventional surveillance techniques . . . such as security cameras"; business records containing location information; and collections involving national security or foreign policy.[43] However, the Court did implicitly acknowledge that its decision extended to GPS data.[44] At various turns, it observed that the "accuracy of CSLI [wa]s rapidly approaching GPS-level precision," and that "CSLI data [wa]s less precise than GPS information," effectively stating that GPS information collection was even more likely to constitute a Fourth Amendment search than CSLI access.[45]

In the immediate aftermath of *Carpenter*'s June 2018 decision, many scholars perceived the case as a landmark ruling that would drastically change

37. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoting Kyllo v. United States, 533 U.S. 27, 35 (2001)).

38. *Id.* at 2216–19.

39. *Id.* at 2217.

40. *Id.* at 2220.

41. *Id.* at 2217.

42. *Id.* at 2220.

43. *Id.*

44. *Id.* at 2210; *see also* United States v. Jones, 565 U.S. 400 (2012) (finding that the government's installation and tracking of a GPS device on the defendant's car constituted a Fourth Amendment search).

45. *Carpenter*, 138 S. Ct. at 2210.

the landscape of digital Fourth Amendment cases. "Oceans of ink have been spilled by those worried about how the dramatic expansion of technologically fueled corporate surveillance of our private lives automatically expands police surveillance, too," Professor Paul Ohm wrote in December 2018.[46] As such, *Carpenter* was "the opinion most privacy law scholars and privacy advocates ha[d] been awaiting for decades."[47] Others agreed and predicted that *Carpenter* would provoke significant changes to the Fourth Amendment legal landscape. For *New York Times* reporter Adam Liptak, the case "ha[d] implications for all kinds of personal information held by third parties, including email and text messages, internet searches, and bank and credit card records"; for Sidley Austin attorneys Christopher Fonzone, Kate Heinzelman, and Michael Roberts, the decision "ha[d] potentially dramatic consequences not only for the government, but also for private industry holders of data."[48] Evidently, then, stakeholders had high hopes that lower courts would soon broaden the *Carpenter* decision to other forms of digital data outside of CSLI. Such has not been the case, however, in the year since the decision.

V. LOWER COURT DECISIONS IN THE YEAR SINCE *CARPENTER*

In 2019, lower courts have taken the Supreme Court's word and largely interpreted *Carpenter* as a "narrow" decision.[49] These rulings have been reasonable thus far because their fact patterns have not yet implicated *Carpenter*-level privacy issues, but police officers will soon use—indeed, have already used—alarmingly invasive techniques that *will* amount to the same "tireless and absolute surveillance" so feared by *Carpenter*.[50] As this Part will delineate, the technologies used in the last year's cases each have the potential to breed practices that expose the "privacies of life" and violate the Fourth Amendment.[51]

46. Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 358, 362 (2019).

47. *Id.*

48. Adam Liptak, *In Ruling on Cellphone Location Data, Supreme Court Makes Statement on Digital Privacy*, N.Y. TIMES (June 22, 2018), https://www.nytimes.com/2018/06/22/us/politics/supreme-court-warrants-cell-phone-privacy.html; Christopher Fonzone, Kate Heinzelman & Michael Roberts, Carpenter v. United States*: A Revolution in Fourth Amendment Jurisprudence?*, 4 PRATT'S PRIVACY & CYBERSECURITY LAW REPORT 283, 283 (Nov./Dec. 2018).

49. *See Carpenter*, 138 S. Ct. at 2220.

50. *See id.* at 2218.

51. *See id.* at 2214.

Future courts should continue to address *Carpenter*'s two core inquiries: (1) whether the methods used in the case constituted one of the "seismic shifts in digital technology" that *Carpenter* so feared, and (2) whether the activities at hand invaded the same "privacies of life" that *Carpenter* was so concerned with protecting.[52] In answering these questions, judges should readily adopt the *Carpenter* Court's forward-looking approach: in Kerr's words, the ruling "seem[ed] more interested in where the technology [wa]s thought to be going" than the specific facts of the case.[53] Thus, going forward, judges should remain vigilant and extend *Carpenter* where necessary.

Each Section of this Part will discuss a type of digital data that has been addressed by courts in the past year: (A) pole cameras, (B) GPS devices, (C) IP addresses, and (D) home smart technology. In each Section, this Note will first summarize the last year's decisions for that data type and then consider the data type's future privacy implications.

A. POLE CAMERAS

First and perhaps most predictably, courts have largely remained loyal to the Supreme Court's assertion that *Carpenter* did not "call into question conventional surveillance techniques and tools, such as security cameras."[54] For example, in *United States v. Kay*, the U.S. District Court for the Eastern District of Wisconsin found that, "unlike the new technology addressed in *Carpenter*," law enforcement's pole camera surveillance did not constitute a Fourth Amendment search.[55] The defendant argued that such camera footage constituted the same "too permeating police surveillance" feared by the *Carpenter* Court, and he emphasized that he had a reasonable expectation that his home would not be constantly monitored by the police.[56] In response, the court stressed *Carpenter*'s status as a "limited decision" on a "new phenomenon" and observed that pole cameras had been used for decades.[57] It added that these cameras remained stationary in public spaces, so they were "unlikely to provide the same 'intimate window' into the person's life [that *Carpenter*'s CSLI collection could], revealing his 'political, professional,

52. *See id.*

53. Orin Kerr, *Understanding the Supreme Court's* Carpenter *Decision*, LAWFARE BLOG, (June 22, 2018, 1:18 PM), https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision.

54. *See Carpenter*, 138 S. Ct. at 2220.

55. United States v. Kay, No. 17-CR-16, 2018 U.S. Dist. LEXIS 141615, at *7 (E.D. Wis. Aug. 21, 2018).

56. *Id.* at 5.

57. *Id.* at 7 (quoting *Carpenter*, 138 S. Ct. at 2216).

religious, and sexual associations.' "[58] As such, the court concluded that law enforcement's actions had not violated the Fourth Amendment.[59]

The same district court ruled similarly in *United States v. Tirado*, which the court reconsidered in light of the *Carpenter* decision.[60] Here, too, the defendants challenged law enforcement's use of pole camera surveillance outside of their residences.[61] The court again emphasized the *Carpenter* Court's note that its opinion did not "call into question conventional surveillance . . . such as security cameras," and again asserted that the pole cameras at issue had been in use for decades.[62] Further, though the defendants had drawn on *Carpenter*'s fears to argue that the surveillance "permit[ted] a detailed chronicle of a person's activities," the court was unconvinced.[63] After all, the court reasoned, the cameras never captured footage from inside the homes themselves; thus, the court found that defendants had "fail[ed] to explain how such surveillance provides the same aggregate amount of a person's life, revealing his 'political, professional, religious, and sexual associations' [as CSLI could]."[64]

It is worth noting, however, that a state court recently deviated from *Kay* and *Tirado* and extended *Carpenter* to a case where law enforcement conducted pole camera surveillance for an extended, continuous period of time. In November 2019's *People v. Tafoya*, the Colorado Court of Appeals found that police's long-term, constant use of a pole camera directed at a suspect's house constituted a Fourth Amendment search.[65] In this case, officers streamed and recorded footage of the area around the defendant's home, including regions behind his privacy fence, for over three months.[66] The court acknowledged that many other courts, like the *Kay* and *Tirado* court, did not consider "the nature, continuity, and extended duration of police observation" relevant to this Fourth Amendment analysis and likely would not have found a Fourth Amendment search here.[67] Nevertheless, this court disagreed; the judge here considered these factors, especially the duration of observation, to be "extremely relevant."[68] Here, then, the

58. *Id.* (quoting *Carpenter*, 138 S. Ct. at 2217).
59. *Id.*
60. United States v. Tirado, No. 16-CR-168, 2018 U.S. Dist. LEXIS 141605, at *7 (E.D. Wis. Aug. 21, 2018).
61. *Id.* at 7.
62. *Id.* at 5–6 (quoting *Carpenter*, 138 S. Ct. at 2220).
63. *Id.* at 7.
64. *Id.*
65. *People v. Tafoya*, 2019 COA 176 (Colo. App. Nov. 27, 2019).
66. *Id.* ¶ 6.
67. *Id.* ¶ 33.
68. *Id.* ¶ 35.

surveillance's three-month length infringed on the suspect's reasonable expectation of privacy.[69] As the court observed, even if a neighbor could peer through the suspect's privacy fence and see all that this pole camera revealed, it would still be highly improbable that he or she would stand in place for three months; similarly, a helicopter or drone would not be able stay in the air above the backyard for three months.[70] The court therefore concluded that the warrantless, three-month-long surveillance of the defendant's home curtilage violated the Fourth Amendment.[71]

Given current pole camera surveillance practices, lower courts have been correct in their general reluctance to extend *Carpenter* to these "conventional surveillance techniques."[72] Today, most pole cameras are installed by the government and remain stationary in public spaces, so the recordings available from these devices do not usually amount to *Carpenter*'s "detailed chronicle of a person's physical presence compiled every day, every moment."[73] The *Kay* and *Tirado* cases both heavily emphasized these facts in their discussions.[74] To the *Tafoya* court, of course, this surveillance does rise to *Carpenter*-level intrusiveness when conducted constantly for over three months; this distinction is reasonable, because three months' worth of footage reveals far more than a day's worth.[75] These opinions were thus all understandable given the present nature of pole cameras.

However, law enforcement has begun to augment these cameras with increasingly sophisticated technologies, and soon even these seemingly harmless "conventional" cameras may provide "an intimate window into a person's life."[76] For instance, camera surveillance could quickly constitute an intrusion on the "privacies of life" if these cameras are equipped with facial recognition technology.[77] Such a case will likely appear in the near future, since the United States is, in the words of *MIT Technology Review*'s Angela Chen, "smack in the middle of an era when cameras on the corner can

69. *See id.*
70. *Id.* ¶¶ 47–48.
71. *Id.* ¶ 51.
72. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).
73. *See id.*
74. *See id.*; United States v. Kay, No. 17-CR-16, 2018 U.S. Dist. LEXIS 141615, at *7 (E.D. Wis. Aug. 21, 2018); United States v. Tirado, No. 16-CR-168, 2018 U.S. Dist. LEXIS 141605, at *7 (E.D. Wis. Aug. 21, 2018).
75. *See Tafoya*, 2019 COA 176.
76. *See id.*
77. *See Carpenter*, 138 S. Ct. at 2220.

automatically recognize passersby."[78] While facial recognition is not yet a ubiquitous feature in pole cameras, law enforcement in regions such as Orlando, Florida, and Washington County, Oregon, have already piloted this software on street surveillance cameras.[79]

One can only imagine the numerous "privacies of life" that will be intruded upon in a future where nearly every pole camera is equipped with facial recognition technology. Armed with this software, the police could effortlessly follow a person through the same "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, [and] the criminal defense attorney" that *Jones* feared GPS data would expose.[80] Indeed, *Carpenter*'s warning about CSLI might soon apply to camera surveillance, too: "Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible."[81] So-called traditional technologies like pole cameras therefore may themselves experience "seismic shifts in technology" and lend themselves to Fourth-Amendment-violating practices in the near future.[82]

Additionally, the fact, emphasized by *Kay*, that pole cameras have been used for decades should have no bearing on Fourth Amendment analyses.[83] After all, any technology, no matter how invasive, will eventually become a "conventional" technique that has been in use for decades.[84] The focus instead should be on whether such cameras would intrude upon the sensitive privacies *Carpenter* wished to protect.

Thus, the *Kay*, *Tirado*, and *Tafoya* courts were reasonable in their decisions applying *Carpenter* to pole camera surveillance in the last year. Going forward, courts should remain cautious and keep *Carpenter*'s key inquiries in mind as police officers begin to implement facial recognition software.[85]

---

78. Angela Chen, *This is How You Kick Facial Recognition Out of Your Town*, MIT TECH. REV. (Oct. 4, 2019), https://www.technologyreview.com/s/614477/facial-recognition-law-enforcement-surveillance-private-industry-regulation-ban-backlash.

79. Matt Cagle & Nicole Ozer, *Amazon Teams Up with Government to Deploy Dangerous New Facial Recognition Technology*, FREE FUTURE (May 22, 2018 10:00AM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazon-teams-government-deploy-dangerous-new.

80. *See Carpenter*, 138 S. Ct. at 2220; United States v. Jones, 565 U.S. 400, 415 (2012) (quoting People v. Weaver, 12 N.Y.3d 433, 441–42 (2009)).

81. *See Carpenter*, 138 S. Ct. at 2219.

82. *See id.* at 2214.

83. *See* United States v. Kay, No. 17-CR-16, 2018 U.S. Dist. LEXIS 141615, at *7 (E.D. Wis. Aug. 21, 2018).

84. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

85. *See id.* (quoting Northwest Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944)).

B. GPS DEVICES

Lower courts have followed *Carpenter*'s observations on GPS data's intrusiveness and extended the ruling to GPS information collection. For example, in *United States v. Diggs*, the U.S. District Court for the Northern District of Illinois held that detectives' collection of GPS data violated the Fourth Amendment.[86] Law enforcement officials did not themselves install the GPS tracking device in this case.[87] Instead, they accessed retroactive GPS information spanning over a month from a device installed on the defendant's vehicle by a previous owner.[88] The court identified this data as "fit[ting] squarely within the scope of the reasonable expectation of privacy identified by the *Jones* concurrences and reaffirmed in *Carpenter*"; the records did, after all, supply the same level of "detailed, encyclopedic, and effortlessly compiled" information as the *Carpenter* CSLI, and certainly "provide[d] an intimate window into a person's life."[89] The court thus found that the government had indeed infringed upon the defendant's reasonable expectation of privacy and violated the Fourth Amendment.[90]

This court properly extended *Carpenter* to law enforcement's collection of GPS tracking data. The *Diggs* court was correct to observe that GPS information "fit[s] squarely within the scope of the reasonable expectation of privacy."[91] In fact, as the *Carpenter* Court commented, GPS data is currently even *more* precise than CSLI—GPS can locate an individual within fifteen feet, while CSLI can only estimate to a range of one-half to two miles—and so supplies an even more "detailed, encyclopedic, and effortlessly compiled" record of a person's movements.[92]

C. IP ADDRESSES

Thus far, courts have also declined to extend the *Carpenter* ruling to IP address information collection. Judges comparing IP addresses to CSLI have focused on: (1) the fact that IP addresses are not logged as frequently as CSLI, and (2) the additional steps that law enforcement agents must take even after receiving an IP address to determine the user's identity and location.

86. United States v. Diggs, 385 F. Supp. 3d 648, 655 (N.D. Ill. 2019).
87. *Id.* at 650.
88. *Id.*
89. *Id.* at 653 (quoting *Carpenter*, 138 S. Ct. at 2216–18) (internal quotations omitted).
90. *Id.*
91. *Id.*
92. *See Carpenter*, 138 S. Ct. at 2216–18 (internal quotations omitted); *see also id.* at 2225 (Kennedy, J., dissenting).

In *United States v. Hood*, the First Circuit determined that the police's IP address information collection did not implicate the specific concern noted in *Carpenter* and so did not constitute a Fourth Amendment search.[93] In this case, law enforcement accessed the recent IP addresses associated with an account on Kik, a smartphone messaging application.[94] Officials then gathered location information on the IP addresses from the digital communications providers controlling them and subsequently found the defendant.[95] The defendant challenged this warrantless IP address data collection, contending that the act was analogous to the CSLI in *Carpenter* since it allowed officials to access his exact location when he logged on to Kik.[96] The defendant further argued that "[t]he notion that anytime one accesses the internet from their cell phone, they are effectively providing the police a specific record of their whereabouts, [wa]s in direct contrast to society's expectations."[97] However, the First Circuit was unconvinced and declined to find the police's activities to be a Fourth Amendment search for two reasons. First, unlike CSLI, which was recorded every time a person received a call, text message, or email and even during automatic application updates, IP address data was only generated when a user "ma[de] the affirmative decision to access a website or application."[98] Second, the IP address data "d[id] not itself convey any location information" and was "merely a string of numbers associated with a device," while CSLI immediately revealed a person's location "without any independent investigation."[99]

The First Circuit continued in this vein in another decision the same month: *United States v. Morel*.[100] Here, image-hosting site Imgur provided law enforcement with the IP address associated with certain images uploaded to Imgur's servers; officials then learned the IP address owner's identity from Comcast.[101] The defendant—the owner of the IP address—called on *Carpenter* in his argument, arguing that the ruling had "effected a sea change [sic] in the law of reasonable expectation of privacy, and he [wa]s the beneficiary of that change."[102] The court rejected this contention, noting the

93. United States v. Hood, 920 F.3d 87, 94 (1st Cir. 2019).
94. *Id.* at 88–89.
95. *Id.*
96. *Id.* at 91–92.
97. *Id.* (internal quotations omitted).
98. *Id.* at 92.
99. *Id.*
100. United States v. Morel, 922 F.3d 1, 4 (1st Cir. 2019).
101. *Id.* at 9.
102. *Id.* at 8.

same two reasons mentioned by the *Hood* opinion. "IP address information of the kind and amount collected here," the court concluded, "simply does not give rise to the concerns identified in *Carpenter*."[103]

The U.S. District Court for the District of Rhode Island reached the same holding in *United States v. Monroe*.[104] Here, law enforcement gathered the IP addresses of devices that had downloaded certain illicit files via a Georgia-based internet file sharing service (FSS).[105] Agents then learned the IP addresses' owner's—i.e., the defendant's—identity from an internet service provider.[106] The court, in a discussion similar to the First Circuit's observations in *Hood* and *Morel*, asserted that the collected IP address information "was not an 'exhaustive chronicle' of [the defendant's] physical or digital activities," since it "c[ould] only provide 'the location at which one of any number of computer devices may be deployed, much like a telephone number can be used for any number of telephones.' "[107] As such, the IP addresses themselves did not immediately reveal the user's identity and served only as "one link held by a third party in a chain of information that may lead to a particular person," with none of *Carpenter*'s "minutely detailed, historical portrait of 'the whole of [a person's] physical movements.' "[108] The court therefore ruled that the defendant did not have a reasonable expectation of privacy in the data collected, so the police's activities did not count as a Fourth Amendment search.[109]

Courts have properly declined to apply *Carpenter* in their IP address data opinions thus far, but they may need to find Fourth Amendment violations as fact patterns change in the near future. *Hood*, *Morel*, and *Monroe* each distinguished IP addresses from CSLI by arguing that IP addresses were not logged nearly as frequently as CSLI, and that IP addresses were multiple steps removed from the user's identity and location.[110] These decisions were appropriate given current law enforcement's limited access to IP address information in these instances. However, if law enforcement's IP address surveillance becomes more comprehensive, courts should carefully reevaluate

103. *Id.* at 9.
104. United States v. Monroe, 350 F. Supp. 3d 43, 49 (D.R.I. 2018).
105. *Id.* at 44.
106. *Id.*
107. *Id.* at 48.
108. *Id.* at 49.
109. *Id.*
110. *See Hood*, 920 F.3d at 91–92; United States v. Morel, 922 F.3d 1, 8 (1st Cir. 2019); United States v. Monroe, 350 F. Supp. 3d 43, 48–49 (D.R.I. 2018).

the distinctions they drew in *Hood*, *Morel*, and *Monroe*—IP addresses could actually expose just as much of the "privacies of life" as CSLI.[111]

Police officers could feasibly access IP address information via two different avenues. In the first, more limited method, law enforcement officials could discover an illicit online behavior—e.g., a forum post, a file upload, an instant message—and reach out to the platform (and, later, the relevant internet service provider) for information on the specific user involved. Officers thus may gain IP addresses, physical addresses, and names through this practice, but their entire query is restricted to the particular illegal incident they uncovered. In the second, far broader approach, police officers could target the entire history of a criminal suspect's online activity. They can gather the suspect's IP addresses from their internet service provider, translate the IP addresses into a domain name, and then identify the websites the suspect was visiting in a given time period.

In the last year, lower courts' Fourth Amendment IP address rulings have involved only the first technique. Police officers in these cases accessed solely the narrowest information on a particular user in a particular situation. Law enforcement only collected the recent IP addresses associated with a specific Kik account in *Hood*; the IP addresses associated with specific images uploaded to Imgur in *Morel*; and the IP addresses of devices that had downloaded specific files via an FSS in *Monroe*.[112] Because these fact patterns addressed isolated moments in a person's online actions and not their internet history in its entirety, none of these law enforcement practices amounted to the "tireless and absolute surveillance" discussed in *Carpenter*.[113] Thus, these lower courts were correct not to broaden *Carpenter*, because the police's actions were not nearly invasive enough to implicate the "privacies of life."[114]

Lower courts *should* extend *Carpenter*, however, if law enforcement begins to adopt the second method and track an IP address's entire browsing history. The courts will also need to reexamine their CSLI-versus-IP-address distinctions in the process.

First, the *Hood*, *Morel*, and *Monroe* courts use the wrong framing when they contend that IP address information is not as privacy-intrusive as CSLI because it is recorded less frequently than CSLI. Such a comparison focuses on how often IP addresses reveal the *physical* location of users; however, the proper equivalent analogy would be how often IP addresses reveal users'

111. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).
112. *See Hood*, 920 F.3d at 88–89; *Morel*, 922 F.3d at 8; *Monroe*, 350 F. Supp. 3d at 48–49.
113. *See Carpenter*, 138 S. Ct. at 2218.
114. *See id.* at 2217.

virtual location. Just as a person's CSLI "tracks nearly exactly the movements of its owner" in the physical world, IP addresses track nearly exactly the movements of their owners in the *virtual* world—every website a user visits sees that user's IP address.[115] To again cite *Jones*'s concerns, IP addresses could thus easily expose the online equivalents of a user's "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, [and] the criminal defense attorney"; for example, these addresses could show that the user visited the websites of any of these places or visited forum pages covering sensitive topics related to criminal defense or strip clubs.[116] Through this *virtual* location lens, then, IP addresses reveal location just as, if not more, frequently than CSLI does, and could no doubt invade the "privacies of life" as well.[117]

The courts' other distinction that IP addresses are merely "one link . . . in a chain of information that may lead to a particular person" is similarly misguided.[118] These cases place too heavy an emphasis on the few additional steps law enforcement would need to take to ascertain an IP address owner's identity. Even more critically, the courts miss the fact that *Carpenter* still found a search even after acknowledging that the government could only "deduce a detailed log of Carpenter's movements" from CSLI "*in combination with* other information."[119] The additional steps are often negligible. Once law enforcement obtains an IP address, it need only reach out to the service provider controlling that address to learn the address's owner. Indeed, the Office of the Privacy Commissioner of Canada recently reported that one could "build a detailed profile of a person or group associated with the IP address" by merely "carrying out . . . a simple test" of searching through public databases online, "no special equipment or software . . . needed."[120] Additionally, *Monroe*'s contention that IP address data "c[ould] only provide 'the location at which one of any number of computer devices may be deployed' " ignores the reality that many public IP addresses are shared by a small number of people.[121] Setting aside businesses and academic institutions—where internet users are probably less likely to engage in

115. *See id.* at 2218.

116. *See* United States v. Jones, 565 U.S. 400, 416 (2012) (quoting *Weaver*, 12 N.Y.3d at 441–42).

117. *See Carpenter*, 138 S. Ct. at 2220.

118. *See* United States v. Monroe, 350 F. Supp. 3d 43, 49 (D.R.I. 2018).

119. *See Carpenter*, 138 S. Ct. at 2218 (emphasis added).

120. Technology Analysis Branch of the Office of the Privacy Commissioner of Canada, *What an IP Address Can Reveal About You*, OFF. OF THE PRIVACY COMM'R OF CAN. (May 2013), https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip_201305.

121. *See Monroe*, 350 F. Supp. 3d at 48.

incriminating activities in the first place—home internet routers (which each have unique public IP addresses) usually have only a handful of regular users.[122] IP address information therefore is not merely one "link" in a long chain of clues leading to an individual; in many cases, it serves as a crucial, identifying segment of the chain.[123]

To conclude, then, while the *Hood*, *Morel*, and *Monroe* courts appropriately declined to broaden *Carpenter* to cover the fact patterns at issue, their reasoning may not hold water as police officials begin to track IP addresses' entire browsing histories. In today's increasingly digital age—when citizens spend perhaps the same amount of time surfing the internet as they do moving around in the physical world—IP address data has the potential to expose as much information as CSLI.

D. HOME IOT DEVICES

Courts have yet to consider home IoT device data, but the last year's opinions on government access to home public utility data provide some guidance on how courts may handle IoT in the future. For example, the Seventh Circuit's *Naperville Smart Meter Awareness v. City of Naperville* decision concerned a city government's collection of home electricity usage information.[124] The City of Naperville in this case entered all electricity-enabled Naperville homes into a mandatory smart-meter program that collected residents' energy-usage data at fifteen-minute intervals; the City then stored these records for up to three years.[125]

The *Naperville* court likened the program to law enforcement's CSLI collection in *Carpenter*.[126] In the court's words:

> 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 [as in

122. *See* Bradley Mitchell, *How Many Devices Can Connect to One Wireless Router*, LIFEWIRE (Apr. 15, 2020), https://www.lifewire.com/how-many-devices-can-share-a-wifi-network-818298 (observing that most home networks use a single wireless access point); Richard Fry, *The Number of People in the Average U.S. Household is Going Up for the First Time in Over 160 Years*, PEW RESEARCH CENTER (Oct. 1, 2019), https://pewresearch.org/fact-tank/2019/10/01/the-number-of-people-in-the-average-u-s-household-is-going-up-for-the-first-time-in-over-160-years (finding that there was an average of 2.63 people per household in the United States in 2018). Given these statistics, a single household router likely has around 2.63 regular users on average.

123. *See id.* at 49.

124. *See* Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 521 (7th Cir. 2018).

125. *Id.* at 524.

126. *Id.* at 527.

> *Carpenter*], . . . it also goes that a home occupant does not assume the risk of near constant monitoring by choosing to have electricity in her home.[127]

After all, "a choice to share data imposed by fiat is no choice at all."[128] Additionally, it noted, the "technology-assisted data collection" at issue, i.e., the smart-meter measurement of electricity usage, was both "not in general public use" and "at least as rich as that found to be a search in *Kyllo*."[129] As such, the court concluded, the City's activities were a search under the Fourth Amendment.[130]

Importantly, though, and unlike the other cases in this Note, the City here "conduct[ed] the search with no prosecutorial intent."[131] Only public utility employees, not law enforcement, accessed the data.[132] This fact, the court emphasized, "lessen[ed] an individual's privacy interest."[133] The government, meanwhile, did have a significant, legitimate interest in this information (for the sake of providing cheaper energy, promoting power efficiency, and helping grid stability), and only collected usage data at fifteen-minute intervals.[134] After balancing the lowered privacy interest against the government's legitimate interests and limited practices, the Seventh Circuit held that the act, while a search, was still a *reasonable* search that did not violate the Fourth Amendment.[135] Thus, *Naperville* provided a rather convoluted, inconclusive application of *Carpenter* principles.[136]

However, the *Naperville* opinion did cast light on *Carpenter*'s potential applicability to IoT device data.[137] In its acknowledgement of the search's reasonableness, the *Naperville* court warned that its finding "depend[ed] on the particular circumstances of this case," and if "a city [were] to collect the data at shorter intervals, [the court's] conclusion could change."[138] "Likewise," it added, "[the court's] conclusion might change if the data was more easily accessible to law enforcement or other city officials outside the

127. *Id.*
128. *Id.*
129. *Id.* at 526 (quoting Kyllo v. United States, 533 U.S. 27, 40 (2001)) (internal quotations omitted).
130. *Id.*
131. *Id.* at 527.
132. *Id.* at 528.
133. *Id.*
134. *Id.* at 526.
135. *Id.*
136. *See id.*
137. *Id.* at 529.
138. *Id.*

utility."[139] From these statements, then, the Seventh Circuit implied that, in the future, *Carpenter* may well extend to, say, cities' collection of electricity usage at ten-minute intervals or law enforcement's warrantless access to fifteen-minute-interval electricity usage data.[140]

As law enforcement inevitably begins to investigate IoT data in the future, courts should follow *Naperville*'s lead and keep *Kyllo* in mind.[141] With the recent advent of smart home devices such as Google Home and Amazon Echo, this issue will likely arise in courts soon. Once homes become fully wired with these devices, courts should continue to read police collection of transactional data (e.g., records showing when certain lights in the home are turned on or off) as Fourth Amendment searches that require a warrant.

One could easily argue that home IoT transactional data, like the *Naperville* smart meter program's electricity usage information, is also "at least as rich as that found to be a search in *Kyllo*."[142] Law enforcement agents in *Kyllo* merely used thermal images to detect infrared radiation from inside Kyllo's house.[143] Transactional usage data pulled from an IoT home device, meanwhile, could expose *Kyllo*-like infrared lights and much more; from the information, officials could glean when residents arrived at home, entered and left rooms, and went to sleep.[144] Further, as Justice Scalia stated, "in the case of the search of the interior of homes"—which certainly includes the collection of home device data—". . . there is a ready criterion . . . of the minimal expectation of privacy . . . acknowledged to be *reasonable*."[145]

Additionally, home IoT data could be likened to an equivalent of a person's cell phone in their home. Like the cell phone, which *Carpenter* described as "almost a 'feature of human anatomy' . . . [that] tracks nearly exactly the movements of its owner,"[146] a device tracking which lights are turned on in a home can reveal exactly which room a person was in at any time (indeed, it may even be more precise than a cell phone in these instances, since many people do not keep their cell phones with them at all times while at home). In light of *Kyllo* and even *Carpenter*, then, a court should readily conclude that access to home devices' transactional records would

139. *Id.*
140. *Id.*
141. *See id.* at 526; Kyllo v. United States, 533 U.S. 27, 40 (2001).
142. *See Naperville*, 900 F.3d at 526 (quoting *Kyllo*, 533 U.S. at 40) (internal quotations omitted).
143. *See Kyllo*, 533 U.S. at 29–30.
144. *See id.*
145. *See id.* at 34.
146. *See* Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

violate a citizen's reasonable expectation of privacy and so would constitute a Fourth Amendment search.

In response, law enforcement agencies may assert that people with home IoT technologies have voluntarily assumed the risk of having their data turned over to the police. While this claim may hold water today, it will likely become less and less effective as home IoT devices become increasingly ubiquitous. Fifty-nine percent of American adults surveyed in a 2018 Forrester Research report said they were interested in using a smart home device; as *New York Times* reporter Janet Morrissey observed in January 2019, "the soaring popularity of smart speakers . . . is starting to move the 'Smart Home' into mainstream America."[147] As the number of smart-device-wired homes grows, citizens will have increasingly compelling arguments that these devices, like the cell phones of *Carpenter*, are " 'such a pervasive and insistent part of daily life' that [owning] one is indispensable to participation in modern society."[148] Thus, in the near future, those with home IoT will likely be able to convincingly claim that they, like the residents of Naperville, do not " 'voluntarily "assume the risk" of turning over a comprehensive dossier of physical movements' " by having smart homes.[149]

As these smart home devices increase in prevalence, the government may invoke *Kyllo*'s requirement that the technology not be "in general public use."[150] However, this "general public use" qualification is a problematic standard for reasonable privacy assessments; indeed, it may, in the words of Derek Conom in the *Willamette Law Review*, prove to be a "potentially troublesome sliding scale of privacy that depends on how fast technology goes into general public use."[151] As Justice Stevens in his *Kyllo* dissent observed: "[T]his [general public use] criterion is somewhat perverse because it seems likely that the threat of privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available."[152] This concerning standard pulls the emphasis away from ordinary citizens' privacy expectations and instead focuses on potential privacy invaders' actions. The

147. Janet Morrissey, *In the Rush to Join the Smart Home Crowd, Buyers Should Beware*, N.Y. TIMES (Jan. 22, 2019), https://www.nytimes.com/2019/01/22/business/smart-home-buyers-security-risks.html.

148. *See Carpenter*, 138 S. Ct. at 2220 (quoting Riley v. California, 134 S. Ct. 2473, 2484 (2014)).

149. *See* Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 527 (7th Cir. 2018) (quoting *Carpenter*, 138 S. Ct. at 2220).

150. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001).

151. Derek T. Conom, *Sense-Enhancing Technology and the Search in the Wake of* Kyllo v. United States*: Will Prevalence Kill Privacy?*, 41 WILLAMETTE L. REV. 749, 761 (2005).

152. *See Kyllo*, 533 U.S. at 47 (Stevens, J., dissenting).

Kyllo majority claimed the *Katz* test supported this public use requirement—presumably because it believed people should expect police to employ widely-used surveillance technologies—but the majority failed to consider a future in which law enforcement uses technologies that citizens simply cannot prepare for or protect themselves against.[153] In *Naperville*'s words, "under *Kyllo* . . . even an extremely invasive technology can evade the warrant requirement if it is 'in general public use.' "[154] Citizens should not be at the whim of the general public's use of a surveillance technology, and courts should instead draw a hard line so that officials' handling of "extremely invasive technolog[ies]" would still constitute a Fourth Amendment search.[155]

Thus, even as smart home devices increase in prevalence over the coming years, courts should remain wary of law enforcement's access to these technologies' transactional data and continue to find that collection of such information constitutes a Fourth Amendment search.

VI. FUTURE TECHNOLOGIES RELEVANT TO *CARPENTER*

Law enforcement has begun to turn to big data surveillance in its tracking of citizens, and courts should be cautious and protective of citizens' privacy when adjudicating big-data-related Fourth Amendment cases. Big data mining—defined by Professor Adam Frank as "the machine-based collection and analysis of astronomical quantities of information"—can capture astonishingly intricate profiles of individuals' behaviors.[156] As they consider these cases, courts should keep the dangerously invasive potential of big data in mind, even if the particular facts at issue do not yet involve extremely sophisticated technology. The *Carpenter* Court, after all, "seem[ed] more interested in where the technology [wa]s thought to be going," and *Kyllo* asserted that Fourth Amendment rulings must take heed of more intrusive systems that are already in use.[157]

As an example, U.S. Immigration and Customs Enforcement (ICE) officials have begun to mine previously unrelated computer databases for data on every realm of citizens' lives. As a recent *New York Times* article reported: "[T]he business of deportation, like so much else in the modern

153. *See* Katz v. United States, 389 U.S. 353 (1967); *Kyllo*, 533 U.S. at 34–35.

154. *See Naperville,* 900 F.3d at 527.

155. *See id.*

156. Adam Frank, *A Brave New World: Big Data's Big Dangers*, NATIONAL PUBLIC RADIO 13.7 COSMOS & CULTURE (June 11, 2013 2:41 PM), https://www.npr.org/sections/13.7/2013/06/10/190516689/a-brave-new-world-big-datas-big-dangers.

157. Kerr, *supra* note 53; *see Kyllo*, 533 U.S. at 36.

world, has been transformed by the power of big data."[158] Under "relentless pressure from the White House to deport people," ICE agents have begun to "suck[] up terabytes of information from hundreds of disparate computer systems, from state and local governments, from private data brokers and from social networks . . . fusing little bits of stray information together into dossiers."[159] While immigrants are the main targets of these particular searches, "it's an increasingly trivial exercise to track any of us."[160] These two passages perfectly capture the precise facts that so concerned the Supreme Court in *Carpenter*.

First, this all-inclusive brand of tracking certainly "provide[s] an intimate window into a person's life, revealing . . . his 'familial, political, professional, religious, and sexual associations,' " like CSLI.[161] Indeed, in today's increasingly digital world, it arguably reveals an even more "comprehensive dossier," since it exposes every aspect of a person's online presence.[162] Also, as with CSLI, citizens cannot be said to have voluntarily consented to giving others this aggregated information. The internet is just as "indispensable to participation in modern society" as cell phones; in particular, social media is now inextricably tied to people's abilities to contact friends, read news, find jobs, and learn about the world around them.[163] Further, internet users probably do not quite understand the intrusive potential of big data, and while they may be aware of each individual social media platform's privacy implications, they likely have not yet imagined just how much an aggregation of *all* their social media accounts can expose about their personal behaviors and preferences.

Second, this type of all-encompassing tracking is just as "effortlessly compiled" as the CSLI in *Carpenter*.[164] The Supreme Court particularly feared the reality that CSLI was "remarkably easy, cheap, and efficient" and could happen "with just the click of a button."[165] The *New York Times* noted that ICE's immigrant tracking practices are "increasingly trivial."[166] For example, dozens of ICE officers have accounts on a "flexible search" computer

158. McKenzie Funk, *How ICE Picks Its Targets in the Surveillance Age*, N.Y. TIMES MAGAZINE, https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html (last updated Oct. 3, 2019).

159. *Id.*

160. *Id.*

161. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217, 2220 (2018).

162. *See id.*

163. *See id.* at 2220.

164. *See id.* at 2216.

165. *See id.* at 2218.

166. Funk, *supra* note 158.

interface known as Driver and Plate Search on which they run tens of thousands of searches "again and again, nearly every day at all times of day."[167] Like CSLI, these databases do not require officials to engage in lengthy stakeouts, search through piles of documents, or even leave their desks; instead, they can find vast troves of personal information on citizens "with just the click of a button."[168]

Finally, *Carpenter*'s concern with the "vast store of sensitive information" in a cell phone's "immense storage capacity" applies to ICE's use of big data tracking since in this case, the "store of sensitive information" is the internet itself.[169] In the realm of big data, no public record on the internet is safe from the government, and it is difficult to imagine something that has a more "immense storage capacity" than the internet itself.[170]

In the near future, these searches may be deemed even more intrusive and harmful with the addition of artificial intelligence (AI) algorithms. In July 2017, ICE announced the "Extreme Vetting Initiative," a project that aimed to evangelize "determinations via automation."[171] It referenced "partners whose algorithms could scan social media and other publicly available information" to "assess whether an immigrant was likely to become a 'positively contributing member of society'—or whether he or she intended 'to commit criminal or terrorist attacks.' "[172] This new initiative is particularly concerning given the reality that AI cannot currently be designed without biases. In the words of *MIT Technology Review*'s Karen Hao, "bias can creep in at many stages of the deep-learning process, and the standard practices in computer science aren't designed to detect it."[173] In November 2017, Google Translate announced that its AI algorithms were sexist; in October 2018, Amazon scrapped its attempts at using AI to screen potential applicants in light of the software's aversion to resumes that contained the word "women."[174] Not only, then, do ICE officers now practice the same "tireless and absolute surveillance" dreaded by *Carpenter*; they could soon also use this information to profile and discriminate against immigrants—who already

167. *Id.*
168. *See Carpenter*, 138 S. Ct. at 2218.
169. *See id.* at 2214.
170. *See id.*
171. Funk, *supra* note 158.
172. *Id.*
173. Karen Hao, *This is How AI Bias Really Happens—and Why It's So Hard to Fix*, MIT TECH. REV. (Feb. 4, 2019), https://www.technologyreview.com/s/612876/this-is-how-ai-bias-really-happensand-why-its-so-hard-to-fix.
174. Michael Li, *Addressing the Biases Plaguing Algorithms*, HARV. BUS. REV. (May 13, 2019), https://hbr.org/2019/05/addressing-the-biases-plaguing-algorithms.

suffer from a host of discrimination-related challenges—in frighteningly prejudiced ways.[175]

Suffice it to say, then, that government officials now can and *have* easily pulled together vast troves of previously decentralized data to create alarmingly thorough profiles of every citizen. Indeed, the same *New York Times* report on ICE techniques mentioned that "public records make clear that . . . other federal agencies" also engage in ICE-like practices.[176] As discussed above, these practices both implicate severe *Carpenter* concerns *and* may lead to discriminatory practices that harm vulnerable populations. As Justice Brandeis emphasized in *Olmstead v. United States*, courts should be wary as these "[s]ubtler and more far-reaching means of invading privacy have become available."[177] Judges should work to "ensure that the 'progress of science' does not erode Fourth Amendment protections" by readily extending *Carpenter* to big data surveillance cases.[178]

VII. CONCLUSION

In the year since the allegedly groundbreaking *Carpenter* decision, lower courts have been reluctant to extend the holding to forms of digital data not explicitly mentioned in the opinion. Judges have largely declined to apply the *Carpenter* exception to cases involving pole camera footage, IP address information, and home device data. The only type of data these courts have clearly extended *Carpenter* to include is GPS data, which the *Carpenter* Court referenced as being even more intrusive than CSLI.

However, these findings appear to be more a reflection of the specific facts at issue than an indication that courts will never extend *Carpenter* beyond retroactive CSLI. These courts were in fact correct to construe *Carpenter* narrowly given the less invasive methods utilized in the last year's cases. New surveillance techniques will inevitably proliferate in the coming years, though, so courts should continue pressing *Carpenter*'s key inquiries and seek to extend *Carpenter* in cases involving "seismic shifts in digital technology" that intrude upon "the privacies of life."[179]

Hope is not lost even if lower courts maintain their narrow *Carpenter* applications in the future; state legislatures may still forge ahead themselves and adopt privacy bills broadening *Carpenter*'s logic. Indeed, earlier this year,

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

176. Funk, *supra* note 158.

177. *See Carpenter*, 138 S. Ct. at 2223 (quoting Olmstead v. United States, 277 U.S. 438, 473–74 (1928)).

178. *See id.*

179. *See id.* at 2214, 2219.

Utah took a step in this direction with its Electronic Information or Data Privacy Act, which, with certain limited exceptions, requires law enforcement to obtain a warrant to access information shared with third parties.[180] This new bill may inspire other state legislatures to follow suit. Since Utah's law was voted into action, Maine and Illinois have enacted their own *Carpenter*-expanding privacy statutes.[181] Even if the judiciary fails to properly extend *Carpenter*, then, the legislature may still intervene and help cement *Carpenter* as "the opinion most privacy law scholars and privacy advocates have been awaiting for decades."[182]

Finally, even if both courts and state legislatures fail to broaden *Carpenter* to other invasive technologies, corporate actors may themselves push back on privacy-violating law enforcement requests. Google's Sensorvault records, for example, have been protected by Google's demands of law enforcement. In the last few years, law enforcement agents have accessed Sensorvault—an enormous database of detailed location data from iOS devices with Google Maps installed and most Android devices—to investigate, arrest, and convict citizens.[183] Notably, though, officers have issued warrants each time they review Sensorvault data—Google, then, is holding officers to its own standard and is itself defining Sensorvault access as a Fourth Amendment search that requires a warrant.[184] While investigators have told the *New York Times* that they do not request this kind of information from companies besides Google, the Sensorvault database sets an interesting—even promising—example of the potential corporate-side interventions to come.[185] Hopefully, future companies will follow in Google's footsteps and similarly require warrants for law enforcement officials seeking access to the "privacies of life."[186]

It is important to note, however, that *Carpenter*'s broadening may not be enough to protect citizens from all unreasonable privacy invasions by the

180. Cynthia Cole, Brooke Chatterton & Sarah Phillips, *Utah Blazes Trail with Law Shielding Data from Gov't Search*, LAW360 (Sept. 17, 2019 11:50AM), https://www.law360.com/articles/1198954/utah-blazes-trail-with-law-shielding-data-from-gov-t-search.

181. *Id.*

182. Ohm, *supra* note 46.

183. Jennifer Valentino-DeVries, *Tracking Phones, Google is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html.

184. Jennifer Lynch, *Google's Sensorvault Can Tell Police Where You've Been*, ELEC. FRONTIER FOUND. (Apr. 18, 2019), https://www.eff.org/deeplinks/2019/04/googles-sensorvault-can-tell-police-where-youve-been.

185. Valentino-DeVries, *supra* note 183.

186. *See* Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

police. The cases discussed in this Note did not contemplate what happens *after* police obtain a warrant for a Fourth Amendment search. What if there are data types that the police should not access under any circumstances, even with a warrant? Consider, for example, a Florida judge's recent approval of a warrant to search the database of GEDmatch, a consumer DNA site with nearly one million users.[187] These searches would affect "huge swaths of the population" outside of just site users; armed with this new forensic method, law enforcement would be able to identify individuals "even through distant family relationships."[188] With these warrants, police will thus have a free license to access millions upon millions of powerless, innocent citizens' DNA profiles, even if they have never used or heard of DNA consumer sites or have never spoken to the distant relative who did use the site.[189] As such, beyond *Carpenter*, there may still be searches so intrusive that law enforcement should never be able to conduct them, even with a warrant.

Carpenter may well find new life, then, in many different arenas—in courts, state legislatures, and even data-harvesting companies. The ruling could feasibly help protect citizens from "seismic shifts in digital technology" for years to come.[190] Extending *Carpenter* alone, though, may not be sufficient to protect citizens from invasive surveillance. As police techniques increase in sophistication over the coming years, judges and legislators should consider whether certain types of data should *never* be accessed by law enforcement, with or without a warrant.

187. Kashmir Hill & Heather Murphy, *Your DNA Profile is Private? A Florida Judge Just Said Otherwise*, N.Y. TIMES, https://www.nytimes.com/2019/11/05/business/dna-database-search-warrant.html (last updated Dec. 30, 2019).

188. *Id.*

189. *Id.*

190. *See Carpenter*, 138 S. Ct. at 2219.