Bend and Snap: Adding Flexibility to the *Carpenter* Inquiry

SHERWIN NAM*

The Supreme Court's decision in Carpenter v. United States*, which requires law enforcement to obtain warrants to access historical cell-site location information, raises new questions about the application of the Fourth Amendment to biometric technologies, such as facial recognition technology (FRT) and voice recognition technology (VRT). While "no single rubric definitively resolves which expectations of privacy are entitled to protection," this Note seeks to demonstrate that current applications of the rubric offered in* Carpenter *— considering voluntariness, invasiveness, comprehensiveness, ease of data collection, and retrospectivity — are inadequately flexible. To safeguard the private and intimate details that ongoing "seismic shifts in digital technology" continue to reveal, the courts need a bolder, more robust framework for Fourth Amendment protection. Using FRT and VRT as illustrative examples, this Note argues that analyses of reasonable expectations of privacy involving biometric technologies should recognize the right to anonymity as an integral part of the* Carpenter *inquiry.*

* Executive Managing Editor, Colum. J.L. & Soc. Probs., 2020–2021. J.D. Candidate 2021, Columbia Law School; B.A., University of California, Santa Barbara. The author thanks Professor Matthew Waxman for his invaluable advice during the writing process. The author expresses loving gratitude to his father, Julius Nam, for the countless hours and late nights spent discussing this Note. And special thanks to the editorial and executive boards of the *Columbia Journal of Law and Social Problems* for their helpful comments and edits.

I. INTRODUCTION

The Supreme Court's 2018 decision in *Carpenter v. United States*[1] has been widely recognized as one of the most significant Fourth Amendment decisions in the digital age.[2] It has been hailed as "an inflection point in the history of the Fourth Amendment[,]"[3] after which "we will be talking about what the Fourth Amendment means in pre-*Carpenter* and post-*Carpenter* terms."[4] *Carpenter* is undoubtedly significant, as it broke new ground in the constitutional right to privacy in electronic data. Not only did it reaffirm the reasonable-expectation-of-privacy standard of *Katz v. United States*,[5] it applied that standard to an altogether new category of data: historical cell-site location information (CSLI) — time-stamped geographical information that "cell phones convey to nearby cell towers"[6] by "dint of operation."[7] The *Carpenter* Court's reasoning, properly understood, employed a five-factor inquiry of voluntariness, invasiveness, comprehensiveness, ease of data collection, and retrospectivity.[8] Now, after *Carpenter*, law enforcement must obtain a warrant before acquiring historical CSLI from third-party telecommunications service providers.[9]

---

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

2. *See, e.g.*, Orin Kerr, *Implementing* Carpenter, LAWFARE (Dec. 17, 2018 11:36 AM), https://www.lawfareblog.com/implementing-carpenter [https://perma.cc/JHU2-BR7R] (calling *Carpenter* a "blockbuster" decision); Vania Mia Chaker, *Your Spying Smartphone: Individual Privacy is Narrowly Strengthened in* Carpenter v. United States, *the U.S. Supreme Court's Most Recent Fourth Amendment Ruling*, 22 J. TECH. L. & POL'Y 1, 1 (2018) (calling *Carpenter* a "landmark case"); Maddalena DeSimone, Note, *Can We Curate It? Why Luggage and Smartphones Merit Different Treatment at the United States Border*, 2019 COLUM. BUS. L. REV. 696, 707 (2019) (calling *Carpenter* a "landmark" case).

3. Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L & TECH. 357, 361 (2019).

4. *Id.*

5. Katz v. United States, 389 U.S. 347 (1967).

6. Stephanie Lacambra, *Cell Site Location Information: A Guide for Criminal Defense Attorneys*, ELEC. FRONTIER FOUND. (Mar. 28, 2019), https://www.eff.org/files/2019/03/28/csli_one-pager.pdf [https://perma.cc/XKC2-VLJL].

7. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

8. In *Carpenter*, the Court considered whether law enforcement's warrantless acquisition of the defendant's historical CSLI violated the Fourth Amendment. *See id.* at 2211. While not explicitly applying a formal, five-factor test, the *Carpenter* Court considered five standards grounded in the Court's precedents to find that Carpenter retained a reasonable expectation of privacy in his CSLI: voluntariness, invasiveness, comprehensiveness, ease of data collection, and retrospectivity. *Voluntary* conveyance of data was the underlying principle motivating the third-party doctrine cases and directly applied in *Carpenter*. *See id.* at 2216 (declining to extend Smith v. Maryland, 442 U.S. 735 (1979), and United States v. Miller, 425 U.S. 435 (1976), to historical CSLI as "not truly 'shared'"). Additionally, *invasions* into the intimate details that reveal the privacies of life remained front-and-center in

In reaching this landmark decision, the Court declined to extend the third-party doctrine of *Smith v. Maryland*[10] and *United States v. Miller*[11] to historical CSLI. Instead, *Carpenter* looked to Fourth Amendment principles embodied in *Kyllo v. United States*,[12] *Riley v. California*,[13] and *United States v. Jones*.[14] As it had in *Kyllo* and *Riley*, the *Carpenter* Court recognized that the Fourth Amendment must keep up with advances in surveillance and tracking technologies.[15] The *Carpenter* Court — in citing Justice Sonia Sotomayor's concurrence in *Jones* rather than the majority's property-based holding[16] — also recognized that the Fourth Amendment protects against more than just physical intrusions. Namely, the Court recognized the privacy interests at stake in historical CSLI concern intrusions into the intimate details of a person, including her "familial, political, professional, religious, and sexual associations."[17] As its reasoning shows, *Carpenter* was a

---

the *Carpenter* reasoning. *Id.* at 2217–18 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)); Riley v. California, 573 U.S. 373, 403 (2014)). The Court further reasoned that, as in *Jones*, the detailed, *comprehensive* record of the whole of the defendant's movements unconstitutionally intruded into Carpenter's reasonable expectations of privacy. *See id.* at 2217 (citing *Jones*, 565 U.S. at 430 (Alito, J., concurring); *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)). So too, the effortless compilation of the whole of a person's movements presented too pervading a power to go unchecked. *See id.* at 2216 ("Much like GPS tracking of a vehicle [in *Jones*], cell phone location information is detailed, encyclopedic, and *effortlessly compiled*.") (emphasis added)). Lastly, the *retrospective* nature of historical CSLI allowed the government to collect "a category of information otherwise unknowable." *Id.* at 2218. *See also infra* Part II.C.

9. *See Carpenter*, 138 S. Ct. at 2221 ("Before compelling a wireless carrier to turn over a subscriber's CSLI, the Government's obligation is a familiar one — get a warrant.").

10. 442 U.S. 735 (1979) (no reasonable expectation of privacy in records of dialed telephone numbers conveyed to telephone company).

11. 425 U.S. 435 (1976) (no reasonable expectation of privacy in financial records held by a bank).

12. 533 U.S. 27 (2001) (requiring a warrant for evidence captured on a thermal imager on the defendant's home).

13. 573 U.S. 373 (2014) (requiring a warrant for evidence taken from an arrestee's cell phone).

14. 565 U.S. 400 (2012) (requiring a warrant for evidence obtained from a GPS tracker placed on the suspect's car).

15. *See* Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018) ("As Justice Brandeis explained in his famous dissent, the Court is obligated . . . to ensure that the 'progress of science' does not erode Fourth Amendment protections.") (quoting Olmstead v. United States, 277 U.S. 438, 473–74 (1928) (Brandeis, J., dissenting)).

16. *See* Nicholas A. Kahn-Fogel, *Property, Privacy, and Justice Gorsuch's Expansive Fourth Amendment Originalism*, 43 HARV. J.L. & PUB. POL'Y 425, 450 (2020) ("In 2012, in *United States v. Jones*, the Court rehabilitated the Olmstead-era property framework, holding that a physical intrusion into a constitutionally protected area to gather information constitutes a search[.]").

17. *Carpenter*, 138 S. Ct. at 2217 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)) (internal quotation marks omitted).

product of the Court's willingness to consider technological advances and exercise flexibility in reasoning of Fourth Amendment challenges to warrantless acquisitions of electronic data.[18]

However, lower courts have rigidly applied the *Carpenter* factors,[19] both when addressing historical CSLI and other technologies.[20] The predominant trend has been to mechanically apply *Carpenter*'s factors without much consideration beyond the Court's own framing of each factor.[21] All the while, technological progress has raced forward, providing law enforcement an increasingly wide range of invasive surveillance tools at its disposal, including biometric technology.[22] As discussed below, the merger of traditional surveillance and biometrics poses novel questions regarding whether information unearthed from biometric surveillance would receive Fourth Amendment protection.[23] But so far, courts have shown little indication that they would extend *Carpenter* protection to biometric technologies such as facial recognition technology (FRT) and voice recognition technology (VRT) despite these technologies' capacity to reveal the kinds of intimate details the Fourth Amendment seeks to protect.[24]

This Note proposes that, for biometric information to receive Fourth Amendment protection similar to historical CSLI, courts should incorporate a right to anonymity — a right implicit in the expectation of privacy — into the *Carpenter* framework. Specifically, courts should consider the right to anonymity as part of *Carpenter*'s invasiveness factor. As some have argued, the right to anonymity is an embedded value in many of the Supreme Court's Fourth Amendment opinions.[25] This Note expands on these

18. *Id.* at 2214 ("For that reason, we rejected in *Kyllo* a 'mechanical interpretation' of the Fourth Amendment and held that use of a thermal imager to detect heat radiating from the side of the defendant's home was a search.") (quoting Kyllo v. United States, 533 U.S. 27, 35 (2001)).

19. *Id.* at 2234 (Kennedy, J., dissenting) (listing "intimacy, comprehensiveness, expense, retrospectivity, and voluntariness" as the five major considerations of the Court's "multifactor analysis").

20. *See infra* Part III.C.

21. *See infra* Part III.

22. *See infra* Part III.A–B.

23. *See infra* Part II.C.

24. *See infra* Part IV.A.

25. *See, e.g.*, Jeffrey M. Skopek, *Reasonable Expectations of Anonymity*, 101 VA. L. REV. 691, 761 (2015) (arguing that the Fourth Amendment protects reasonable expectations of anonymity); Christopher Slobogin, Symposium, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 217 (2002) (arguing that the Fourth Amendment provides a right to anonymity in public).

arguments, contending that the right to anonymity — that is, the right to privacy in information so intimate that it reveals identity — should be recognized in evaluating the right to privacy attached to information gathered through FRT, VRT, and other deanonymizing biometric technologies.[26] Unless courts construe the *Carpenter* factors to capture the right to anonymity, it is unlikely that the Fourth Amendment will remain adequately flexible to protect citizens from rapidly advancing surveillance technologies. Fortunately, doctrinal flexibility remains a foundational principle animating Fourth Amendment precedent.

Part II discusses the precedential background leading to the Supreme Court's decision in *Carpenter*. Part III then applies *Carpenter*'s reasoning — and that of its progeny — to the attributes of FRT and VRT. Finally, Part IV argues that recognizing the right to anonymity as an integral part of the *Carpenter* framework would allow for adequate Fourth Amendment protection of biometric information while remaining grounded in the Court's precedent.

II. THE *CARPENTER* COURT EXPANDS FOURTH AMENDMENT PROTECTION TO THE "DETAILED AND COMPREHENSIVE RECORD OF THE PERSON'S MOVEMENTS"

In *Carpenter*, the Supreme Court concluded that law enforcement's warrantless acquisition of seven days of historical CSLI constituted an unconstitutional search.[27] Chief Justice John Roberts, writing for the majority, declared that the Fourth Amendment's warrant requirement applied to historical CSLI stored by third-party telecommunications companies, Sprint and MetroPCS, because the cell phone user retained a reasonable expectation of privacy in the accumulated data that revealed "a comprehensive chronicle of the user's past movements."[28] Applying a five-factor inquiry,[29] the *Carpenter* Court reaffirmed the vitality of the "reasonable expectation of privacy" standard established in *Katz*[30] and

26. Myriad biometric technologies exist today, including gait-based identification systems, iris and retinal scans, and keystroke analysis, just to name a few. Because of their prevalence and widespread use, this Note focuses specifically on FRT and VRT.

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

28. *Id.* at 2211.

29. *Id.* at 2234 (Kennedy, J., dissenting) (listing "intimacy, comprehensiveness, expense, retrospectivity, and voluntariness" as the five major considerations of the Court's "multifactor analysis").

30. Katz v. United States, 389 U.S. 347 (1967).

extended Fourth Amendment privacy protection to "a detailed and comprehensive record of the person's movements," even though such records were in the possession of a third party.[31]

Section A details the doctrinal developments that led to *Carpenter*'s reaffirmation of *Katz*. Section B then introduces the third-party doctrine and explains its place within the Fourth Amendment tradition. Finally, Section C describes the significance of *Carpenter*'s reasoning in the digital age.

A. THE EVOLUTION OF THE REASONABLE EXPECTATION OF PRIVACY STANDARD

The Fourth Amendment states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[32] Traditionally, courts interpreted the Fourth Amendment under a property-based, trespass rule. Under this rule, the government conducts a search or seizure when "agents physically intrude on a suspect's private property for the purpose of obtaining information."[33] *Olmstead v. United States*[34] was "the quintessential expression of this model."[35] There, the Supreme Court held that law enforcement's wiretapping of telephone wires on public telephone poles did not constitute a search because "[t]here was no entry of the houses or offices of the defendants."[36] The Court adhered to *Olmstead* in ensuing decades.[37] However, in the 1960's, the Court began to expand Fourth Amendment protection to cases that did

31. *See Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting) ("[I cannot] fault the Court today for its implicit but unmistakable conclusion that the rationale of *Smith* and *Miller* is wrong; indeed, I agree with that."); *see also* Sharon Bradford Franklin, Carpenter *and the End of Bulk Surveillance of Americans*, LAWFARE (June 24, 2018 11:36 AM), https://www.lawfareblog.com/carpenter-and-end-bulk-surveillance-americans [https://perma.cc/4U86-66F4] ("The decades-old 'third-party doctrine[ ]' . . . has appropriately been confined to the pre-digital age scenarios in which it rose.").

32. U.S. CONST. amend. IV.

33. Peter C. Ormerod & Lawrence J. Trautman, *A Descriptive Analysis of the Fourth Amendment and the Third-Party Doctrine in the Digital Age*, 28 ALB. L.J. SCI. & TECH. 73, 78–79 (2018) (citation omitted).

34. 277 U.S. 438 (1928).

35. Kahn-Fogel, *supra* note 16, at 427.

36. *Olmstead*, 277 U.S. at 464.

37. *See* On Lee v. United States, 343 U.S. 747, 749–53 (1952); Goldman v. United States, 316 U.S. 129, 131–32, 135–36 (1942).

not always involve intrusions onto private property or the taking of physical property.[38]

In *Katz*, the Court repudiated what was left of the *Olmstead* framework and placed the right to privacy at the heart of the Fourth Amendment inquiry.[39] There, the Court held that law enforcement's electronic eavesdropping on the defendant's conversation in a public telephone booth constituted a search.[40] Writing for the majority, Justice Potter Stewart famously reasoned that "the Fourth Amendment protects people, not places."[41] But it was Justice John Marshall Harlan's concurrence, which the Court endorsed as *Katz*'s holding in subsequent cases,[42] that established reasonableness as the touchstone[43] of a Fourth Amendment search analysis. Under subsequent understandings of *Katz*, the government conducts a search if it intrudes on an expectation of privacy that "society is prepared to recognize as 'reasonable.'"[44] Decades later, in *Jones*, the Court clarified that the privacy-based reasonableness standard of *Katz* did not displace the property-based rule exemplified in *Olmstead*. Rather, the *Katz* rule "*added to*, not *substituted for*, the common-law trespass test."[45]

Amid criticism of the reasonable-expectation-of-privacy test as surveillance technologies advance,[46] the Court has expanded notions of reasonableness to apply to changing expectations of privacy. In 2001, the Court in *Kyllo* held that law enforcement's use of a thermal imager on the defendant's home violated his reasonable expectation of privacy.[47] There, the Court was concerned with the government's unchecked use of rapidly advancing surveillance technologies that erode constitutional guarantees of privacy in the "intimate details" of home activities.[48] The Court provided protection against the "[g]overnment's capacity to encroach upon areas

38. *See* Carpenter v. United States, 138 S. Ct. 2206, 2236–37 (2018) (Thomas, J., dissenting) (citing Silverman v. United States, 365 U.S. 505 (1961); Wong Sun v. United States, 371 U.S. 471, 485 (1963); Berger v. New York, 388 U.S. 41, 52-54 (1967)).

39. *See* Kahn-Fogel, *supra* note 16, at 427–28.

40. Katz v. United States, 389 U.S. 347, 359 (1967).

41. *Id.* at 351.

42. *See* Kahn-Fogel, *supra* note 16, at 427–28.

43. *See* Ohio v. Robinette, 519 U.S. 33, 34 (1996).

44. *Katz*, 389 U.S. at 360–61 (Harlan, J., concurring).

45. United States v. Jones, 565 U.S. 400, 409 (2012) (emphasis in original).

46. *See e.g.*, 1 W. LAFAVE, SEARCH AND SEIZURE § 2.1(d) (3d ed. 1996); Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173, 188 (1979); Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring).

47. Kyllo v. Riley, 533 U.S. 27, 40 (2001).

48. *See id.* at 34, 38–39.

normally guarded from inquisitive eyes[.]"[49] *Kyllo* is significant in two key respects. First, its decision sought to limit intrusions into intimate spaces by "prying government eyes."[50] Second, and more importantly, in considering the dangers of unchecked government use of advanced, sense-enhancing technology, the *Kyllo* Court reaffirmed a flexible Fourth Amendment, a principle underlying *Katz*.[51]

Subsequent opinions echoed *Kyllo*'s reasoning. In *Jones*, a 2012 decision, a unanimous Court held that the government's attachment of a GPS device to the defendant's car constituted a search.[52] In his concurrence, Justice Samuel Alito reasoned that advances in technology could affect a person's expectation of privacy as well as those that society are prepared to accept as reasonable.[53] In a separate concurrence, Justice Sonia Sotomayor expressed concerns that GPS monitoring could unduly invade a person's "familial, political, professional, religious, and sexual associations."[54] Two years later, the Court in *Riley* held that the government must obtain a warrant before examining the digital contents of an arrestee's cell phone, in large part because government access to modern cell phones' immense storage capacity would reveal "for many Americans the 'privacies of life[.]'"[55]

In 2018, the *Carpenter* Court relied heavily on *Riley* and Justice Sotomayor's concurrence in *Jones* to find a heightened expectation of privacy in a person's historical CSLI. *Riley* provided the *Carpenter* Court the basis for recognizing the enhanced degree to which cell phone technology especially implicates Fourth Amendment privacy concerns in contemporary life.[56] In formulating the standard for weighing the invasiveness of surveillance tools, *Carpenter* also incorporated Justice Sotomayor's associational-information concern in *Jones*.[57]

---

49. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (citing *Kyllo*, 533 U.S. at 34).

50. *Kyllo*, 533 U.S. at 37.

51. *See id.* at 35–36 ("We rejected such a mechanical interpretation of the Fourth Amendment in *Katz*[.] . . . Reversing that approach would leave the homeowner at the mercy of advancing technology — including imaging technology that could discern all human activity in the home.").

52. United States v. Jones, 565 U.S. 400, 413 (2012).

53. *See id.* at 427 (Alito, J., concurring).

54. *Id.* at 415 (Sotomayor, J., concurring).

55. Riley v. California, 573 U.S. 373, 375, 403 (2014) (citation omitted).

56. *See id.* at 403.

57. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (citing *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).

B. THE THIRD-PARTY DOCTRINE

Parallel to the evolution of the reasonable-expectation-of-privacy standard in Fourth Amendment jurisprudence was the emergence of the third-party doctrine. That doctrine, a post-*Katz* development in *Miller*[58] and *Smith*,[59] has stood for the proposition that a person loses Fourth Amendment protection for information voluntarily revealed to a third party because any expectation of privacy in such information is no longer reasonable.[60] In *Miller*, the Court held that the warrant requirement does not apply to bank records.[61] It concluded that bank records did not merit Fourth Amendment protection because they "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[62] Building upon *Miller*, the *Smith* Court held that the government did not need to obtain a warrant to search pen registers[63] — devices that record the numbers dialed on telephones. The Court determined that the defendant did not have any reasonable expectation of privacy in those numbers because he "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business."[64]

Carpenter signaled a significant break from the third-party doctrine by concluding that knowingly supplying cell phone location information to a third-party telecommunications company over time "does not make it any less deserving of Fourth Amendment protection," in light of "the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection."[65] The Court stated, without further elaboration, that it did not disturb *Smith* and *Miller* or "call into question *conventional* surveillance techniques and tools, such

58. 425 U.S. 435 (1976).

59. 442 U.S. 735 (1979); *cf. Carpenter*, 138 S. Ct. at 2216 ("The third-party doctrine largely traces its roots to *Miller*. . . . Three years later, *Smith* applied the [*Miller*] principles in the context of information conveyed to a telephone company.").

60. *See Smith*, 442 U.S. at 743 (holding that the defendant retained no reasonable expectation of privacy in voluntarily conveyed numerical information to the telephone company); *Miller*, 425 U.S. at 442 (holding that the defendant retained no reasonable expectation of privacy in financial information voluntarily conveyed to the bank in the ordinary course of business).

61. *See Miller*, 425 U.S. at 445.

62. *Id.* at 442.

63. *Smith*, 442 U.S. at 745–46.

64. *Id.* at 744.

65. Carpenter v. United States, 138 S. Ct. 2206, 2222, 2223 (2018).

as security cameras."[66] But what is "conventional" is changing.[67] The *Carpenter* Court recognized the limits of the third-party doctrine as it wrestled with what the right to privacy means in the digital age. Were the Court to hear a case addressing intimate and comprehensive biometric information produced by sophisticated technologies and held by third parties, *Carpenter* suggests that the third-party doctrine might not apply.

C. *CARPENTER* AND ITS IMPACT ON DIGITAL INFORMATION

Carpenter represents the Supreme Court's latest expansion of the reasonable-expectation-of-privacy standard to address advancing digital surveillance. Though the Court emphasized its holding as "narrow,"[68] the decision nonetheless opens new possibilities for extending Fourth Amendment protections to cover increasingly invasive surveillance technologies.

The specific issue in *Carpenter* was whether the government violated a cell phone user's reasonable expectation of privacy when it obtained his historical CSLI without a warrant.[69] There, the government obtained over 12,898 location points — an average of roughly 101 per day[70] with each point detailing the defendant's movements within about a two-mile radius.[71] Writing for the majority, Chief Justice Roberts found that the government's access of just seven days' worth of historical CSLI constituted a search.[72] In reaching its decision, the Court weighed five considerations: voluntariness, invasiveness, comprehensiveness, ease of data collection, and retrospectivity.[73] The Court reasoned that because cell phones were so "indispensable to participation in modern society,"[74] the user did not truly share his CSLI voluntarily to

66. *Id.* at 2220 ("Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or 'tower dumps[.]'") (emphasis added). While the Court intended to limit the scope of its holding to only historical CSLI, its *reasoning* has nonetheless been applied in other contexts. *See infra* Part III.C.

67. *See infra* Part I.C.

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

69. *See id.* at 2211.

70. *See id.* at 2212.

71. *See id.* at 2226 (Kennedy, J., dissenting).

72. *See id.* at 2219.

73. *See id.* at 2234 (Kennedy, J., dissenting) (listing "intimacy, comprehensiveness, expense, retrospectivity, and voluntariness" as the five major considerations of the Court's "multifactor analysis"); *see also supra* note 8.

74. *Carpenter*, 138 S. Ct. at 2220 (citing Riley v. California, 573 U.S. 373, 385 (2014)).

MetroPCS or Sprint.[75] Much like the GPS tracking in *Jones*, historical CSLI has the power to invade into the "familial, political, professional, religious, and sexual associations[ ]"[76] that comprise the privacies of life.[77] This "tireless and absolute surveillance"[78] allowed the government to track every movement of every day for extended periods of time, a reach too comprehensive for the Court to permit without a warrant.[79] Moreover, this "effortlessly compiled" information showing the whole of a person's movements presents too worrisome a power to go unchecked.[80] And finally, the retrospective nature of historical CSLI allows the government to collect "a category of information otherwise unknowable."[81] Upon considering each factor, the Court reaffirmed the continuing vitality of the *Katz* standard and, in effect, opened additional potential avenues for Fourth Amendment protection for digital surveillance information.[82]

Carpenter thus signaled a significant deviation from the third-party doctrine[83] as it recognized "seismic shifts"[84] in the "depth, breadth, and comprehensive reach"[85] of evolving surveillance technology. Those shifts certainly involve the fusion of surveillance and biometric technology. Indeed, Chief Justice Roberts recognized such a merging of technology and personally identifiable information when he described the cell phone as "almost a 'feature of human anatomy.'"[86]

Biometric technology — like the increasingly ubiquitous FRT and VRT — translates intimate details of human anatomy into "detailed, encyclopedic, and effortlessly compiled" information.[87]

---

75. *See id.* at 2216–17.
76. *Id.* at 2217 (citation and internal quotation marks omitted).
77. *Id.* (citation omitted).
78. *Id.* at 2218.
79. *Id.* at 2218–19.
80. *See id.* at 2216, 2217, 2219.
81. *See id.* at 2218.
82. *See* Kahn-Fogel, *supra* note 16, at 426.
83. *See, e.g.*, Michael Gentithes, *The End of* Miller*'s Time: How Sensitivity Can Categorize Third-Party Data After* Carpenter, 53 GA. L. REV. 1039, 1067 (2019) (stating that *Carpenter* "all but buried" the third-party doctrine); Trevor Burrus & James Knight, Katz *Nipped and* Katz *Cradled:* Carpenter *and the Evolving Fourth Amendment*, 2018 CATO SUP. CT. REV. 79, 110 (2018) ("The third-party doctrine, as well as the *Katz* reasonable-expectation-of-privacy test, still stand on shaky doctrinal and theoretical grounds, and it's likely shakier now due to *Carpenter*.").
84. Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).
85. *Id.* at 2223.
86. *Id.* at 2218 (citation omitted).
87. *Id.* at 2216, 2219.

Facial recognition is currently integrated into airport surveillance systems throughout the world[88] and planned for implementation in concert venues[89] to replace once-conventional ticketing measures and to increase security.[90] Researchers at the University of California, Santa Barbara have developed a gait-based identification system using video-WiFi technology.[91] Voice recognition technology has already been developed into digital assistants like Siri, Alexa, and Google Assistant that constantly listen to user conversations.[92]

Further, technologies with tracking functions have become, like cell phones,[93] pseudo-appendages. These ubiquitous technologies thus add a biometric dimension even if the technology is not biometric in nature, because they remain on the user's person for the vast majority of the day. Apple Watches, Fitbits, and other smart watches have become indispensable extensions of smartphones, always leaving the home with their users. Recently, Amazon released Echo Frames, Echo Buds, and Echo Loop to take virtual assistant, Alexa, everywhere with their users.[94]

The ever-expanding merger of surveillance and biometrics will continue to raise new challenges to courts' interpretations of the Fourth Amendment, particularly as law enforcement increasingly wield these technologies and ask technology companies to reveal users' information. But given the rigid way courts have applied *Carpenter*'s five factors, courts may need a bolder, more robust framework to provide protection for biometric information that is

---

88. *See, e.g.*, Scott McCartney, *Are You Ready for Facial Recognition at the Airport?*, WALL ST. J. (Aug. 14, 2019, 8:58 AM), https://www.wsj.com/articles/are-you-ready-for-facial-recognition-at-the-airport-11565775008 [https://perma.cc/QC4M-MJQJ].

89. *See, e.g.*, *Musicians Call for Facial Recognition Ban at Gigs*, BBC NEWS (Sept. 10, 2019), https://www.bbc.com/news/technology-49647244 [https://perma.cc/D3ZC-X579].

90. *See* Steve Knopper, *Why Taylor Swift Is Using Facial Recognition at Concerts*, ROLLING STONE (Dec. 13, 2018, 11:24 AM), https://www.rollingstone.com/music/music-news/taylor-swift-facial-recognition-concerts-768741/ [https://perma.cc/8X96-VT99].

91. Sonia Fernandez, *Your Video Can ID You Through Walls*, CURRENT (Sept. 30, 2019, 10:15 AM), https://www.news.ucsb.edu/2019/019643/your-video-can-id-you-through-walls [https://perma.cc/7NGW-HEXV].

92. Christopher Mims, *All Ears: Always-On Listening Devices Could Soon Be Everywhere*, WALL ST. J. (July 12, 2018, 12:00 PM), https://www.wsj.com/articles/all-ears-always-on-listening-devices-could-soon-be-everywhere-1531411250 [https://perma.cc/SNN2-CCRM].

93. *See* Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) (describing the cell-phone as "almost a 'feature of human anatomy[ ]'") (citation omitted).

94. *See* Rachel Metz, *First, Alexa Came Into Your Home. Now It Wants to Get on Your Body*, CNN BUS. (Sept. 26, 2019, 12:29 PM), https://www.cnn.com/2019/09/25/tech/amazon-alexa-wearables-loop-earbuds-frames/index.html [https://perma.cc/6SPP-67ME].

equivalent to the Fourth Amendment protection extended to historical CSLI.

III. APPLYING *CARPENTER* TO FACIAL AND VOICE RECOGNITION TECHNOLOGIES IN SURVEILLANCE AND TRACKING SYSTEMS

As surveillance and tracking technologies advance, courts will need to confront the extent to which *Carpenter*'s expansion of Fourth Amendment protection applies to biometrics in surveillance. Yet, as discussed below, courts applying *Carpenter* to surveillance technologies have applied the five factors narrowly, generally declining to extend Fourth Amendment protection. Moreover, approaches taken by post-*Carpenter* courts suggest that current applications of the factors identified in *Carpenter* may be insufficiently flexible to protect biometric surveillance information, even when the information contains comprehensive data on a person's intimate details.

Sections A and B explain how current technologies incorporate FRT and VRT to enhance surveillance capabilities.[95] Section C then describes how courts, based on current trends, would likely apply *Carpenter*'s five factors to the government's acquisition and use of FRT and VRT surveillance data were such a challenge to come before a court. This Part applies *Carpenter*'s factors to FRT and VRT because of their prevalence in society and readiness for merging with conventional surveillance technologies.

A. FACIAL RECOGNITION IN SURVEILLANCE CAMERAS

FRT compares a data subject's captured image to templates already uploaded to the system's database.[96] To determine identity, FRT typically has two components that work in tandem: a database of known photo templates[97] and a software capable of

95. Kristine Hamman & Rachel Smith, *Facial Recognition Technology: Where Will It Take Us?*, AM. BAR ASS'N (2019), https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/ [https://perma.cc/2Y3X-9HVM].

96. Steve Symanovich, *How Does Facial Recognition Work?*, NORTON (2019), https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html [https://perma.cc/PKB6-AVXE].

97. Kyle Chayka, *Biometric Surveillance Means Someone is Always Watching*, NEWSWEEK (Apr. 17, 2014 6:06 AM), https://www.newsweek.com/2014/04/25/biometric-surveillance-means-someone-always-watching-248161.html [https://perma.cc/6S3S-A4WS].

comparing these templates to the geometry of the subject's face, identifying up to 30,000 facial landmarks.[98] Researchers have achieved incredible accuracy when developing facial recognition systems.[99] Cities have installed networks of hundreds[100] or even thousands[101] of security cameras to curb criminal activity. In addition to garnering critiques of an encroaching Orwellian state,[102] incorporating FRT into surveillance networks raises considerable Fourth Amendment concerns.

Gathering an adequate number of confirmed templates to create an effective facial recognition system is a great challenge. However, according to a report by Georgetown Law's Center on Privacy and Technology, law enforcement has been able to access one gold mine of known photo templates: state driver's license photos.[103] Law enforcement agents can run searches, comparing a surveillance image to the millions of templates made available by several states' Department of Motor Vehicles (DMV).[104] Another reliable and seemingly unlimited source of facial templates is Clearview AI, a start-up that sources facial templates from social media and "millions of other websites" and applies them to its advanced facial recognition system.[105] More than 600 law enforcement agencies have used Clearview's services to identify persons of interest.[106] Because of its prevalence and advancement, FRT is poised to raise a formidable challenge to the right to privacy in public

98. *About Face ID Advanced Technology*, APPLE (Sept. 19, 2019), https://support.apple.com/en-us/HT208108 [https://perma.cc/2LYZ-JN8J].

99. *See* Florian Schroff et al., *FaceNet: A Unified Embedding for Face Recognition and Clustering*, 2015 IEEE CONFERENCE ON COMPUTER VISION AND PATTERN RECOGNITION, 822 (June 2015), https://www.cv-foundation.org/openaccess/content_cvpr_2015/app/1A_089.pdf [https://perma.cc/V9JW-HCDZ] (achieving "a classification accuracy of . . . [99.63%]").

100. Nancy G. La Vigne et al., *Evaluating the Use of Public Surveillance Cameras for Crime Control — A Summary*, URB. INST.: JUST. POL'Y CTR. (Sept. 2011), https://www.urban.org/sites/default/files/publication/27546/412401-Evaluating-the-Use-of-Public-Surveillance-Cameras-for-Crime-Control-and-Prevention-A-Summary.PDF [https://perma.cc/CZ6F-N5ME].

101. William M. Bulkeley, *Chicago's Camera Network Is Everywhere*, WALL ST. J. (Nov. 17, 2009 12:01 AM), https://www.wsj.com/articles/SB10001424052748704538404574539910412824756 [https://perma.cc/FJ6E-786M].

102. *See id.*

103. *See The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. LAW CTR. ON PRIV. & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org/ [https://perma.cc/UF8U-GV59].

104. *See id.*

105. Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/5Z9M-NXLF].

106. *See id.*

spaces,[107] perhaps even more than conventional video surveillance networks have.

B. VOICE RECOGNITION TECHNOLOGY IN SMART DEVICES

VRT is a well-developed biometric technology that measures the pitch, tone, and cadence of data subjects' voices to identify them.[108] Many individually tailored technologies, such as Apple's Siri on portable digital devices[109] and Amazon's Alexa on stand-alone smart home devices,[110] use VRT for their basic functions and commands to improve accuracy when detecting their users' voices. These devices use "always on" features that constantly surveil their surroundings to listen and quickly respond to users' questions and commands.[111] When Alexa hears her name or another wake word, she instantly begins recording the command or question to send to the Amazon Cloud for analysis.[112] As smart devices like Alexa grow in prevalence and perpetually collect private information from the home,[113] their use of VRT, like that of FRT, could pose a substantial threat to privacy rights.

---

107. *See id.*

108. *See* Clifford S. Fishman & Anne T. McKenna, WIRETAPPING AND EAVESDROPPING § 31:8 (2019).

109. *See* Todd Haselton, *How to Get Siri Working Again If It Stops Listening to You on Your iPhone*, CNBC (Nov. 24, 2018 10:00 AM), https://www.cnbc.com/2018/11/23/how-to-re-train-siri-to-recognize-your-voice.html [https://perma.cc/BDG7-N4ZU] ("Apple has a way that lets you retrain Siri to recognize your voice.").

110. *See* Taylor Martin, *How to Set up Voice Profiles on the Amazon Echo*, CNET (Oct. 12, 2017 11:41 AM), https://www.cnet.com/how-to/how-to-setup-voice-profiles-on-the-amazon-echo-alexa/ [https://perma.cc/M2MX-FHPT] ("Amazon brought . . . multi-user support with voice recognition to Alexa.").

111. *See* Jay Stanley, *The Privacy Threat From Always-On Microphones Like the Amazon Echo*, ACLU (Jan. 13, 2017 10:15 AM), https://www.aclu.org/blog/privacy-technology/privacy-threat-always-microphones-amazon-echo [https://perma.cc/TTF5-CSDW].

112. *See Alexa and Alexa Device FAQs*, AMAZON (last visited Aug. 18, 2020), https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230 [https://perma.cc/Y6EW-D48Q].

113. Ryan G. Bishop, Note, *The Walls Have Ears . . . and Eyes . . . and Noses: Home Smart Devices and the Fourth Amendment*, 61 ARIZ. L. REV. 667, 680 (2019).

C. HOW COURTS HAVE APPLIED THE *CARPENTER* FACTORS — AND MIGHT APPLY THEM TO FRT AND VRT DATA

Lower courts applying *Carpenter* have resisted extending the broader protection afforded to historical CSLI to other surveillance and tracking tools. When addressing defendants' motions to suppress evidence, a great number of post-*Carpenter* courts have disposed of such motions by invoking the *Leon* good-faith exception,[114] which admits contested evidence where a law enforcement agent relied in good faith on the constitutionality of a search or seizure.[115] A few others — very much a minority position — have held that *Carpenter* protection does not apply retroactively to searches executed before *Carpenter* reached the Supreme Court.[116] Regardless of their stated reasoning, however, post-*Carpenter* courts have generally disposed of suppression motions following a mechanical application of the *Carpenter* factors of invasiveness, comprehensiveness, voluntariness, ease of data collection, and retrospectivity.[117] By all indications, courts would likely apply these factors narrowly to FRT and VRT information.

1. *Invasiveness*

The standard for invasiveness under *Carpenter* is whether the information reveals intimate details that comprise the privacies of life.[118] *Carpenter* principally framed intimate details as "familial, political, professional, religious, and sexual associations" revealed by "the whole of [a person's] physical movements" over a

114. *See, e.g.*, United States v. Korte, 918 F.3d 750, 758 (9th Cir. 2019) (affirming the district court's application of the good-faith exception where the government reasonably relied on the Stored Communications Act (SCA) to obtain the defendant's CSLI); United States v. Curtis, 901 F.3d 846, 848 (7th Cir. 2018) (holding that law enforcement's good-faith reliance on the SCA is dispositive); United States v. Joyner, 899 F.3d 1199, 1204–205 (11th Cir. 2018) (holding that under *Leon*, the district court's denial of the motions to suppress cell-site location data was not reversible error); Reed v. Commonwealth, 819 S.E.2d 446, 449–50 (Va. Ct. App. 2018).

115. United States v. Leon, 468 U.S. 897, 897 (1984).

116. *See, e.g.*, United States v. Davis, No. 1:13-CR-28, 2019 WL 1584634 at *2 (M.D. Pa. Apr. 12, 2019); State v. Neil, 133 N.E.3d 585, 590 (Ohio Ct. App. 2019); State v. Dober, No. A-18-1088, 2019 WL 3934769 at *4 (Neb. Ct. App. Aug. 20, 2019).

117. Some courts have, however, exhibited a degree of flexibility in applying *Carpenter* by disposing of Fourth Amendment challenges without addressing some of the five factors. *See infra* Part III.D.

118. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

substantial amount of time.[119] Thus, under *Carpenter*, where a surveillance or tracking tool reveals this type of associational information, the Fourth Amendment warrant requirement is triggered.[120] This associational-information standard considers information about the data subject that is connected, primarily, to his or her relationships with other people.[121] The basic premise is that the government cannot, without a warrant supported by probable cause, compile deeply private information such as a combination of professional, religious, and sexual associations by learning where, with whom, and how the surveillance target spends her time. But not all intimate details are relational. Some traits — for example, bodily characteristics or health status — are just as intimate, but exist independent of any external relationship. Non-relational associational information is the information intrinsically associated with the person without reference to the extrinsic associational information concerned in *Carpenter*. As discussed below, this distinction is important for understanding *Carpenter*'s deficiencies when applied to biometrics.

When considering *Carpenter*-based challenges to information retained by internet service providers (ISPs), courts applying *Carpenter*'s invasiveness factor have routinely found that ISP information does not reveal enough associational information to justify a warrant requirement. ISPs track Internet use and produce the user's time-stamped website browsing history. ISP information refers to this metadata and other data that ISPs track about their consumers' Internet use. Courts have predominantly held that ISP information, including the internet protocol (IP) addresses assigned to each user's Internet-connected device, does not reveal the detailed, long-term locational information that constitutes the type of intimate details that *Carpenter* protected.[122] For example, in

119. *Id.* (citing United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

120. *See id.* at 2217–18.

121. The *Carpenter* Court, in citing to Justice Sotomayor's *Jones* concurrence, brought front-and-center to the invasiveness inquiry a person's "familial, political, professional, religious, and sexual associations." *Id.* at 2217 (quoting 565 U.S. at 415 (Sotomayor, J., concurring)). These associations are inherently relational, as they frame different facets of a person's identity principally by her membership in a group. In *Carpenter* terms, the intimate details that matter are those that reveal where a person spends her time — such as at church, a LGBTQ bar, or at the office — and with *whom* — the kinds of people who frequent those places.

122. *See, e.g.*, United States v. Hood, 920 F.3d 87, 92 (1st Cir. 2019); United States v. Jenkins, No. 1:18-CR-00181, 2019 WL 1568154, at *4–5 (N.D. Ga. Apr. 11, 2019); United States v. Tolbert, 326 F. Supp. 3d 1211, 1224–25 (D.N.M. 2018).

United States v. McCutchin,[123] the District of Arizona declined to extend Fourth Amendment protection to ISP information, arguing in part that this information does not reveal the kind of the associational information concerned in *Carpenter*.[124]

In one lone case from the Arizona Court of Appeals, *State v. Mixton*,[125] Judge Peter Eckerstrom dissented from the majority's decision that the Fourth Amendment did not require a warrant for the government to obtain ISP information identifying the defendant as the sender of certain Internet messages.[126] Judge Eckerstrom responded that *Carpenter* dispositively applies in favor of the defendant's challenge to the government's warrantless acquisition of his identifying ISP information, observing that the Internet has become "a place we shop, converse with friends and romantic partners, seek information about medical conditions, and debate issues of the day,[ ]" and thus yields the type of information captured by historical CSLI.[127] He further reasoned that warrantless acquisition of ISP information, when combined with the user's separately obtained Internet browsing history, represents an invasion into the user's "presumptively anonymous" conduct on the Internet and "acutely private thought process[es]" that the Fourth Amendment protects.[128] However, to date, no court has adopted Judge Eckerstrom's approach recognizing an expectation of anonymity in Internet use, with courts continuing to find that warrantless acquisitions of ISP information do not offend the Fourth Amendment.

Courts have similarly held that surveillance cameras do not implicate the same concerns of invasiveness as historical CSLI. For example, a federal court in Wisconsin analyzed *Carpenter* and concluded that, at most, surveillance cameras in public places reveal only the comings and goings at a fixed, limited location and are not invasive enough to invoke the warrant requirement.[129] Another federal court in Georgia held that surveillance cameras do not capture a person's intimate details, unlike the way historical CSLI

123. No. CR-17-01517-001-TUC-JAS (BPV), 2019 WL 1075544 (D. Ariz. Mar. 7, 2019).
124. *See id.* at *2.
125. 447 P.3d 829 (Ariz. Ct. App. 2019).
126. *Id.* at 845–47 (Eckerstrom, J., concurring in part and dissenting in part).
127. *Id.* at 846.
128. *Id.*
129. *See* United States v. Kelly, 385 F. Supp. 3d 721, 729 (E.D. Wis. 2019).

does, because cameras are unable to track a defendant's location beyond the area within their fixed field of view.[130]

Notably, in *United States v. Tuggle*,[131] the Central District of Illinois recognized that although video surveillance is generally not protected by the Fourth Amendment, prolonged recording beyond eighteen months might reveal protected, intimate details, though the Court ultimately found that eighteen months of video surveillance was not a search.[132] This reasoning is an extension of *Carpenter*'s implicit reasoning that invasiveness depends in part on comprehensiveness, where *Carpenter* found that "accessing seven days of CSLI constitutes a Fourth Amendment search" as the collected information provided an all-encompassing record of a person's movements, which in turn revealed the associational information protected by the Fourth Amendment.[133] However, most courts have been unwilling to apply *Carpenter* to surveillance and tracking technologies other than historical CSLI.[134]

Courts, if ever confronted with FRT, would likely decline to offer protection under the majority approach of *Carpenter*. As discussed above, lower courts have most often found that video surveillance does not violate a person's right to privacy.[135] When considering invasiveness, courts have noted the dearth of associational information revealed by such surveillance, finding no Fourth Amendment protection when a fixed video camera, however surreptitiously, captured the movements of individuals in public places or in private places viewable from public vantage points.[136] Even when FRT is added to traditional video surveillance, courts that rigidly apply the *Carpenter* analysis will unlikely find invasiveness in such technology because facial recognition does not immediately reveal the type of associational information identified in *Carpenter*.[137]

---

130. *See* United States v. Gbenedio, No. 17-CR-430-TWT-JSA, 2019 WL 2177943, at *4 (N.D. Ga. Mar. 29, 2019) (finding "no protectible privacy interest . . . implicated by [nearly 17 months' pole-camera surveillance]"), *report and recommendation adopted*, No. 1:17-CR-430-TWT, 2019 WL 2173994, at *1 (N.D. Ga. May 17, 2019).

131. No. 16-CR-20070-JES-JEH, 2018 WL 3631881 (C.D. Ill. July 31, 2018).

132. *Id.* at *3.

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

134. *See supra* Part III.C.

135. *See, e.g.*, *Tuggle*, 2018 WL 3631881, at *3–4; *Gbenedio*, 2019 WL 2177943, at *4 (finding "no protectible privacy interest . . . implicated by [nearly 17 months' pole-camera surveillance]"); *Kelly*, 385 F. Supp. 3d at 723, 727.

136. *See Kelly*, 385 F. Supp. 3d at 724–25; United States v. Kubasiak, No. 18-CR-120-PP, 2018 WL 4846761, at *5 (E.D. Wis. Oct. 5, 2018).

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

A review of post-*Carpenter* decisions suggests that courts will not find VRT information obtained without a warrant to be unconstitutionally invasive either. Voice recognition would reveal a limited amount of the associational information concerned in *Carpenter*.[138] Similar to ISP information, voice recordings sent to the cloud from smart devices could reveal the applications and websites that users seek to access. However, courts applying *Carpenter* have routinely found that ISP information is not invasive because this form of tracking does not reveal associational information to the same degree, as does the whole of a person's movements.[139]

Judge Eckerstrom's partial dissent in *Mixton* provides an alternative understanding, as he recognized invasiveness in IP addresses revealing web-browsing history. In the same vein as his reasoning that Internet activity reveals deeply private information,[140] web-browsing history can just as easily reveal a person's associational information when coupled with VRT information. Namely, information obtained incidental yet necessary to VRT analysis — the names of the sites and applications accessed or the text of voice-commanded messages sent — can just as well reveal a person's associational information.[141] However, if current applications of the doctrine continue, courts likely will not find invasiveness in the government's warrantless acquisition of VRT or FRT information under *Carpenter*.

---

138. *See id.*

139. *See, e.g.*, United States v. Hood, 920 F.3d 87, 92 (1st Cir. 2019); United States v. Jenkins, No. 1:18-CR-00181, 2019 WL 1568154, at *4–5 (N.D. Ga. Apr. 11, 2019); United States v. Tolbert, 326 F. Supp. 3d 1211, 1224–25 (D.N.M. 2018).

140. *See* State v. Mixton, 447 P.3d 829, 846 (Ariz. Ct. App. 2019) (Eckerstrom, J., concurring in part and dissenting in part) ("[The Internet] is a place we shop, converse with friends and romantic partners, seek information about medical conditions, and debate issues of the day.").

141. For example, were law enforcement to obtain VRT information indicating that the cellphone user asked Siri to access Bumble, Hinge, and Grindr — popular dating applications — an agent could deduce that the user is active in the dating pool and identifies as LGBTQ. Or, if the user regularly accessed the Wall Street Journal and Robinhood apps, an agent could deduce that the user actively trades in securities. Such examples are seemingly endless.

2. *Comprehensiveness*

The comprehensiveness factor looks to how "all-encompassing" the recorded information is.[142] In *Carpenter*, the Court found that the "exhaustive chronicle" of the whole of the defendant's movements over the course of just seven days would reveal too many intimate details to obtain without a warrant.[143] Lower courts have framed comprehensiveness as the "totality of the defendant's movements,"[144] whether the surveillance tool is limited or fixed,[145] and as a function of the length of time the suspect is surveilled.[146] That is, the more information a surveillance technology reveals, the more invasive the totality of that information becomes. The principal inquiry in a finding of comprehensiveness is at what point the surveillance reveals the suspect's associational information.[147]

Most courts weighing *Carpenter*'s comprehensiveness factor in their analyses of video camera surveillance have focused on the length of time. The bar for finding comprehensiveness, however, appears to be quite high. In *United States v. Gbenedio*,[148] for example, the Northern District of Georgia held that nearly seventeen months' pole-camera surveillance did not record sufficiently comprehensive information to constitute a search.[149] As discussed above, even though *Tuggle* noted that, at some length of time, the duration of monitoring may become comprehensive enough to constitute a search, it still held that eighteen months' video surveillance did not constitute a search.[150]

In contrast, in *People v. Tafoya*,[151] the Colorado Court of Appeals concluded that "continuous, three-month-long use of the pole camera constituted a search under the Fourth Amendment

142. *See Carpenter*, 138 S. Ct. at 2217.
143. *See id.* at 2217, 2219.
144. United States v. Kelly, 385 F. Supp. 3d 721, 727 (E.D. Wis. 2019).
145. *See id.* at 729.
146. *See* United States v. Diggs, 385 F. Supp. 3d 648, 652 (N.D. Ill. 2019) (finding that GPS tracking of over one month constituted a comprehensive record of the defendant's movements).
147. *See Carpenter*, 138 S. Ct. at 2217.
148. No. 17-CR-430-TWT-JSA, 2019 WL 2177943 (N.D. Ga. Mar. 29, 2019).
149. *See id.* at *4 (finding "no protectible privacy interest . . . implicated by [nearly 17 months' pole-camera surveillance]"), *report and recommendation adopted*, No. 1:17-CR-430-TWT, 2019 WL 2173994, at *1 (N.D. Ga. May 17, 2019).
150. *See* United States v. Tuggle, No. 16-CR-20070-JES-JEH, 2018 WL 3631881, at *3 (C.D. Ill. July 31, 2018).
151. No. 17-CA-1243, 2019 WL 6333762 (Colo. App. Nov. 27, 2019).

[because] [t]he information gathered through the use of targeted, long-term video surveillance will necessarily include a mosaic of intimate details of the person's private life and associations."[152] Similarly, in *United States v. Vargas*,[153] a pre-*Carpenter* case, the Eastern District of Washington held that even one month of pole-camera surveillance into the mostly enclosed front yard of a residence was a search, even though the front yard was visible from public vantage points.[154]

Notwithstanding *Vargas* and *Tafoya* and their findings of comprehensiveness after one and three months' video surveillance, respectively, courts have largely been unwilling to find comprehensiveness even with longer durations of surveillance. Still, the length of time remains the key consideration in courts' analyses of the comprehensiveness factor.

Separately, courts considering ISP information have focused on the mobility of the surveillance mechanism — that is, the ability or inability of ISP tracking tools to go where the data subject goes — in determining comprehensiveness. The majority view has been that this information does not reveal an exhaustive chronicle of the defendant's "physical or digital activities"[155] because at most, it reveals only a single location where the user logged on to a particular website or application.[156]

Facial recognition systems, like ordinary video surveillance, are limited by the single, fixed[157] locations of video cameras and capture still facial images to recognize data subjects. On this view, courts are unlikely to find FRT information as sufficiently comprehensive to require a warrant under the majority approach. But when FRT is integrated into vast networks of video surveillance cameras covering up to thousands of locations and revealing a far greater range of "comings and goings"[158] of a whole population of individuals, such networks stand in stark contrast to the kind of single, fixed location video surveillance addressed in the majority-

152. *Id.* at *8 (quoting *State v. Jones*, 903 N.W.2d 101, 110 (S.D. 2017)), *cert. granted*, 2020 WL 4343762 (Colo. June 27, 2020).
153. No. CR-13-6025-EFS, 2014 U.S. Dist. LEXIS 184672 (E.D. Wash. Dec. 15, 2014).
154. *See id.* at *13–37.
155. United States v. Monroe, 350 F. Supp. 3d 43, 48 (D.R.I. 2018) (citation omitted).
156. *See* United States v. Jenkins, No. 1:18-CR-00181, 2019 WL 1568154, at *4 (N.D. Ga. Apr. 11, 2019).
157. *See* United States v. Kelly, 385 F. Supp. 3d 721, 726–27 (E.D. Wis. 2019).
158. *Id.* at 729.

view cases.[159] Thus, a court could reasonably find that even when FRT in video surveillance is used for relatively brief periods, the comprehensive catalog of specific individuals' movements within a surveillance network of hundreds or thousands of points throughout a city, including facial identification at each of these points, may sufficiently reveal the "totality of [her] movements"[160] to meet the comprehensiveness factor set out in *Carpenter*. There is no clear indication, however, that the majority of jurisdictions would be willing to take that path.

Likewise, courts are unlikely to regard VRT surveillance as comprehensive. Concededly, voice recognition systems can incidentally reveal private information about the user's identity in addition to the names of the websites and applications accessed or the text of messages sent.[161] Because of the "always on" features of devices that use voice recognition, many months' worth of private conversations or commands from the unknowing users could exist.[162] When the VRT information tied to the user's identity is combined with separately collected recordings of the user's conversations and commands, the composite information can provide an incredible amount of personal information, in much the same way composite FRT surveillance information can. Nevertheless, while some courts in minority jurisdictions may be more open to finding comprehensiveness depending on the length of the voice monitoring, most courts will likely determine that VRT coupled with long-term voice recordings does not provide sufficiently detailed, comprehensive information to merit Fourth Amendment protection.[163]

---

159. *See, e.g.*, United States v. Gbenedio, No. 17-CR-430-TWT-JSA, 2019 WL 2177943, at *4 (N.D. Ga. Mar. 29, 2019), *report and recommendation adopted*, No. 1:17-CR-430-TWT, 2019 WL 2173994, at *1 (N.D. Ga. May 17, 2019); United States v. Tuggle, No. 16-CR-20070-JES-JEH, 2018 WL 3631881, at *3 (C.D. Ill. July 31, 2018).

160. *Kelly*, 385 F. Supp. 3d at 727.

161. *See* State v. Mixton 447 P.3d 829, 846 (Ariz. Ct. App. 2019) (Eckerstrom, J., concurring in part and dissenting part) (framing *Carpenter*'s reasoning, in part, as rejecting the third-party doctrine when "the privacy domain cannot be accessed without the incidental disclosure of some private information").

162. *See* Grace Manning, *Alexa: Can You Keep a Secret? The Third-Party Doctrine in the Age of the Smart Home*, 56 AM. CRIM. L. REV. ONLINE 25, 25, 30 (2019).

163. *See, e.g.*, United States v. Diggs, 385 F. Supp. 3d 648, 652 (N.D. Ill. 2019) (finding that the precise, detailed tracking of the *whole* of the defendant's movements was similarly comprehensive as in *Jones* and in *Carpenter*).

3. *Voluntariness*

Voluntary exposure of information to another person or entity is the cornerstone of the third-party doctrine.[164] The *Carpenter* Court framed voluntariness as whether the information was "truly 'shared' as one normally understands the term."[165] If a technology is "'such a pervasive and insistent part of daily life' that carrying [it] is indispensable to participation in modern society[,]" the data collected from that source is not truly shared.[166] Because cell phones are one such technology, *Carpenter* found that the user did not truly share his historical CSLI.[167]

Post-*Carpenter* courts have further interpreted voluntariness with respect to whether the user made an affirmative and intentional decision to provide her information.[168] When confronted with IP addresses and other forms of ISP information, courts such as the First Circuit in *Hood* have ruled that the defendants did not retain a reasonable expectation of privacy in that information because they had intentionally accessed the internet through their ISPs and made affirmative decisions to access websites and online applications.[169]

In the context of video surveillance, courts have presumed voluntariness when the suspects were in public because they have no reasonable expectation of privacy in public spaces.[170] That presumption was broadened in *California v. Ciraolo*[171] to include private areas that are visible to the public under the public exposure

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

165. *Id.*

166. *Id.* (quoting *Riley v. California*, 573 U.S. 373, 385 (2014)).

167. *Id.*

168. *See, e.g.*, *id.* (recognizing that cell phones log location information "without any affirmative act on the part of the user"); United v. Maclin, 393 F. Supp. 3d 701, 708 (N.D. Ohio 2019) ("Subscriber information requires an individual's active participation. . . ."); United States v. Frei, No. 3:17-CR-00032, 2019 WL 189826, at *3 (M.D. Tenn. Jan. 14, 2019) ("To create a bank record, an individual must choose to voluntarily participate in a commercial transaction with his or her bank card.").

169. *See* United States v. Hood, 920 F.3d 87, 90–92 (1st Cir. 2019); *see also* United States v. Kidd, 394 F. Supp. 3d 357, 365–68 (S.D.N.Y. 2019); State v. Mixton, 447 P.3d 829, 835–37 (Ariz. Ct. App. 2019) (finding that the defendant had no recognized privacy interest in ISP information).

170. *See, e.g.*, United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."); Maryland v. Macon, 472 U.S. 463, 469 (1985) ("Here, respondent did not have any reasonable expectation of privacy in areas of the store where the public was invited to enter and to transact business.") (citing *Knotts*, 460 U.S. at 281–82).

171. 476 U.S. 207 (1986).

doctrine.[172] In *Ciraolo*, the Supreme Court held that the officer's observations of the defendant's home from "a public vantage point where [the officer] ha[d] a right to be" did not constitute a search.[173] Instead of following *Carpenter*'s lead in limiting the presumption of voluntariness, many post-*Carpenter* courts addressing surreptitious government use of surveillance cameras have relied on *Ciraolo* to find voluntariness.[174] In other words, courts have been unwilling to accord other forms of technology the same exception to the third-party doctrine that *Carpenter* afforded to historical CSLI.

Given post-*Carpenter* courts' routine findings of voluntariness, courts conducting Fourth Amendment analyses of FRT information would likely conclude that such information was voluntarily handed over to the government. First, courts would likely consider how the government obtained the original template photo, which are typically derived from photos collected by various government agencies.[175] Courts would then consider whether the filmed subject placed herself voluntarily where an officer might see her from a public vantage point.[176] Courts would thus likely conclude that when the government mines DMV photos for facial templates and uses those photos in conjunction with videos taken in public places or private places visible to the public, the resulting FRT information was voluntarily relinquished to the government. Alternatively, courts could consider driver's licenses and state-issued identification cards as "indispensable to participation in modern society[ ]"[177] to support a finding of involuntariness. However, courts have long held that individuals have "no legitimate expectation of privacy" in their DMV records because they are "matters of public record."[178] Photos of faces are captured by a network of surveillance cameras installed in "public vantage point[s] where

172. *See id.* at 213. The public exposure doctrine states that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." Katz v. United States, 389 U.S. 347, 351 (1967) (citations omitted).

173. *Ciraolo*, 476 U.S. at 213.

174. *See, e.g.*, United States v. Tuggle, No. 16-CR-20070-JES-JEH, 2018 WL 3631881, at *3–4 (C.D. Ill. July 31, 2018); United States v. Gbenedio, No. 17-CR-430-TWT-JSA, 2019 WL 2177943, at *4 (N.D. Ga. Mar. 29, 2019), *report and recommendation adopted*, No. 1:17-CR-430-TWT, 2019 WL 2173994, at *14 (N.D. Ga. May 17, 2019); United States v. Kelly, 385 F. Supp. 3d 721, 723, 727 (E.D. Wis. 2019).

175. *See* GEO. L. CTR. ON PRIV. & TECH., *supra* note 103.

176. *Ciraolo*, 476 U.S. at 213.

177. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

178. Phillips v. Bailey, 337 F. Supp. 2d 804, 806 (W.D. Va. 2004) (citing Doe v. City of New York, 15 F.3d 264, 268 (2d Cir. 1994)).

[law enforcement] has a right to be[,]"[179] so it is unlikely that a court would find voluntariness in favor of the data subject.

Courts considering information recorded through VRT, even more so than FRT information, would likely find it voluntarily relinquished. The "always on" feature of smart home devices, cell phones, and other "Internet of Things" devices[180] might raise concerns of voluntariness, as this setting leaves users no choice but to allow these devices to listen to their conversations. Nonetheless, until carrying VRT devices becomes indispensable to participation in modern society,[181] courts will likely find that Internet subscribers using their voices to access online features make the affirmative decision to access services and have no reasonable expectation of privacy in their VRT information. Thus, a court applying *Carpenter* under current trends would likely find VRT information to be voluntarily relinquished.

4. *Ease of Data Collection*

The *Carpenter* Court framed ease of data collection as a function of "expense."[182] Lower courts have understood expense to include the amount of effort and resources saved in using a particular surveillance technology relative to the costliness of in-person surveillance. As the Southern District of New York recognized, the government's subpoena power alone could render information cheap and easy to obtain.[183] With respect to video surveillance, some courts have analogized this technology to police officers staking out a target area for extended periods of time, and some have concluded that ease of collection of visual information heightens

179. *Ciraolo*, 476 U.S. at 213.

180. *See* Stanley, *supra* note 111 (describing "Internet of Things" devices as personal assistants — like Siri, Amazon Echo, and Google Home — whose microphones and video recorders are always on).

181. While the *Carpenter* Court stated that carrying a cell phone is "indispensable to participation in modern society[,]" *Carpenter*, 138 S. Ct. at 2220, it remains unclear whether that cell phone must be a smartphone, whose voice-activated assistants feature crude, VRT-like functions, *see supra* note 109.

182. *Carpenter*, 138 S. Ct. at 2217–18 ("[L]ike GPS monitoring, cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense."); *see also id.* at 2235 (Kennedy, J., dissenting).

183. *See* United States v. Kidd, 394 F. Supp. 3d 357, 365 (S.D.N.Y. 2019) ("Both data types are cheap and easy to obtain by law enforcement officer via a *simple* subpoena.") (emphasis added).

the need for a warrant.[184] Lower courts, however, have often disposed of Fourth Amendment challenges without addressing this factor.[185]

As for the ease of data collection factor, both FRT and VRT allow law enforcement to obtain information about the identity of data subjects without having to request identification cards and without even having to follow them while in public, reducing overall expense and effort. Instead of painstakingly surveilling or seeking to record the suspect surreptitiously, agents would only need to acquire the information from the networks, databases, or companies holding FRT and VRT information.[186] Thus, the ease of data collection factor, to the extent courts consider it, will likely weigh in favor of protection of both types of biometric surveillance.

5. *Retrospectivity*

Finally, the *Carpenter* Court found that the retrospective quality of historical CSLI gave "police access to a category of information otherwise unknowable."[187] *Carpenter* seems to have added this factor to create a carve-out protection for historical CSLI while excluding real-time and prospective CSLI.[188] The retrospectivity inquiry asks whether the government would have been able to know the information at the time of a search or the issuance of a compelled disclosure, such as a subpoena or court order.[189]

FRT in video surveillance, particularly within networks, allows the government to know exactly who was present at a previous point in time, leading to the re-creation of a person's past

184. *See* United States v. Kelly, 385 F. Supp. 3d 721, 727–28 (E.D. Wis. 2019).

185. *See, e.g.*, United States v. Hood, 920 F.3d 87, 90–92 (1st Cir. 2019) (discussing voluntariness, comprehensiveness, and invasiveness); United States v. Adkinson, 916 F.3d 605, 610–11 (7th Cir. 2019) (applying voluntariness and comprehensiveness); United States v. Contreras, 905 F.3d 853, 857 (5th Cir. 2018) (disposing of the suppression argument by applying the third-party doctrine).

186. *See* Manning, *supra* note 162 at 27.

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

188. *Id.* at 2220.

189. Retrospectivity applies at the time the government initiates the search as opposed to the time the government holds the information. If courts looked to the latter time, all information would be retrospective. That is, even a search warrant for prospective CSLI would qualify as retrospective at the time the government holds the information. But at the time the government executes the search for prospective CSLI — the time it presents the telecommunications carrier the warrant — that warrant is for information not yet collected. Thus, retrospectivity looks to the time the government initiates the search because framing it otherwise would render any distinction between retrospective and prospective information meaningless.

movements. This information would be "otherwise unknowable"[190] absent law enforcement agents physically following a data subject and requesting her identification. Thus, FRT in video surveillance networks is likely to be considered retrospective.

Information from VRT is also likely to be considered retrospective. A voice recording captures the user's words and allows future listeners to know a category of information "otherwise unknowable."[191] That is, it allows future listeners to place themselves back in time as if at the location of the voice recording. This is similar to the concerns raised in *Carpenter* where historical CSLI allowed the government to know the cell phone users' past movements without actually having to follow them.[192] Thus, a court applying *Carpenter* would likely characterize both FRT and VRT information as retrospective.

D. SUMMARY

On balance, given the current state of Fourth Amendment doctrine, courts seem unlikely to extend *Carpenter* protection to either FRT in video surveillance networks or VRT in "Internet of Things" devices. While the retrospectivity and ease of data collection factors weigh in favor of protection, neither of these factors have been reliable indicators of Fourth Amendment protection.[193] And invasiveness, comprehensiveness, and voluntariness — the more conclusive factors[194] — all weigh against protection under the majority approach to those factors. Under current applications of the *Carpenter* factors, therefore, it is unlikely that courts would extend Fourth Amendment protection to the heightened privacy concerns

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

191. *See id.*

192. *See id.*

193. Courts that have declined to extend Fourth Amendment to video surveillance cases have nonetheless noted the "surreptitious" and retrospective nature of video surveillance. *See, e.g.*, Commonwealth v. McCarthy, 484 Mass. 439, 500, 506–09 (2020) ("Like both CSLI and GPS data, [automatic license plate readers] circumvent traditional constraints on police surveillance power by being cheap (relative to human surveillance) and surreptitious."). Automatic license plate readers — or "ALPRs" — are surveillance camera networks that are paired with software that allow agents to "read" and identify license plate numbers instantly; producing both real-time and historical data. *Id.* at 494–95.

194. *See, e.g.*, United States v. Gbenedio, No. 17-CR-430-TWT-JSA, 2019 WL 2177943, at *3 (N.D. Ga. Mar. 29, 2019) (noting the "single, fixed location[ ]" of the pole cameras as inadequately comprehensive), *report and recommendation adopted*, No. 1:17-CR-430-TWT, 2019 WL 2173994, at *1 (N.D. Ga. May 17, 2019); United States v. Kubasiak, No. 18-CR-120-PP, 2018 WL 4846761, at *5–7 (E.D. Wis. Oct. 5, 2018) (discussing the fixed location of pole cameras and their consequent lack of invasiveness into intimate details).

in the context of biometric technologies such as FRT or VRT surveillance.

Post-*Carpenter* courts' narrow and rigid applications of the five factors may have stayed within the boundaries of precedent, but they are incongruous with two doctrinal concerns that propelled the *Carpenter* decision: that the Fourth Amendment must keep up with technological advances,[195] and that it must protect invasions into the intimate details that comprise the privacies of life.[196] Specifically, courts have taken a view of invasiveness that elevates the importance of extrinsic associational information (i.e., information bearing on the data subject's relationships to those with whom he or she interacts) without taking into account intrinsic information (i.e., non-relational information bearing on the data subject's identity, beliefs, and desires) — information that is equally, if not more deeply, private.

As technologies advance, law enforcement has gained powerful surveillance and tracking tools to conduct criminal investigations. The line of cases between *Katz* and *Carpenter* represents the Court's willingness to expand the Fourth Amendment in keeping with ever-advancing technology. And while the Court rejected a "mechanical interpretation" of the Fourth Amendment in both *Kyllo*[197] and in *Carpenter*,[198] the trend in the lower courts has been to mechanically apply the *Carpenter* factors to other forms of surveillance and tracking technologies.[199] Only a few lower courts have recognized the privacy interests at stake in *Carpenter* exist just as prominently, if not more so, in other surveillance technologies.[200] In contrast, adhering to narrow interpretations of the *Carpenter* factors, the great majority of courts have declined to extend Fourth Amendment protection to emerging and advancing technologies involving ISPs,[201] surveillance cameras,[202] and real-time

195. *See Carpenter*, 138 S. Ct. at 2214 (citing Kyllo v. United States, 533 U.S. 27, 34 (2001)).

196. *See id.* at 2217–18 (citing United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring); Riley v. California, 573 U.S. 373, 403 (2014)).

197. *See Kyllo*, 533 U.S. at 35–36.

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

199. *See, e.g.*, United States v. Kelly, 385 F. Supp. 3d 721, 726–28 (E.D. Wis. 2019); United States v. Diggs, 385 F. Supp. 3d 648, 652–53 (N.D. Ill. 2019).

200. *See, e.g.*, State v. Sylvestre, 254 So. 3d 986, 991 (Fla. Dist. Ct. App. 2018).

201. *See, e.g.*, United States v. Hood, 920 F.3d 87, 90–92 (1st Cir. 2019).

202. *See, e.g.*, United States v. Tuggle, No. 16-CR-20070-JES-JEH, 2018 WL 3631881, at *3 (C.D. Ill. July 31, 2018).

CSLI.[203] While courts have not yet applied *Carpenter* to biometric surveillance systems, it seems unlikely that applying the *Carpenter* factors in the same manner as do post-*Carpenter* courts would lead to a full and robust protection of the kind of intimate details that biometric technologies reveal.[204]

IV. INCORPORATING THE RIGHT TO ANONYMITY IN *CARPENTER* ANALYSES OF BIOMETRIC INFORMATION

Meeting the challenges of "new sense-enhancing technologies"[205] and providing adequate protection for the intimate details of individuals' private lives will require a corrective adjustment to the way courts apply *Carpenter*. This Note argues that courts should recognize a right to anonymity when assessing, for Fourth Amendment purposes, the reasonable expectations of privacy inherent in biometric information such as FRT and VRT. Specifically, this Part argues that courts can — consistent with Fourth Amendment doctrine and with the goals of *Carpenter* — incorporate their consideration of the right to anonymity into their assessment of *Carpenter*'s invasiveness factor. While the right to anonymity has traditionally found its roots in the First Amendment,[206] legal scholars have argued that courts should also recognize such a right in the Fourth Amendment.[207] Recognition of anonymity as a privacy right inherent in the Fourth Amendment would help strengthen courts' analyses of biometric information and protect intimate information that contemporary individuals have come to expect to remain private.

In this Part, Section A introduces the right to anonymity pre- and post-*Katz*. Section B then defines the right to anonymity

---

203. *See, e.g.*, United States v. Woodson, No. 4:16-CR-541-AGF-SPM, 2018 WL 7150388, at *9 (E.D. Mo. Nov. 21, 2018) (finding the instant case distinguishable from *Carpenter*), *report and recommendation adopted*, No. 4:16-CR-541-AGF-SPM, 2019 WL 398453, at *1 (E.D. Mo. Jan. 31, 2019).

204. *See supra* Part III (discussing extrinsic and intrinsic intimate details).

205. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (citation omitted).

206. *See* Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150, 166 (2002); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995).

207. *See, e.g.*, Atanu Das, *Chilling Social Media: Warrantless Border Searches of Social Media Accounts Infringe Upon the Freedom of Association and the Freedom to Be Anonymous Under the First Amendment*, 84 BROOK. L. REV. 1287 (2019); Mihailis E. Diamantis, *Privileging Privacy: Confidentiality as a Source of Fourth Amendment Protection*, 21 U. PA. J. CONST. L. 485 (2018); A. Michael Froomkin, *Lessons Learned Too Well: Anonymity in a Time of Surveillance*, 59 ARIZ. L. REV. 95 (2017).

according to post-*Katz* understandings of the kind of intimate details protected by the Fourth Amendment.

A. TRADITIONAL UNDERSTANDINGS OF THE RIGHT TO ANONYMITY PRE- AND POST-*KATZ*

While the *Katz* line of cases has not yet recognized a right to anonymity, that right has long been protected as a constitutional interest in public spaces and public discourse in other contexts. In *NAACP v. Alabama ex rel. Patterson*,[208] a pre-*Katz* Supreme Court upheld the NAACP's refusal to release its membership list.[209] The Court held that compelling disclosure of membership lists would violate privacy in group association, a right "indispensable to preservation of freedom of association[.]"[210] Decades later in *McIntyre v. Ohio Elections Comm'n*,[211] the Supreme Court held that anonymous pamphleteering is a constitutionally protected activity.[212] There, the Court recognized anonymity as "a shield from the tyranny of the majority[ ]" and "the purpose behind the Bill of Rights[.]"[213] And more recently in *Watchtower Bible and Tract Soc'y of N.Y. v. Vill. of Stratton*,[214] the Court struck down a local ordinance requiring door-to-door pamphleteers to first register with the municipal government.[215] There, the Court further recognized anonymity as an important interest meriting constitutional protection.[216]

A right to anonymity has also lurked in the background of some post-*Katz* Fourth Amendment opinions. In *Hiibel v. Sixth Judicial District Court of Nevada*,[217] the Supreme Court considered a Fourth Amendment challenge to a state "stop and identify" statute which allowed law enforcement agents to compel identification from suspects and to arrest them should they refuse.[218] The Court held that law enforcement agents could compel an individual's

208. 357 U.S. 449 (1958).
209. *See id.* at 466.
210. *Id.* at 462.
211. 514 U.S. 334 (1995).
212. *See id.* at 357.
213. *Id.* at 357.
214. 536 U.S. 150 (2002).
215. *See id.* at 165–69.
216. *Id.* at 166–67.
217. 542 U.S. 177 (2004).
218. *See id.* at 181–82.

identification only in the context of a valid *Terry* stop.[219] This decision is significant because, absent an officer's reasonable suspicion of a safety threat posed by the individual, that individual has the right to remain free from frisking and consequent identification.[220] In other words, the Court required a valid *Terry* stop — another constitutional protection against overly inquisitive government eyes — before encroaching on a person's right to anonymity in public.[221]

Justice Lewis F. Powell's dissent in *Ciraolo* also invoked anonymity in urging the Court to extend the Fourth Amendment to the government's aerial observation of a suspect's backyard.[222] Justice Powell argued that the public exposure doctrine should not apply in that case because airplane passengers observe "at most a fleeting, *anonymous*, and nondiscriminating glimpse of the landscape and buildings over which they pass."[223] There, Justice Powell, joined by three other justices, recognized that people maintain an expectation of anonymity, even when exposing themselves and their activities to the public.

In *United States v. Pineda-Moreno*,[224] the Ninth Circuit denied a petition for rehearing en banc in a GPS tracking case.[225] Then-Chief Judge Alex Kozinski dissented from the denial for rehearing, arguing, like Justice Powell's dissent in *Ciraolo*, that the public exposure doctrine does not apply to the entirety of one's public movements.[226] Chief Judge Kozinski wrote, "You can preserve your *anonymity* from prying eyes, even in public, by traveling at

---

219. *See id.* at 188. A *Terry* stop is an investigative stop subject to the Fourth Amendment requirement that a search and seizure be reasonable, the idea being that when law enforcement stops a person and restrains her freedom to leave, the officer effects a seizure of the person. *See* 1 STEPHEN E. ARTHUR & ROBERT S. HUNTER, FEDERAL TRIAL HANDBOOK: CRIMINAL § 38:3 (4th ed. 2018). For a stop to be valid under *Terry*, the officer must have a particularized and objective basis for suspecting that the arrestee is presently (or about to be) engaged in criminal activity. *See id.* (citations omitted).

220. *See, e.g.*, Mariko Hirose, *Privacy in Public Places: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 Conn. L. Rev. 1591, 1615 (2017) ("It is only when officers have reasonable suspicion for stopping a person in the first place that the law enforcement interest in demanding to know the person's name exceeds the privacy interest in one's identity.").

221. *See Hiibel*, 542 U.S. at 188–89 ("A state law requiring a suspect to disclose his name in the course of a *valid Terry* stop is consistent with Fourth Amendment prohibitions against unreasonable searches and seizures.") (emphasis added).

222. *See* California v. Ciraolo, 476 U.S. 207, 223–24 (1986) (Powell, J., dissenting).

223. *Id.* (emphasis added).

224. 617 F.3d 1120 (9th Cir. 2010).

225. *See id.* at 1120–21.

226. *See id.* at 1121–23.

night, through heavy traffic, in crowds, by using a circuitous route, [and doing a number of other things]."[227] There, Chief Judge Kozinski recognized that even while in public, people retain a protectable expectation of anonymity in their otherwise public activities, so long as they exert enough effort to remain anonymous.[228]

After *Carpenter*, a minority of courts has intimated that an individual could retain a heightened expectation of privacy in the context of identity-revealing ISP information.[229] As Judge Eckerstrom wrote in his dissent in *Mixton*,

> A visit to an internet site is *presumptively anonymous* unless we choose to make it otherwise; our movements on public streets are presumptively visible to all we encounter. For this reason, the [U.S. Supreme] Court has required a warrant for the locational tracking of criminal suspects only when that tracking is sufficiently protracted to reveal private features of their lives.[230]

B. INCORPORATING THE RIGHT TO ANONYMITY INTO FOURTH AMENDMENT INVASIVENESS ANALYSES

While anonymity is often framed as "namelessness,"[231] the right to anonymity is better framed as a protection of information so personal and intimate that it reveals identity. Information only becomes an identifier when it is so connected to an individual's attributes that it could apply only to one person.[232] Names are just one among many identifiers.

Under this reading, anonymity is a subset of privacy. A privacy interest protects information generally, subject to the *Katz* standard of reasonableness, whereas an anonymity interest protects a

---

227. *Id.* at 1126 (emphasis added).

228. *See id.*

229. *See* United States v. Jenkins, No. 1:18-CR-00181, 2019 WL 1568154, at *4–5 (N.D. Ga. Apr. 11, 2019) (noting that the ISP information at issue "does not even identify the user[ ]"); United States v. Monroe, 350 F. Supp. 3d 43, 48 (D.R.I. 2018) (stating that the ISP information at issue "does not, in and of itself, reveal a particular user's identity").

230. *See* State v. Mixton, 447 P.3d 829, 846 (Ariz. Ct. App. 2019) (Eckerstrom, J., concurring in part and dissenting in part) (citing Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018); United States v. Jones, 565 U.S. 400, 430 (2012)).

231. *See, e.g.*, Slobogin, *supra* note 25, at 238–39; Kimberly N. Brown, *Anonymity, Faceprints, and the Constitution*, 21 GEO. MASON L. REV. 409, 414 (2014); *see also Anonymous*, MERRIAM-WEBSTER.COM DICTIONARY, https://www.merriam-webster.com/dictionary/anonymous [https://perma.cc/GH62-MNCR] (last visited Sept. 7, 2020).

232. *See* Skopek, *supra* note 25, at 724.

subset of information that necessarily identifies the person to whom the information refers.[233] The referred class of information is so personal and integral to the intrinsic qualities of a person that it identifies who the individual is. While *Carpenter* seeks to protect extrinsic associational information, this conception of anonymity would protect the non-relational, intrinsic information necessarily implicated by biometric technologies. This understanding of anonymity falls within the purview of the *Katz* "reasonable expectation of privacy" standard because under this reading, the right to anonymity in public spaces is a subset of the right to privacy.

Incorporating an analysis of anonymity — information so personal that it reveals identity — into *Carpenter*'s invasiveness factor would provide a better measure of Fourth Amendment protection in the biometrics context. Biometric surveillance implicates information so intrinsically associated with the data subject that it reveals her identity. FRT, by way of analyzing up to thousands of points on a data subject's face, conveys highly unique, identifying information directly connected to the individual. While a face in public is not necessarily private, a person's identity can be. As Chief Judge Kozinski argued in *Pineda-Moreno*, a person can take steps toward preserving his or her anonymity, even in public.[234] FRT exploits what is not private — the face — to unearth identity, information that would otherwise remain private. Like FRT, VRT exploits what data subjects voluntarily reveal — their voice and the information that the voice contains[235] — to unearth identity, information that would otherwise remain private. By encroaching on a person's reasonable expectation of anonymity, biometric surveillance takes away what should rightfully be kept as private: that individual's identity.

Incorporating the right to anonymity into an analysis of a technology's invasiveness strengthens the *Carpenter* framework in ways that rigid and mechanical applications of the five factors would not. The Fourth Amendment already protects extrinsic associational information,[236] but current applications of *Carpenter*,

---

233. *See id.* at 761.

234. *See* United States v. Pineda-Moreno, 617 F.3d 1120, 1126 (9th Cir. 2010).

235. *See* Sarah Krouse, *What Your Voice Reveals About You: Banks, Doctors and Investigators Are Analyzing the Human Voice for Help in Tracking Down Criminals, Diagnosing Diseases*, WALL ST. J. (Aug. 13, 2019), https://www.wsj.com/articles/what-your-voice-reveals-about-you-11565716426 [https://perma.cc/2R4W-3QQG].

236. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

and the Fourth Amendment generally, may not sufficiently protect information gleaned from biometrics[237] or other technologies that analyze intrinsic information to invade a person's anonymity. Biometric analyses use personal information like facial structures and vocal qualities to reveal not only a name but also highly unique and deeply personal intrinsic information. When a court considers invasiveness only in relation to extrinsic associational information — that is, information bearing on a person's connections to other individuals — without considering intrinsic information,[238] that court fails to appreciate what makes information truly personal: namely, when the information is inextricably tied to a single person. Recognizing a right to anonymity as an integral part of the invasiveness analysis would remedy potential doctrinal oversights by post-Carpenter courts by accurately capturing the interplay between personal information and identity.

Recognizing a right to anonymity would also be consistent with the Supreme Court's Fourth Amendment jurisprudence. While a controlling Supreme Court decision has not yet explicitly extended Fourth Amendment protection to reasonable expectations of anonymity, many Fourth Amendment decisions have engaged in this type of inquiry, seeking to protect deeply personal, identifying information. For example, in *Kyllo*, the Court protected activities within one's home from government surveillance, no matter how "crude" the surveillance technology.[239] The Court viewed information within the home as so intimate — or personal — that even heat emanating from the suspect's home was protected.[240] Similarly, the *Riley* Court protected digital information within a suspect's cell phone, a technology with "immense storage capacity."[241] There, the Court recognized that warrantless access to such immense amounts of information would expose far more than even the most exhaustive search of a home.[242] And in *Carpenter*, the Court found that the whole of one's movements, revealed by seven days of historical CSLI, were deserving of Fourth Amendment protection.[243] Activities within the home and data contained within a

237. *See supra* Part III.C.
238. That is, non-relational information bearing on the data subject's identity, beliefs, and desires.
239. *See* Kyllo v. United States, 533 U.S. 27, 38–40 (2001).
240. *See id.*
241. Riley v. California, 573 U.S. 373, 393–96 (2014).
242. *See id.* at 396–97.
243. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

smartphone reveal not only extrinsic associational information, but also deeply personal, intrinsic information, including the identity of their owners. Under this framing of *Kyllo*, *Riley*, and *Carpenter*, a right to anonymity can and should be recognized as an integral right in the Fourth Amendment. Those cases all protect information linked so strongly to the data subject that the information inevitably reveals identity. This unmasking of identity through personal, intrinsic information is at the heart of the right to anonymity.

Construing the Fourth Amendment to protect against warrantless biometric surveillance would also comport with *Kyllo* and *Riley*, as both weighed technological advances when expanding the Fourth Amendment.[244] A lagging Fourth Amendment, rigidly applied, would allow the government to "capitalize on . . . new sense-enhancing technolog[ies]"[245] like FRT and VRT to encroach on a person's expectation of privacy in her identity. Because invasiveness as a Fourth Amendment consideration has long preceded *Carpenter* and remains the most significant factor in reasonable-expectation-of-privacy analyses, reframing courts' analysis of the invasiveness factor would provide a sensible and much-needed corrective.[246]

Decades before *Carpenter*, in *Silverman v. United States*,[247] the Court recognized the importance of a person's right to retreat into her "own home and there be free from unreasonable government *intrusion*."[248] Meanwhile, *Kyllo* sought to protect intimate details from "prying government eyes."[249] Invasion into intimate details is not unique to *Carpenter*. Rather, invasiveness has long been, and will likely continue to be, central to the Fourth Amendment right to privacy. Thus, in the biometrics context, considering the right to anonymity as an integral part of the invasiveness analysis

244. *See Riley*, 573 U.S. at 393–97; *Kyllo*, 533 U.S. at 38–39.

245. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (citation omitted).

246. When deciding motions to suppress that invoke *Carpenter*, the courts have treated invasiveness as the most important factor in their analyses. Many courts have decided cases without considering ease of data collection or retrospectivity, but almost all have considered whether a surveillance technique invades into the suspect's intimate details. *See, e.g.*, United States v. Maclin, 393 F. Supp. 3d 701, 708 (N.D. Ohio 2019) (weighing invasiveness, comprehensiveness, and voluntariness); United States v. Jenkins, No. 1:18-CR-00181, 2019 WL 1568154, at *4–5 (N.D. Ga. Apr. 11, 2019) (weighing invasiveness, comprehensiveness, and ease of data collection).

247. 365 U.S. 505 (1961).

248. *Id.* at 511 (emphasis added).

249. *Kyllo*, 533 U.S. at 37.

would allow for a flexible Fourth Amendment while remaining true to the Amendment's foundational principles exemplified in cases like *Kyllo*, *Riley*, and *Silverman*.

Reading the invasiveness factor to incorporate a right to anonymity safeguards what the Fourth Amendment already purports to do: keeping the government's intrusive eyes (and ears) away from the intimate details of its citizens. This proposed approach keeps the promise of a flexible and robust Fourth Amendment while remaining responsive to rapid advances in technology. It also offers a viable reading of the principles and precedents of invasiveness that have protected against government intrusions into the intimate details that comprise the privacies of life.

V. CONCLUSION

This Note's application of the five *Carpenter* factors to biometric information demonstrates that conventional Fourth Amendment analysis provides an inadequate framework for evaluating biometric data. Myriad biometric technologies have integrated into modern surveillance and tracking tools, and this convergence of biometrics and surveillance affords law enforcement incredible investigatory power at the expense of fundamental privacy rights. While *Carpenter* purports to offer the flexibility needed to address such "seismic shifts"[250] in technology, lower courts have largely declined to extend Fourth Amendment protection to surveillance and tracking tools beyond historical CSLI. Courts have instead adhered to the same kind of mechanical application rejected in *Carpenter*[251] in the name of faithfully applying its multi-factor test. If courts do not adopt a fresh understanding of the *Carpenter* factors, the Fourth Amendment will likely lag behind the ever-accelerating advancement of surveillance and tracking technologies and fail to sufficiently safeguard "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[252]

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

251. *Id.* at 2214, 2219 (citing *Kyllo*, 533 U.S. at 35) (warning against a "mechanical interpretation of the Fourth Amendment" and "mechanically applying the third-party doctrine").

252. U.S. CONST. amend. IV.