2023

The Carpenter Test as a Transformation of Fourth Amendment Law

Matthew Tokson

Forthcoming, U. Illinois Law Review

THE *CARPENTER* TEST AS A TRANSFORMATION OF FOURTH AMENDMENT LAW

Matthew Tokson

For over fifty years, the Fourth Amendment's scope has been largely dictated by the *Katz* test, which applies the Amendment's protections only when the government has violated a person's "reasonable expectation of privacy." This vague standard is one of the most criticized doctrines in all of American law, and its lack of coherence has made Fourth Amendment search law notoriously confusing. Things have become even more complex following the Supreme Court's landmark decision in *Carpenter v. United States*, which has spawned its own alternative test for determining the Fourth Amendment's scope. The emerging *Carpenter* test looks to the revealing nature of the data at issue, the amount of data collected, and whether the data was voluntarily disclosed to others.

This Essay examines the uneasy state of current Fourth Amendment law, in which the *Katz* and *Carpenter* paradigms overlap and compete in the lower courts. It describes the many ways that courts have attempted to integrate these two frameworks. It also assesses several potential metaprinciples that might be used to determine when each test should be applied.

Based on this analysis, this Essay contends that the *Carpenter* test should be the primary test for Fourth Amendment searches going forward. *Carpenter* creates a coherent, multi-factor test that lower courts have already successfully applied in numerous cases. Its conceptual reach is universal, capable of addressing any Fourth Amendment scenario. And the test focuses arguments and produces clear answers, offering far more predictability than its predecessor. This Essay identifies the theoretical and jurisprudential foundations of the *Carpenter* test, tracing its origins to longstanding Supreme Court precedents and evaluating its application in contemporary cases. Ultimately, the *Carpenter* test can clarify when individuals will be protected against government surveillance and provide courts with meaningful guidance and direction.

INTRODUCTION

The Fourth Amendment prohibits the government from engaging in "unreasonable searches."[1] Government agents generally have to justify their searches by obtaining a warrant or qualifying for an exception to the warrant requirement.[2] But when an act of government surveillance is not a "search," the Fourth Amendment does not apply at all.[3] In these contexts, the government often operates with no constitutional or statutory constraints, gathering sensitive information on an increasingly vast scale.[4]

Yet it is difficult to say what a Fourth Amendment search is with any precision. Current law is in a transition phase, and courts and scholars have struggled to define the Fourth Amendment search for decades. Perhaps the most important question in constitutional criminal procedure—when does the Fourth Amendment apply?—often has no clear answer.

The classic doctrinal standard for Fourth Amendment searches is the *Katz* test, which provides that the government commits a search when it violates an individual's "reasonable expectation of privacy."[5] This is essentially a general reasonableness standard, which gives courts the flexibility to apply the Fourth Amendment to a variety of surveillance contexts but provides almost no guidance or predictability. Instead, Fourth Amendment search law has progressed case-by-case, as the Supreme Court applies the *Katz* test to various fact-patterns.[6] But new Fourth Amendment questions arise frequently, and the *Katz* test offers no way for courts, police officers, or citizens to reliably predict their answers.

Indeed, the *Katz* test is among the most criticized doctrines in American law. It has been attacked as vague,[7] unpredictable,[8] circular,[9] underinclusive of important constitutional

---

[1] U.S. CONST. amend. IV.

[2] Matthew Tokson, *The Normative Fourth Amendment*, 104 MINN. L. REV. 741, 741 (2019).

[3] *Id.*

[4] *E.g.*, Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1042 (2016).

[5] Katz v. United States, 389 U.S. 347, 361 (Harlan, J., concurring) (1967). The Supreme Court has recently adopted a separate, quasi-trespass test that finds a Fourth Amendment search when a government official intrudes on property for the purpose of gathering information. *See* United States v. Jones, 565 U.S. 400, 404–06 (2012). This test is discussed further at *infra* note 30.

[6] *See* Ronald J. Allen & Ross M. Rosenberg, *The Fourth Amendment and the Limits of Theory: Local Versus General Theoretical Knowledge*, 72 ST. JOHNS L. REV. 1149, 1153–58 (1998).

[7] *E.g.*, Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1511 (2010).

[8] *E.g., id.*; Allen & Rosenberg, *supra* note 6, at 1166.

[9] *E.g.*, Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring); William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1824–25 (2016).

values,[10] and underprotective of privacy.[11] Many have also criticized the third-party doctrine, an application of the *Katz* test that withheld Fourth Amendment protection from information exposed to any third party.[12] This doctrine threatened to eliminate constitutional protection for most modern forms of personal information, which tend to be exposed to one's internet service provider or telephone company.[13]

Then, in 2018, the Supreme Court curtailed the third-party doctrine in the landmark case *Carpenter v. United States*.[14] Scholars hailed *Carpenter* as a massively important privacy case,[15] a "blockbuster"[16] that represented "an inflection point in the history of the Fourth Amendment."[17] But exactly what *Carpenter* meant going forward was unclear. The opinion held that government agents had to obtain a warrant before collecting cell phone location data that revealed virtually everywhere a suspect had travelled over a seven-day period.[18] In doing so, it discussed several factors that were relevant to its decision, but did not set out an overt test for future cases.[19] The future of Fourth Amendment law remained "unresolved and

---

[10] *E.g.*, Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 103 (2008); William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1021 (1995). David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069, 1077–79 (2014).

[11] Amitai Etzioni, *Eight Nails into* Katz*'s Coffin*, 65 CASE W. RSRV. L. REV. 413, 413 (2014); Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 120–21 (2002).

[12] *See, e.g.*, Steven M. Bellovin, Matt Blaze, Susan Landau & Stephanie K. Pell*, It's Too Complicated: How the Internet Upends* Katz*,* Smith*, and Electronic Surveillance Law*, 30 HARV. J.L. & TECH. 1, 22–31 (2016); Mary Graw Leary, Katz *on a Hot Tin Roof—Saving the Fourth Amendment from Commercial Conditioning by Reviving Voluntariness in Disclosures to Third Parties*, 50 AM. CRIM. L. REV. 341, 379 (2013); Rubenfeld, *supra* note 10, at 113; Colb, *supra* note 11, at 155–59; Tracey Maclin, Katz*,* Kyllo*, and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51, 136 (2002).

[13] *See, e.g.*, Bellovin et al., *supra* note 12, at 22–31; Leary, *supra* note 12, at 379; Rubenfeld, *supra* note 10, at 113; Colb, *supra* note 11, at 155–59; Maclin, *supra* note 12, at 136.

[14] 138 S. Ct. 2206 (2018).

[15] *See, e.g.*, Matthew B. Kugler & Meredith Hurley, *Protecting Energy Privacy Across the Public/Private Divide*, 72 FLA. L. REV. 452, 480, 496 (2020) (referring to *Carpenter* as a "sharp break" with prior law); Rachel Levinson-Waldman, *Supreme Court Strengthens Digital Privacy*, BRENNAN CTR. FOR JUST. (June 22, 2018), https://www.brennancenter.org/our-work/analysis-opinion/supreme-court-strengthens-digital-privacy (calling *Carpenter* a "landmark privacy case.").

[16] Lior Strahilevitz & Matthew Tokson, *Ten Thoughts on Today's Blockbuster Fourth Amendment Decision — Carpenter v. United States*, CONCURRING OPS., June 22, 2018, https://perma.cc/Y94X-PTXR.

[17] Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 360 (2019).

[18] *Carpenter*, 138 S. Ct. at 2217 n.3 (noting that the government had sought location data from one cellular provider for seven days, although it ultimately obtained data for only two days).

[19] Among the considerations the court discussed were the "deeply revealing nature of [cell phone location data], its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection," as well as the low cost of monitoring individuals via cell phone tracking. *Id.* at 2216–18, 2223.

uncertain,"[20] with numerous issues left to be decided by the lower courts.[21]

Over time, however, a clear *Carpenter* test has begun to emerge from the hundreds of lower court decisions applying the case. It consists of three factors: The revealing nature of the data collected; the amount of data collected; and whether the suspect voluntarily disclosed their information to others.[22] These factors have appeared in a large proportion of substantive post-*Carpenter* cases, and their guidance correlates strongly with case outcomes.[23]

This Essay grapples with the questions raised by the emerging *Carpenter* test and the uncertain future of Fourth Amendment law. It examines the current state of post-*Carpenter* jurisprudence. The *Katz* test and the *Carpenter* test often operate simultaneously in the caselaw, with courts applying concepts from both in various combinations. The overlapping application of the two tests threatens to make Fourth Amendment search law even more chaotic. At present, there appears to be no way to predict whether a court will emphasize the *Katz* test, the *Carpenter* test, or both when resolving a Fourth Amendment search issue. Nor is there likely to be any helpful metaprinciple that can help courts select which test to use. This Essay evaluates several potential metaprinciples governing the blend of *Katz* and *Carpenter* and concludes that none of them are likely to produce an effective or desirable framework.

Yet there is an opportunity to substantially clarify Fourth Amendment search law, something judges and scholars have failed to achieve since *Katz* was decided in the late 1960s. This Essay argues that courts should adopt the emerging *Carpenter* test as a new iteration of the *Katz* test—and as a practical replacement for it. *Carpenter* creates a specific, concrete test that lower courts have successfully applied in numerous cases. It is far more predictable than the *Katz* standard, because each of its factors produces discernable answers. It is based on sound theoretical claims regarding revealing, voluminous, and voluntarily disclosed information. And its factors are not experimental or wholly novel; each one is grounded in Supreme Court precedents decided over the past several decades.[24] This Essay identifies the theoretical and

---

[20] Daniel Solove, Carpenter v. United States*, Cell Phone Location Records, and the Third Party Doctrine*, TEACH PRIV. (July 1, 2018), https://teachprivacy.com/carpenter-v-united-states-cell-phone-location-records-and-the-third-party-doctrine.

[21] Evan Caminker, *Location Tracking and Digital Data: Can* Carpenter *Build A Stable Privacy Doctrine?,* 2018 SUP. CT. REV. 411, 451 (2018).

[22] Matthew Tokson, *The Aftermath of* Carpenter*: An Empirical Study of Fourth Amendment Law, 2018–2021*, at 135 HARV. L. REV. (forthcoming 2022) (manuscript at 34) (on file with author). Technically, the test looks to the amount of data sought rather than the amount of data actually collected, although the amount of data sought and collected will often be identical. For instance, the *Carpenter* Court assessed the duration of surveillance based on the seven days of location information the government requested, rather than the two days of information they were ultimately able to obtain. *Carpenter*, 138 S. Ct. at 2217 n.3.

[23] Tokson, *supra* note 22 (manuscript at 28–29).

[24] For a discussion of these precedents and their relationship to the *Carpenter* factors, *see infra* Part III.B.

jurisprudential foundations of the *Carpenter* test, tracing its origins to prior applications of Fourth Amendment law and connecting each of its factors to theories of surveillance harm.

The *Carpenter* test can also be used, and has already been used, to address a variety of situations beyond the classic third-party disclosure scenario addressed in *Carpenter*. Its conceptual reach is universal. There is, accordingly, little reason to continue applying *Katz*'s vague reasonable expectation of privacy standard, even in concert with *Carpenter*. To do so only perpetuates the confusion that has plagued courts, law students, and anyone who seeks to understand the Constitution's restrictions on government surveillance.

Moreover, *Carpenter*'s continuity with prior law should ease the transition to the new test and allow most of the Supreme Court's Fourth Amendment precedents to remain influential. *Carpenter* represents an important evolution in Fourth Amendment law, not a sharp break with the past. Yet its new approach gives police officers and prosecutors a test to consider rather than a vague principle to disregard. It gives judges tangible guidance rather than a series of disjointed decisions. And it enables legal actors and observers to understand Fourth Amendment search law as something other than an ineffable mystery.[25]

This Essay proceeds in three parts. Part I gives an overview of current Fourth Amendment law, and the *Katz* and *Carpenter* tests. Part II describes the overlapping and competing nature of the two tests in the lower courts. It then evaluates several potential metaprinciples that might be used to determine which test should apply in various situations. Drawing on this analysis, Part III makes the argument that the *Carpenter* test should be used as the primary test for Fourth Amendment searches going forward. It also evaluates the theoretical and jurisprudential foundations of the *Carpenter* test's factors, and describes how each is grounded in decades of Supreme Court precedents.

I. THE AMBIGUITY OF CURRENT LAW

Fourth Amendment law is the product of centuries of precedents, issued by the Supreme Court as it confronts changing surveillance practices and technologies.[26] While early acts of surveillance mostly involved physical trespasses onto a suspect's property, modern surveillance often involves collecting electronic or other data stored by third parties, or remotely recording

[25] For scholars discussing the mystery of *Katz*, see, for example, Baude & Stern, *supra* note 9, at 1825; Caminker, *supra* note 21, at 428–29; Etzioni, *supra* note 11, at 413–15; Allen & Rosenberg, *supra* note 6, at 1149–50; Solove, *supra* note 7, at 1511–12.

[26] *See, e.g.*, Boyd v. United States, 116 U.S. 616 (1886); Olmstead v. United States, 277 U.S. 438 (1928); Katz v. United States, 389 U.S. 347 (1967); *Carpenter*, 138 S. Ct. at 2217.

video or audio data.[27] The Court's precedents reflect that reality.[28] But the current state of Fourth Amendment search law is widely considered to be incoherent and ambiguous, difficult to understand and utterly lacking in predictability.[29] This section gives an overview of current law and its problems.

A. The *Katz* Test

At the heart of current Fourth Amendment law lies the *Katz* test. It determines in most cases what a Fourth Amendment "search" is, and thereby whether the Amendment applies at all.[30] The test originated in Justice Harlan's famous concurrence in *Katz v. United States*, in which he summed up the emerging doctrine of Fourth Amendment searches: "[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[31] Subsequent Supreme Court cases adopted this approach, although they often condensed it into a simpler "reasonable expectation of privacy" standard.[32]

The ambiguity and confusion associated with the *Katz* test begins with its structure. The two-pronged standard, which has the appearance of a coherent test, is anything but. Its first

---

[27] *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 741 (1979) (considering government's installation of pen register at telephone company offices to obtain record of telephone numbers dialed by the suspect); *Katz*, 389 U.S. at 348, 353 (assessing government's recording of a suspect's calls via a microphone placed on the outside of a telephone booth).

[28] *See, e.g.*, cases cited *supra* note 27.

[29] *See infra* notes 53–56 and accompanying text.

[30] The Supreme Court has recently adopted a separate test that finds a Fourth Amendment search when a government official physically intrudes on certain types of property for the purpose of gathering information. *See* Florida v. Jardines, 569 U.S. 1, 7–10 (2013); United States v. Jones, 565 U.S. 400, 404–06 (2012). This has, thus far, added little to the *Katz* test, and the Supreme Court cases where it has been employed would likely have reached the same outcome under *Katz*. *See Jardines*, 569 U.S. at 12–16 (Kagan, J., concurring); *Jones*, 565 U.S. at 418–31 (Alito, J., concurring). It has also rapidly become confusing and difficult to apply, for instance when the Supreme Court had to determine the extent of an implied social license to enter the curtilage of a home—a question bound up in a social norms inquiry similar to and possibly even more amorphous than those that occur under the *Katz* test. *Jardines*, 569 U.S. at 10; George M. Dery III, *Failing to Keep "Easy Cases Easy":* Florida v. Jardines *Refuses to Reconcile Inconsistencies in Fourth Amendment Privacy Law by Instead Focusing on Physical Trespass*, 47 LOY. L.A. L. REV. 451, 471–79 (2014).

[31] *Katz*, 389 U.S. at 361 (Harlan, J., concurring). Under this test, Harlan concluded, recording a suspect's phone calls violated his Fourth Amendment rights. *Id.*

[32] *See, e.g.*, Oliver v. United States, 466 U.S. 170, 178 (1984) (holding that "a search proscribed by the [Fourth] Amendment" occurs when certain government intrusions "violate[] reasonable expectations of privacy"); *Smith*, 442 U.S. at 740, 742–44 (applying the two-pronged version of the *Katz* test); Terry v. Ohio, 392 U.S. 1, 9 (1968) ("[W]herever an individual may harbor a reasonable 'expectation of privacy,' he is entitled to be free from unreasonable governmental intrusion." (citation omitted)).

prong turns out not to matter either conceptually or in practice.[33] Any suspect seeking to suppress evidence likely had a subjective expectation of privacy—they did not expect that evidence of their crimes would be discovered.[34] So courts might as well just skip to the second prong of the test. In fact, modern courts largely ignore the first prong of *Katz*.[35]

That leaves the condensed version, which focuses on an objectively "reasonable expectation of privacy." But this standard does not mean what it says. On its face, it would seem to involve an assessment of the probability of detection—how likely is it that a person's privacy will be violated? Yet there are numerous cases where the Supreme Court ignores the probability of detection and assesses Fourth Amendment searches based on some other criteria, such as the normative value of the privacy at stake.[36] In addition, the literal test suggests that the government could circumvent the Fourth Amendment by announcing a new, invasive surveillance program, thereby changing people's expectations. The Court has indicated that it would not allow such a practice to affect the Fourth Amendment's scope.[37] Indeed, the Court has overtly stated that the *Katz* test cannot be taken literally.[38]

Accordingly, courts applying *Katz* only occasionally concern themselves with probabilistic assessments of the likelihood of something remaining private.[39] They also typically ignore societal attitudes regarding privacy, which are often available in surveys or inferable from circumstances.[40] The Supreme Court has permitted warrantless invasions of things that people

---

[33] Orin S. Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 115 (2015); Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 385–88 (1974).

[34] Likewise, any individual suing the government for violations of Fourth Amendment privacy under *Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics*, 403 U.S. 388 (1971), or under 42 U.S.C. § 1983 (West 2021), likely subjectively expected their privacy not to be violated.

[35] Kerr, *supra* note 33, at 122.

[36] *E.g.*, Illinois v. Caballes, 543 U.S. 405, 408–09 (2005); United States v. Jacobsen, 466 U.S. 109, 118–22 (1984); United States v. White, 401 U.S. 745, 751–52 (1971) (plurality opinion). Consider the Court's hypothetical involving someone burgling a remote cabin in the woods. The burglar reasonably expects privacy as a probabilistic matter, but still does not get Fourth Amendment protection, because his expectation is not a reasonable one per society's normative judgment, which is apparently part of the test. Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978).

[37] *Smith*, 442 U.S. at 740 n.5 (noting that a normative inquiry would be necessary in situations where expectations are shaped by government behavior).

[38] *See Rakas*, 439 U.S. at 143 n.12 (1978) (stating that one's literal expectation of privacy—such as for a "burglar plying his trade in a summer cabin during the off season"—is irrelevant to the court's assessment of a reasonable and constitutionally "legitimate" expectation).

[39] *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 511 (2007).

[40] *See, e.g.*, Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205, 237 (2015) (finding that, in contrast to Mosaic Theory

expect to be private (financial records, household trash, a backyard, a friend's purse) and protected far less private things (the underside of stereo equipment, a shared work office).[41]

What does the Court consider in its many subsequent cases applying the *Katz* test? The scholarly consensus is that it applies a series of contradictory concepts, and does so unpredictably and seemingly at random.[42] In some cases, the Court looks to the actual probability of exposure of private information.[43] In others, it employs a "private facts" model that asks whether the information found by the government was particularly private.[44] In a third set of cases, the Court looks to other sources of law and finds a search only when the police conduct at issue violates such law.[45] In a fourth set of cases, the Court engages in policy balancing, weighing the costs and benefits of allowing suspicionless government searches.[46] To this standard account we might add a fifth set of cases involving social norms and practices, which the Court has overtly invoked as a basis for reasonable expectations of privacy in some opinions.[47] The Court applies these models inconsistently, ignoring or repudiating them in

---

used by many courts, ordinary Americans do not consider duration of surveillance to be dispositive in question of whether tracking geolocation was a search); Christine S. Scott-Hayward et al., *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*, 43 AM. J. CRIM. L. 19, 46 (2015) (examining people's expectations of privacy regarding digital surveillance including cell phone records and social media); Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 335 (2008) (analyzing intrusiveness rating for 25 scenarios such as roadblocks and bedroom searches).

[41] Bernard Chao et al., *Why Courts Fail to Protect Privacy: Race, Age, Bias, and Technology*, 106 CALIF. L. REV. 263, 276–77 (2018) (discussing whether courts should take into account privacy expectations of ordinary Americans and whether consulting survey data is appropriate to determine those expectations). *Compare* United States v. Miller, 425 U.S. 435, 445-46 (1976), California v. Greenwood, 486 U.S. 35, 43 (1988), Florida v. Riley, 488 U.S. 445, 450-51 (1989), *and* Rawlings v. Kentucky, 448 U.S. 98, 104-06 (1980), *with* Arizona v. Hicks, 480 U.S. 321, 324-26 (1987), *and* Mancusi v. DeForte, 392 U.S. 364, 369-70 (1968).

[42] *See* Kerr, *supra* note 39, at 504–06; Kugler & Strahilevitz, *supra* note 40, at 221–22.

[43] Kerr, *supra* note 39, at 508–12.

[44] *Id.* at 512–15.

[45] *Id.* at 516–19.

[46] *Id.* at 519–22.

[47] *See, e.g.*, Minnesota v. Olson, 495 U.S. 91, 98–99 (1990) (holding that a guest staying overnight at a friend's house has a "legitimate expectation of privacy" because "[s]taying overnight in another's home is a longstanding social custom that serves functions recognized as valuable by society"); Minnesota v. Carter, 525 U.S. 83, 89–90 (1998) (stating that while overnight guests may have a reasonable expectation of privacy, society does not recognize the same for those who are merely present in the home for a few hours); Kyllo v. United States, 533 U.S. 27, 34 (2001) (deciding that the use of thermal imaging devices constitutes a search "at least where . . . the technology in question is not in general public use," suggesting that when social norms around technology change, society's expectations may change as well); Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978) (stating that reasonable expectations of privacy "must have a source outside of the Fourth Amendment," one grounded either in property ownership or in "understandings that are recognized and permitted by society"); Robbins v. California, 453 U.S. 420, 428 (1981) (plurality opinion) (our "[e]xpectations of privacy are established by general

some cases and overtly relying on them in others.[48] While they can help to explain and categorize *Katz* test jurisprudence, they cannot render it predictable or coherent.

In short, the Court has failed to clarify what makes an expectation of privacy "reasonable."[49] Its current test is conceptually muddled and the rationales of its cases are often contradictory.[50] In practice, *Katz* operates case-by-case, in largely atheoretical fashion.[51] It is little wonder that *Katz* is a source of confusion and difficulty for nearly all who encounter it.[52]

For these reasons and more, *Katz* has been widely criticized for decades.[53] Critics have called the test unpredictable, unworkable, and circular.[54] They have argued that courts are poorly situated to make policy decisions or assess societal views about privacy.[55] They express concern that *Katz*'s vague standard is underprotective.[56] And they criticize how post-*Katz* law addresses data disclosed to third parties.[57]

B. The Third-Party Doctrine

In the 1970s, the Supreme Court developed the "third-party doctrine," which provides that an individual has no reasonable expectation of privacy in information they disclose to a

---

social norms."), *overruled on other grounds by* United States v. Ross, 456 U.S. 798, 824 (1982). *See generally* Matthew Tokson & Ari Ezra Waldman, *Social Norms in Fourth Amendment Law*, 120 MICH. L. REV. 265, 273–74 (2021); Michael J. Zydney Mannheimer, *Decentralizing Fourth Amendment Search Doctrine*, 107 KY. L.J. 169, 210–11 (2019); William C. Heffernan, *Fourth Amendment Privacy Interests*, 92 J. CRIM. L. & CRIMINOLOGY 1, 37 (2001).

[48] Kerr, *supra* note 39, at 506–07.

[49] *Id.* at 504; Matthew Tokson, *The Emerging Principles of Fourth Amendment Privacy*, 88 GEO. WASH. L. REV. 1, 7 (2020).

[50] *See* Kerr, *supra* note 39, at 504; *see also* O'Connor v. Ortega, 480 U.S. 709, 715 (1987) (plurality opinion) ("We have no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable.").

[51] Allen & Rosenberg, *supra* note 6, at 1197–1200.

[52] *See supra* note 25; *see also* Kerr, *supra* note 39, at 504–06; Joseph D. Grano, Foreword, *Perplexing Questions About Three Basic Fourth Amendment Issues: Fourth Amendment Activity, Probable Cause, and the Warrant Requirement*, 69 J. CRIM. L. & CRIMINOLOGY 425, 429 (1978); Tokson, *supra* note 49, at 6–7, 12.

[53] Criticism of the Katz test began soon after its adoption and continued to the present day. *See, e.g.*, Amsterdam, *supra* note 33, at 384; Grano, *supra* note 52, at 429; Colb, *supra* note 11, at 121; Rubenfeld, *supra* note 10, at 103.

[54] *E.g.*, Baude & Stern, *supra* note 9, at 1825; Rubenfeld, *supra* note 10, at 132–33.

[55] *E.g.,* Solove, *supra* note 7, at 1521–22; Baude & Stern, *supra* note 9, at 1824.

[56] *E.g.,* Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139, 187 (2016); Etzioni, *supra* note 11, at 421–22; Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1325–26 (2012).

[57] *See supra* note 12.

third party.[58] For example, the Court held that the Fourth Amendment did not apply to the phone numbers that a suspect dialed, because he had disclosed those numbers to the phone company that routed his calls.[59] The police can accordingly obtain a list of anyone's dialed numbers without a warrant.[60]

In the internet era, the third-party doctrine threatens to eliminate constitutional protection for a wide variety of personal information, including emails and texts, videos and photos, location information, web-surfing data, subscriber information, biometric data, search terms, and more.[61] These and many other forms of digital information are regularly disclosed to third-party service providers.[62] Accordingly, government investigators would be able to obtain a huge variety and quantity of personal information without a warrant.[63]

The third-party doctrine has been widely criticized as underprotective of privacy and unrealistic about the necessity of information disclosure in modern life.[64] Several states have repudiated the doctrine via constitutional or statutory law.[65] However, until recently, most lower courts vigorously enforced the doctrine.[66] But a few years ago, as government surveillance of digital information was proliferating, the Supreme Court decided to reexamine the third-party doctrine and its application to new technologies.[67]

---

[58] *See, e.g.,* United States v. Miller, 425 U.S. 435, 443–44 (1976); Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

[59] *Smith*, 442 U.S. at 743–46.

[60] Matthew Tokson, *Inescapable Surveillance*, 106 CORNELL L. REV. 409, 416–17 (2021).

[61] *See* Tokson, *supra* note 22 (manuscript at 7).

[62] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

[63] Tokson, *supra* note 60, at 417. Such data is regularly stored in databases and made available to the government upon request or subpoena. *See* Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 585 (2011).

[64] CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 151–64 (2007); *see, e.g.*, Bellovin et al., *supra* note 12, at 22–31; Leary, *supra* note 12, at 379; Rubenfeld, *supra* note 10, at 113; Colb, *supra* note 11, at 155–59; Maclin, *supra* note 12, at 136.

[65] *See* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 395–405 (2006) (reporting numerous states that have rejected the third-party doctrine in whole or in part, including California, New Jersey, and Pennsylvania, among others).

[66] *See, e.g., In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (ruling that cell site data is not protected under the Fourth Amendment); United States v. Warshak, 631 F.3d 266, 330–31 (6th Cir. 2010) (finding that the third-party doctrine applies to e-mail metadata such as to/from addresses); United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008) (holding that email to/from addresses and IP addresses are not protected under the Fourth Amendment); Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174, 182–83 (D. Conn. 2005) (holding that there is no reasonable expectation of privacy in AOL subscriber information when the user permitted AOL to release the information to third parties).

[67] *See generally* Stephen E. Henderson, *After* United States v. Jones*, After the Fourth Amendment Third Party Doctrine*, 14 N.C. J.L. & TECH. 431, 432–33 (2013) (recounting the history and application of the third-party doctrine and speculating that the changing nature of technology will require the Supreme Court to limit the doctrine).

C. The *Carpenter* Test

In June of 2018, the Supreme Court decided *Carpenter v. United States*, which limited the third-party doctrine and potentially ushered in a new era of privacy protection for digital data. The Court held that government officials had to obtain a warrant before collecting a suspect's cell phone location data for a seven-day period.[68] It also overtly limited the third-party doctrine, ruling that it was inapplicable to such data despite its disclosure to a cell phone company.[69]

The Court did not set out an official test to guide future decisions. But it did identify several factors that compelled it to disregard the third-party doctrine in this context. First, the Court discussed the "deeply revealing nature" of location data,[70] which could "provide[] an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations."[71] Second, it addressed the large amount of location data collected by the government, including 101 data points per day that marked Carpenter's movements.[72] The Court emphasized how cell phone location records are generally stored for five years after collection, potentially allowing the government to access enormous databases full of detailed information about a person's movements over several years.[73] These massive quantities of data substantially increased the potential for intrusion on an individual's privacy.[74] Third, the Court mentioned that cell phone data is not voluntarily transmitted by a cell phone user but is automatically transmitted by the cell phone.[75] Likewise, using a cell phone is a largely inescapable part of modern life, so users have little choice but to use one.[76] Accordingly, any disclosure to a third party was essentially involuntary.[77]

The Court mentioned other factors and considerations as well, such as the low cost of tracking a person via their cell phone records and the large number of people potentially

---

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

[69] *Id.* at 2220.

[70] *Id.* at 2221

[71] *Id.* At 2217 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (internal quotation marks omitted)).

[72] *Id.* at 2212 & 2217 n.3.

[73] *Id.* at 2218 (noting that an individual subject to such surveillance "has effectively been tailed every moment of every day for five years"). Technically, the Court looked to the amount of data sought rather than the amount actually collected, *see* discussion *supra* note 22.

[74] *Id*. at 2220 (noting the dangers to privacy of "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years. Such a chronicle implicates privacy concerns far beyond those considered in *Smith* and *Miller*"); Tokson, *supra* note 49, at 18–19.

[75] *Carpenter*, 138 S. Ct. at 2220.

[76] *Id.*

[77] *Id.*

affected by cell phone surveillance.[78] It remained unclear which of these factors, if any, constituted a new test for Fourth Amendment searches, and if so when exactly this test should be used.[79] For example, does *Carpenter* only apply to cases involving data held by third parties, or can it be used to address direct government surveillance as well? These and several other issues were left to be resolved at a later date, or by the lower courts.[80]

Indeed, *Carpenter*'s combination of innovation and ambiguity gave lower court judges license to experiment with a variety of approaches and factors, determining for themselves which they found appropriate to address novel Fourth Amendment issues.[81] Over the several years since *Carpenter* was decided, hundreds of judges have done just that, applying *Carpenter* substantively in a wide variety of cases.[82] Over time, a coherent *Carpenter* test has emerged from this large body of law.[83]

It consists of three factors: The revealing nature of the data collected; the amount of data collected; and whether the suspect voluntarily disclosed their information to others.[84] The relative importance of these factors largely remains to be determined, but early indications are that revealing nature is the most influential of the factors, while amount is slightly more influential than voluntary disclosure.[85] In any event, all three factors appear to matter substantially to case outcomes.[86]

These factors have appeared in numerous recent cases that substantively apply *Carpenter*, according to a recent study examining every case citing *Carpenter* between its release and March 31, 2021.[87] Of the 129 cases discussing at least one *Carpenter* factor, 93 of them mentioned the revealing nature of the data collected; 116 of them mentioned the amount of data collected; and 61 of them mentioned the voluntary or involuntary nature of the data

---

[78] *Id.* at 2217–19.

[79] *E.g.*, Strahilevitz & Tokson, *supra* note 16; Orin S. Kerr, *First Thoughts on* Carpenter v. United States, REASON: VOLOKH CONSPIRACY (June 22, 2018, 12:20 PM), https://reason.com/volokh/2018/06/22/first-thoughts-on-carpenter-v-united-sta/; Solove, *supra* note 20; Kugler & Hurley, *supra* note 15, at 496.

[80] *E.g.*, Caminker, *supra* note 21, at 460.

[81] *Id.* ("[B]y embracing a broader if more uncertain approach, the majority can benefit from unleashed lower-court efforts to help map *Carpenter*'s new doctrinal paths").

[82] Tokson, *supra* note 22 (manuscript at 34).

[83] From the date of *Carpenter*'s decision on June 22, 2018, to March 31, 2021, there were 857 federal and state judgments citing *Carpenter*. *Id.* (manuscript at 15). Of these, 399 applied *Carpenter* substantively, 217 reached a yes-or-no ruling on a Fourth Amendment search question, and 129 discussed at least one of the *Carpenter* factors in reaching a determinative judgment. *Id.* (manuscript at 25). Each of these numbers is likely substantially greater for the entire time period from *Carpenter*'s publication and today.

[84] *Id.* (manuscript at 34). Technically, the test looks to the amount of data sought rather than the amount of data actually collected, but the amount of data sought and collected will often be identical. *See supra* note 22.

[85] Tokson, *supra* note 22 (manuscript at 34).

[86] *Id.* (manuscript at 34–35).

[87] *Id.* (manuscript at 15–16, 25).

disclosure at issue.[88] None of the other considerations discussed in *Carpenter* was mentioned more than 36 times.[89] Moreover, statistical analyses confirm the influence of these three factors. In a correlation analysis, they were the most strongly and significantly correlated with case outcomes.[90] In a logistic regression analysis, which controlled for the effects of the other factors, revealing nature, amount, and voluntary disclosure were the only factors that had significant effects on case outcomes.[91]

In short, these were the three factors that courts most commonly applied in post-*Carpenter* cases addressing novel Fourth Amendment issues. And they were, by far, the most important factors in determining the outcomes of these new cases. To be sure, it may take many years before the Supreme Court explicitly adopts the *Carpenter* factors as an official test, much as it took several years before the Court adopted Justice Harlan's *Katz* concurrence as an official test.[92] But there are many similarities in the early histories of the *Carpenter* and *Katz* tests, and lower courts' embrace of the *Carpenter* factors recalls lower courts' adoption of *Katz* in its early years.[93]

As an example of the application of the *Carpenter* test, consider *United States v. Diggs*, where a police officer had obtained a month's worth of GPS data from a suspect's vehicle.[94] The court examined the revealing nature of the location data, concluding that it could provide an intimate window into a person's life.[95] It discussed at length the amount of data obtained, describing the comprehensive and detailed record of Diggs's location and the potential for the

---

[88] *Id.* (manuscript at 15–16, 25, 27). The related concept of inescapability of a technology was mentioned in 36 total cases. *Id.* (manuscript at 28).

[89] *Id.* (manuscript at 28).

[90] *Id.* (manuscript at 28–29).

[91] *Id.* (manuscript at 30).

[92] *See* Smith v. Maryland, 442 U.S. 735, 740 (1979) (adopting and applying Justice Harlan's two-prong *Katz* formulation). It is also possible that the Court could never adopt the *Carpenter* factors as a test, or could repudiate *Carpenter* altogether, although that appears to be unlikely at present. Tokson, *supra* note 22 (manuscript at 36–37).

[93] *E.g.*, Ponce v. Craven, 409 F.2d 621, 625 (9th Cir. 1969) (applying the *Katz* test to evaluate the search of a motel room); Gov't of Virgin Islands v. Berne, 412 F.2d 1055, 1061 (3d Cir. 1969) (applying the *Katz* test to an automobile search). Examples of cases applying the *Carpenter* test are discussed below.

[94] United States v. Diggs, 385 F. Supp. 3d 648, 649 (N.D. Ill. 2019). The GPS tracking device was already installed in the vehicle at issue; the police then accessed his GPS records via the company that serviced the device. *Id.* at 650. *See also, e.g.*, State v. Eads, 154 N.E.3d 538, 548 (Ohio Ct. App. 2020). In the *Eads* case, a highway patrol officer obtained blood test records for a man who had crashed his car and was treated in a nearby hospital. The court examined the revealing nature of the records sought, determining that they provided an intimate window into Eads's life. It noted the substantial amount of data collected, which went beyond alcohol level and measured various legal and illegal substances in his blood, breath, and urine. And the court determined that Eads did not voluntarily convey this information to the hospital, because he was unconscious at the time the tests were performed. Accordingly, under *Carpenter*, the officer's collection of these records was a Fourth Amendment search that required a warrant. *Id.* at 541, 547–49.

[95] *Id.* at 653.

police to access vast quantities of data retained by the GPS service provider.[96] Further, the court noted that the car's owner did not voluntarily disclose the car's historical GPS data to a third party; the governing contract only allowed the third party access to the car's present location and only in case of default or emergency.[97] Accordingly, under *Carpenter*, the officer's collection of this data was a Fourth Amendment search that required a warrant.[98]

Likewise, in *United States v. Gratkowski*, the court addressed the novel question of a defendant's Fourth Amendment interest in a virtual currency exchange's records of his Bitcoin transactions. The court reasoned that the records were not intimate or revealing; were limited and generic rather than comprehensive or detailed; and were voluntarily provided to the currency exchange through an affirmative act by the user, in contrast to the cell phone data in *Carpenter*.[99] Accordingly, the government's collection of these transaction records was not a Fourth Amendment search.[100]

The factors of 1) revealing nature of the data; 2) amount of data collected; and 3) voluntary or involuntary nature of any disclosure do not appear together in every relevant post-*Carpenter* case. But they do appear frequently in cases applying *Carpenter* in depth, and they appear to drive case outcomes.[101] Together, they make up an emerging three-factor test with powerful influence in current caselaw and the potential to guide courts in a wide variety of future Fourth Amendment cases.[102]

II. THE UNEASY RELATIONSHIP BETWEEN *KATZ* AND *CARPENTER*

Fourth Amendment law is in a sort of limbo, stuck between two paradigms. The *Katz* test is well-established in the caselaw and continues to apply to Fourth Amendment search questions as a doctrinal matter.[103] But it is vague and unhelpful, a generic reasonableness test that fails to guide courts' analyses of novel Fourth Amendment questions.[104] The *Carpenter*

---

[96] *Id.* at 652–53.

[97] *Id.* at 660. This discussion arose in the context of the good faith exception analysis, where it was central to the court's granting of relief to the defendant. The Court analyzed and applied *Carpenter* extensively in this portion of its opinion as well. *Id.* at 660–61.

[98] *Id.* at 655, 661.

[99] United States v. Gratkowski, 964 F.3d 307, 312–13 (5th Cir. 2020).

[100] *Id.* at 312.

[101] Tokson, *supra* note 22 (manuscript at 25, 29).

[102] *Id.* (manuscript at 34, 36).

[103] Although the *Carpenter* opinion engages in relatively little discussion of the *Katz* test, it does refer to it as the overarching, governing framework of Fourth Amendment search analysis. Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018).

[104] *See supra* Part I.A.

test is far clearer.[105] It is based on three relatively concrete factors that courts can effectively assess and have effectively assessed in numerous cases over the past several years.[106] But when the *Carpenter* test should apply remains unclear.

This Part examines the current state of post-*Carpenter* caselaw, with an emphasis on the continuing influence of the *Katz* test and its concepts of reasonableness and privacy. It concludes that the overlapping paradigms of *Katz* and *Carpenter* threaten to throw Fourth Amendment law into even greater disarray.

A. Two Overlapping Frameworks

The *Katz* test and the *Carpenter* test currently operate simultaneously in Fourth Amendment search law. Their relationship to each other remains undefined by the Supreme Court. In the absence of a framework for choosing among these approaches, lower courts can choose to emphasize one or the other, or both, in a variety of configurations. The current era of Fourth Amendment law is characterized by a diversity of approaches to *Katz* and *Carpenter*, and a profound uncertainty as to how to coherently apply their concepts to novel Fourth Amendment questions.

Some courts continue to primarily apply the *Katz* test, not mentioning *Carpenter* or doing so only in passing.[107] For example, in *United States v. Fanning*, the court held that the government could warrantlessly install a telephone pole camera near a warehouse where Fanning worked.[108] Applying classic *Katz* analysis, the court reasoned that Fanning possessed no legitimate expectation of privacy in a public area and had taken no steps to protect himself from view or otherwise manifest his expectation of privacy.[109]

Other courts have largely ignored the *Katz* test and focused primarily on the *Carpenter* factors in addressing new Fourth Amendment questions.[110] In *United States v. Tolbert*, for

---

[105] *See supra* Part I.C; *infra* Part III.A.

[106] Tokson, *supra* note 22 (manuscript at 34).

[107] *See, e.g.*, United States v. Norris, 942 F.3d 902 (9th Cir. 2019); United States v. Bronner, No. 3:19-cr-109-J-34JRK, 2020 BL 240436 (M.D. Fla. May 18, 2020).

[108] United States v. Fanning, No. 1:18-CR-362-AT-CMS, 2019 WL 6462830, at *1, *4 (N.D. Ga. May 28, 2019).

[109] *Id.* at *4. *Katz* analyses sometimes focus on the steps that a suspect takes to demonstrate their expectation of privacy, although as is typical for *Katz* concepts, this one is conceptually dubious and only inconsistently applied. *Compare* Katz v. United States 389 U.S. 347, 352 (1967) (emphasizing that Katz took steps to protect himself against eavesdropping), *with* Florida v. Riley, 488 U.S. 445, 448–50 (1989) (no reasonable expectation of privacy in a greenhouse in a backyard despite the owner's protecting it with several high fences and a "DO NOT ENTER" sign), *and* California v. Ciraolo, 476 U.S. 207, 213–14 (1986) (no reasonable expectation of privacy in the backyard of a home despite the homeowner enclosing it with high double fences).

[110] *See, e.g.*, United States v. Cox, 465 F. Supp. 3d 854, 856 (N.D. Ind. 2020); Holder v. State, 595 S.W.3d 691, 703–704 (Tex. Crim. App. 2020).

instance, the court held that subscriber information, IP connection logs, and a list of friends associated with two AOL accounts was not protected by the Fourth Amendment.[111] Its opinion evaluated the *Carpenter* factors in some detail, concluding that the information at issue was unprotected because it was not intimate or revealing, was limited in amount, and was generated by Tolbert's affirmative, voluntary acts.[112] The court did not cite *Katz* or apply its test.

Finally, many courts use a blend of *Katz* and *Carpenter* concepts, conceptualizing and configuring these tests in various ways in the course of evaluating new Fourth Amendment issues.[113] For example, in *United States v. Gayden*, the Eleventh Circuit combined the *Katz* and *Carpenter* frameworks with an emphasis on the primacy of *Katz*, first invoking the reasonable expectation of privacy test and the third-party doctrine and then applying *Carpenter* as a refinement of these concepts.[114] In *Bailey v. State*, the court mostly relied on a *Carpenter* analysis but folded it into the larger *Katz* framework, weaving concepts of subjective and objective expectations of privacy into its *Carpenter* analysis.[115] Other cases have used different tests to address different aspects of government surveillance, applying the *Katz* test to publicly exposed data and the *Carpenter* test to data exposed only to a single third-party.[116] The potential permutations are virtually limitless.

In all of these cases, the relative influence of the *Katz* and *Carpenter* tests seems to be largely a matter of judicial whim. No metaprinciples have arisen to govern when each test should be used, and no guidance can be found in the Supreme Court's cases. Nor have any clear patterns emerged in the broader caselaw. Both tests are used to address simple surveillance practices *and* advanced digital technologies;[117] both tests are used to address third-party data *and* direct government surveillance.[118] In the face of this uncertainty, litigants are also likely

---

[111] United States v. Tolbert, No. 14-3761, 2019 WL 2006464, at *3 (D.N.M. May 7, 2019).

[112] *Id.*

[113] *See, e.g.*, United States v. Gbenedio, No. 1:17-CR-430-TWT-JSA, 2019 WL 2177943, at *3 (N.D. Ga. Mar. 29, 2019).

[114] United States v. Gayden, 977 F.3d 1146, 1151–52 (11th Cir. 2020); s*ee also* People v. Tafoya, 494 P.3d 613, 622–23 (Colo. 2021) (applying concepts used in *Carpenter* such as amount and revealing nature in the context of an application of the *Katz* framework).

[115] Bailey v. State, 311 So. 3d 303, 310–11 (Fla. Dist. Ct. App. 2020).

[116] United States v. Gratkowski, 964 F.3d 307, 311–13 (5th Cir. 2020).

[117] *See, e.g.*, *Gbenedio*, 2019 WL 2177943, at *1 (applying *Katz* to surveillance camera footage); *Gratkowski*, 964 F.3d at 311–13. (applying the *Katz* test to digital data stored on a blockchain); State v. Eads, 154 N.E.3d 538, 541 (Ohio Ct. App. 2020) (applying *Carpenter* to blood and urine samples taken for medical purposes); United States v. Kidd, 394 F. Supp. 3d 357, 364–65 (S.D.N.Y. 2019) (applying *Carpenter* to the collection of a large volume of IP address information associated with a cell phone).

[118] *See, e.g.*, *Gayden*, 977 F.3d at 1151–52 (applying *Katz* to prescription drug data held by a third party); United States v. Bronner, No. 3:19-cr-109-J-34JRK, 2020 BL 240436, at *21–22, *24 (M.D. Fla. May 18, 2020)

motivated to argue under both the *Katz* and *Carpenter* tests, possibly to the detriment of the clarity of their arguments.[119] It is, in short, a free-for all.

B. Potential Metaprinciples for Selecting a Fourth Amendment Framework

If Fourth Amendment law is to be made coherent, courts must determine which test to apply when faced with a novel Fourth Amendment question. They might select one or the other test as the dominant approach. Or they might establish a metaprinciple that determines which test to employ in various situations. This Section surveys some possible metaprinciples for determining which test should govern Fourth Amendment cases.

1. Limiting *Carpenter* to Third-Party Data

Carpenter addresses data held by a private third party, and it plausibly might be limited to cases where a suspect's data has been disclosed to a private entity.[120] Yet there is little reason to interpret *Carpenter* so narrowly, particularly if we consider its test to be clearer and more coherent than the *Katz* standard.[121] Conceptually, the *Carpenter* test fits direct government surveillance well, about as well as it fits data-gathering from third parties.[122] Its first two factors, the deeply revealing nature of the data and the amount of data collected, operate similarly regardless of whether the data was collected by the government or a third party. The *Carpenter* test's third factor is potentially less suited to direct surveillance, because it focuses on whether the data was voluntarily disclosed to another party.[123] But in situations where there has been no voluntary exposure of information to anyone, courts can weigh this factor in the suspect's

(applying *Katz* to the government's installation of a telephone pole camera); Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521 (7th Cir. 2018) (applying *Carpenter* to smart utility meter data stored by a third party); United States v. Harris, No. 17-cr-175-pp, 2021 WL 268322, at *3 (E.D. Wisc. Jan. 27, 2021) (applying *Carpenter* to the government's installation of surveillance cameras).

[119] For examples of briefs citing both the *Katz* and *Carpenter* tests, albeit with admirable eloquence, see, for example, Petition for a Writ of Certiorari at 19–23, United States v. Tuggle, 4 F.4th 505 (2021) (No. 21-541), 2021 WL 4790611; Reply of Defendant-Appellant at 8–9, 11–14, United States v. Morel, 922 F.3d 1 (2019) (No. 17-1696), 2019 WL 1434348.

[120] *See* Caminker, *supra* note 21, at 457–58 (discussing *Carpenter*'s potential applications solely in the context of third party data); Ohm, *supra* note 17, at 392–93 (criticizing the view of *Carpenter* as limited to only third-party data scenarios).

[121] *See infra* Part III.A.

[122] Ohm, *supra* note 17, at 392.

[123] *See supra* text accompanying notes 75–76.

favor. For instance, if the police use some new technology[124] to observe activities inside of a building, they are obtaining information that the suspect has not voluntarily exposed to outside observation. This should weigh in favor of finding a Fourth Amendment search. In situations where individuals voluntarily expose their activities to direct observation, this factor would favor the government—for example if a suspect were bagging drugs on a picnic table in a public park.

The *Carpenter* test can even work in classic Fourth Amendment scenarios involving physical intrusion into a private place rather than technological data collection. In these situations, the deeply revealing factor can work as an "intimacy" factor, assessing the intimacy or sensitivity of the place examined by the police.[125] Indeed, the Supreme Court linked intimacy and revealing nature in *Carpenter* itself.[126] Future courts can also draw on the Court's extensive caselaw analyzing the intimacy of various locations, including homes, yards, fields, commercial spaces, and public streets.[127] In any event, most physical searches of a person's property are now *per se* searches under the Supreme Court's recently revived trespass test.[128]

---

[124] Brad Heath, *New Police Radars Can "See" Inside Homes*, U.S.A. TODAY (Jan. 19, 2015, 6:26 PM), https://www.usatoday.com/story/news/2015/01/19/police-radar-see-through-walls/22007615/; DEP'T OF JUST., THROUGH-THE-WALL SENSORS FOR LAW ENFORCEMENT: BEST PRACTICES 9–13 (2014), https://www.ojp.gov/pdffiles1/nij/nlectc/245746.pdf. *See generally* Kyllo v. United States, 533 U.S. 27 (2001).

[125] *See infra* notes 176–183 and accompanying text on the shared conceptual and doctrinal roots of revealing nature and intimacy.

[126] *Carpenter* at 2217 (discussing how location data can "provide[] an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations.") (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (internal quotation marks omitted)). *See also, e.g.*, United States v. Gratkowski, 964 F.3d 307, 312 (5th Cir. 2020) (analyzing the intimacy of financial records under a *Carpenter* analysis); United States v. Diggs, 385 F. Supp. 3d 648, 653 (N.D. Ill. 2019) (discussing the intimate, revealing nature of GPS data under a *Carpenter* analysis). To be sure, the *Carpenter* standard may be somewhat in tension with older cases involving open fields or undercover agents. But even those cases regularly incorporated principles similar to those discussed in *Carpenter*. Open fields cases such as *Oliver v. United States*, 466 U.S. 170 (1984), and *United States v. Dunn*, 480 U.S. 294 (1987), emphasize the intimacy of the places and information at issue—a concept quite close to "revealing nature." *See supra* note 125 and accompanying text. For instance, *Oliver* concluded that "open fields do not provide the setting for those intimate activities that the Amendment is intended to shelter from government interference or surveillance." *Oliver*, 466 U.S. at 179. *See also Dunn*, 480 U.S. at 302 ("It is especially significant that the law enforcement officials possessed objective data indicating that the barn was not being used for intimate activities of the home."). In addition, the undercover agent case *United States v. White*, 401 U.S. 745 (1971), depended heavily on voluntary disclosure concepts. The voluntary disclosure at issue in the case could arguably outweigh the deeply revealing and somewhat voluminous nature of the data collected, although *White* may be an example of a case suitable for reconsideration under *Carpenter*.

[127] *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 31, 37 (2001) (the home); Florida v. Riley, 488 U.S. 445, 452 (1989) (the yard); Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986) (commercial property); United States v. Karo, 468 U.S. 705, 715 (1984) (public streets); Oliver v. United States, 466 U.S. 170, 179 (1984) (open fields).

[128] Florida v. Jardines, 569 U.S. 1, 4 (2013); United States v. Jones, 565 U.S. 400, 404–05 (2012).

The types of surveillance to which *Carpenter* is ideally suited are those most likely to arise in modern Fourth Amendment cases: non-physical captures of data via new surveillance technologies.

Lower courts have already applied *Carpenter* to direct government surveillance without apparent difficulty. *Carpenter* has been used to assess the installation of surveillance cameras in an apartment hallway;[129] ankle monitors attached to probationers;[130] telephone pole cameras pointed at a suspect's house;[131] surveillance airplanes observing an entire city;[132] automatic license plate readers (ALPRs);[133] and more.[134] There is no significant theoretical or practical obstacle to using *Carpenter* to address direct surveillance.

2. Limiting *Carpenter* to Digital Data

Orin Kerr has argued that *Carpenter* should only apply to digital-age forms of data.[135] Kerr's argument is largely doctrinal; he believes that *Carpenter* itself was directed only towards digital data, which it treated as categorically different from analog data.[136] As evidence for this, he notes that the Court did not overturn its pre-digital precedents involving dialed phone numbers or bank records, which arguably shared many characteristics with the cell phone location data at issue in *Carpenter*.[137] Kerr also defends the distinction as embodying a qualitative difference between digital records, which are efficiently stored and widely distributed, and non-digital records, which tend to be more limited in storage and distribution.[138]

But the distinction between digital and non-digital records is largely arbitrary and difficult to defend. Kerr concedes that the distinction does a poor job of distinguishing police practices that invade privacy from those that do not, acknowledging that "[m]any longstanding

---

[129] United States v. Harris, 2021 WL 26832, at *3 (E.D. Wisc. Jan. 27, 2021).

[130] Commonwealth v. Johnson, 119 N.E.3d 669, 675-76, 683-86 (Mass. 2019).

[131] People v. Tafoya, 490 P.3d 532, 542 (Colo. App. 2019).

[132] Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 341 (4th Cir. 2021).

[133] Commonwealth v. McCarthy, 142 N.E.3d 1090, 1101 (Mass. 2020).

[134] *See, e.g.*, United States v. Gbenedio, No. 1:17-CR-430-TWT-JSA, 2019 WL 2177943, at *3 (N.D. Ga. Mar. 29, 2019); United States v. Kubasiak, No. 18-cr-120-pp, 2018 WL 4846761, at *3–4 (E.D. Wis. Oct. 5, 2018); State v. Bunce, No. 119,048, 2020 WL 122642, at *1, *4 (Kan. Ct. App. Jan. 10, 2020).

[135] Orin S. Kerr, *Implementing* Carpenter, *in* THE DIGITAL FOURTH AMENDMENT (forthcoming) (manuscript at 16), https://ssrn.com/abstract=3301257.

[136] Kerr quotes the Supreme Court's reference to cell phone location information as "an entirely different species" of data, emblematic of the "new concerns wrought by digital technology" and therefore not covered by existing precedents. *Id.* (citing Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018)).

[137] Kerr, *supra* note 135 (manuscript at 17).

[138] *Id.* (manuscript at 18–19, 44) (describing digital messaging to/from information as "different because the Internet facilitates and stores communications on a scale never before seen").

investigative practices invade privacy, often more than newer techniques."[139] While digital data can be stored in large quantities and searched easily, the same is increasingly true of pre-digital records, which are often easy to digitize, store, and search.[140] Finally, the line between digital and pre-digital data types is often fuzzy and would "require some hard judgment calls" to implement.[141] Likewise, many old forms of data have been substantially transformed by the digital age, arguably granting them the status of digital data.[142] The medium of information storage is not a stable or especially meaningful category in this context. There is, in short, little reason to adopt a distinction between digital and pre-digital data as a metaprinciple for choosing between *Carpenter* and *Katz*. The line is difficult to draw intelligibly, does not track concerns about privacy or security against government abuse, and is partially duplicative of the amount inquiry already embodied in the *Carpenter* test.

Unsurprisingly, courts have not adopted a distinction between digital and non-digital data in cases applying *Carpenter*. Rather, they regularly apply *Carpenter* to non-digital searches, including the examination of a purse, analysis of blood and urine samples, traditional video surveillance, and more.[143] Digital technology cases are common in the post-*Carpenter* caselaw, but the test appears to be applicable to a wide variety of technologies and surveillance techniques.[144]

---

[139] *Id.* (manuscript at 17).

[140] *E.g.*, Bill Atkinson, *Petersburg Plans to Digitally Preserve Court Records, Some of Which are Centuries Old*, PROGRESS INDEX (Dec. 24, 2021, 6:30 AM), https://www.progress-index.com/story/news/2021/12/24/petersburg-va-court-uses-grant-money-digitize-centuries-old-records/9000690002/; Nicholas Fearn & Brian Turner, *Best Document Scanning Apps of 2022*, TECH RADAR (Dec. 3, 2021), https://www.techradar.com/best/best-document-scanning-apps. In addition, Kerr concedes that "[d]igital networks work like any [analog] network in some ways, of course. They send and receive communications, substituting for in-person transaction, just like the traditional postal network and telephone network." Kerr, *supra* note 135 (manuscript at 18). The most relevant difference is that digital records are easier to collect and store on a large scale. *Id.* (manuscript at 19, 44). But it is the large quantity and revealing nature of data that implicates privacy, not whether the data is in digital form or on paper.

[141] *Id.* (manuscript at 19).

[142] Kugler & Hurley, *supra* note 15, at 487.

[143] *E.g.*, Speidell v. IRS, 978 F.3d 731, 736, 743–44 (10th Cir. 2020) (applying *Carpenter* to business records of a marijuana business); State v. Bunce, No. 119,048, 2020 WL 122642, at *1, *4 (Kan. Ct. App. Jan. 10, 2020) (applying *Carpenter* to the warrantless search of a purse); State v. Eads, 154 N.E.3d 538, 541 (Ohio Ct. App. 2020) (applying *Carpenter* to blood and urine samples taken for medical purposes); People v. Tafoya, 490 P.3d 532, 534-35, 542 (Colo. App. 2019) (applying *Carpenter* and holding that the Fourth Amendment prohibited the warrantless video surveillance of a home).

[144] Tokson, *supra* note 22 (manuscript at 34).

3. Limiting *Katz* to Public Exposure

Lower court cases applying *Carpenter* and *Katz* together suggest another possible approach: primarily applying the *Carpenter* test, while still using *Katz* to evaluate data that is publicly exposed and therefore not private. In cases like *United States v. Gbenedio*[145] and *Bailey v. State*,[146] courts mainly applied *Carpenter* but then employed *Katz*'s concept of general exposure to the public to conclude that a suspect lacked a reasonable expectation of privacy in their movements in public. The benefit of this approach is that it helps keep "easy cases easy"[147] by allowing courts to quickly resolve cases where suspects plainly exposed their movements or data to public observation. In *Gbenedio*, for example, the defendant sought to suppress surveillance camera footage obtained from a camera in a commercial strip mall. The court "easily"[148] found that the defendant lacked a reasonable expectation of privacy in part because his comings and goings in the strip mall were exposed to the public.[149]

But focusing a Fourth Amendment analysis on public exposure ultimately carries more risks than benefits. A core insight of *Carpenter* was that "the whole of [an individual's] physical movements" are private and deserving of Fourth Amendment protection, even if they occur in public.[150] The entirety of one's movements is theoretically observable but practically obscure, and the elimination of this obscurity violates a person's privacy.[151] The classic *Katz* focus on public exposure threatens to undermine this principle, as it suggests that activities observable by members of the public can never receive Fourth Amendment protection.[152] Courts applying a blend of *Carpenter* and *Katz* in public exposure cases may too readily deny Fourth Amendment protection to activities in public.[153] The better approach is to do as the Supreme Court did in *Carpenter*, evaluating information allegedly exposed to the public to see whether it is deeply revealing, voluminous, and voluntarily exposed to others. In many cases,

---

[145] No. 1:17-CR-430-TWT-JSA, 2019 WL 2177943, at *3 (N.D. Ga. Mar. 29, 2019).

[146] 311 So. 3d 303, 310–11, 315 (Fla. Dist. Ct. App. 2020).

[147] Florida v. Jardines, 569 U.S. 1, 11 (2013).

[148] *Gbenedio*, 2019 WL 2177943, at *2.

[149] *Id.* ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." (citing Katz v. United States, 389 U.S. 347, 351 (1967))).

[150] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

[151] *Id.*; *see generally* Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1346 (2015).

[152] *Cf. Carpenter*, 138 S. Ct. at 2231 (Kennedy, J., dissenting) (conceding that an individuals' activities in public should receive constitutional protection against dragnet-type surveillance, but contending that the classic approach of withholding protection from movements on public roads should apply in the context of cell phone tracking conducted under a sensible statutory regime).

[153] *E.g.*, Bailey v. State, 311 So.3d 303, 307, 315 (Fla. Dist. Ct. App. 2020) (holding that the Fourth Amendment did not apply to GPS location data showing movements on public roads, based in part on an application of *Katz* and its progeny).

information that might in theory have been observable by the public will be practically private, because no member of the public would ever obtain the quantity or type of data obtained by the government.[154] Classifying such data as publicly exposed would be an error, one that could lead to substantial underprotection of sensitive personal information.[155] Applying the *Carpenter* test without relying on older *Katz* concepts avoids this pitfall and more effectively centers the analysis on government privacy violations and potential abuses of power.[156]

Having evaluated several potential metaprinciples for blending *Katz* and *Carpenter*, this Article next explores a more transformative approach: using the *Carpenter* test exclusively, as a functional replacement for the *Katz* test.

III. TRANSFORMING FOURTH AMENDMENT LAW

The *Carpenter* test is better suited than the *Katz* test for determining when a government action constitutes a Fourth Amendment search. The first Part of this Essay summarized the *Katz* test's flaws, which are profound.[157] The second Part detailed the problems associated with potential combinations of the *Katz* and *Carpenter* tests.[158] This Part makes the case for adopting the *Carpenter* test as the exclusive test for non-trespassory Fourth Amendment searches.[159]

A. *Carpenter* as the Primary Fourth Amendment Search Test

The *Carpenter* test presents a unique opportunity for courts to substantially clarify Fourth Amendment search law, something they have been unable to achieve since *Katz* was decided. The *Carpenter* framework is more substantive, predictable, and structured than *Katz*'s vague

---

[154] *See Carpenter*, 138 S. Ct. at 2217 (stating that monitoring the whole of a person's movements over any extended period of time was not possible prior to the digital age and accordingly violates an individual's privacy); *id.* at 2217–18 (discussing the sensitive personal activities that location data can reveal); United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring in judgment) ("[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.").

[155] *See Carpenter*, 138 S. Ct. at 2217–18.

[156] Ohm, *supra* note 17, at 390.

[157] *See supra* Part I.A.

[158] *See supra* Part II.

[159] I am indebted here to Paul Ohm's prescient argument in favor of *Carpenter* over *Katz* shortly after *Carpenter* was decided. To be sure, Ohm proposed a *Carpenter* test different from the one that has emerged from the lower courts and considered *Carpenter* a revolutionary, technology-centered break from prior law rather than an evolution of that law. Ohm, supra note 17, at 359–60. But he recognized the importance and transformative potential of the *Carpenter* test almost as soon the decision was issued. His analysis was an inspiration and foundation for this Essay.

reasonableness standard.[160] Indeed, *Carpenter* distills the amorphous concepts of *Katz* into concrete factors.[161] Courts are capable of effectively assessing these factors, and many courts have already done so.[162] To be sure, judges will inevitably disagree over how to assess one or another of the factors, or about how to weigh the various factors against each other.[163] But the spectrum of potential disagreement over *Carpenter*'s factors is narrow compared to the almost limitless range of disagreement possible under *Katz*.[164] The amorphous paradigm of *Katz*, with its multiple, conflicting models of privacy, permits courts to reach virtually any conclusion on virtually any rationale they choose.

Carpenter provides a standard that cabins and shapes courts' reasoning. It requires at least an attempt at good faith argumentation, in a way that *Katz* does not. Judges faced with high volumes of revealing data not voluntarily disclosed to others will be hard pressed to withhold Fourth Amendment protection.[165] And judges considering small quantities of non-revealing information voluntarily disclosed to others will find it difficult to extend Fourth Amendment protection.[166] The *Carpenter* test, unlike *Katz*, is a real standard.

Moreover, *Carpenter*'s standard can be applied in any case involving a potential Fourth Amendment search.[167] It is useful for both third-party disclosure cases and direct government surveillance cases.[168] It is equally effective at addressing digital and non-digital data.[169] Lower courts may not always apply the *Carpenter* test with perfect accuracy—a statement that applies to any legal standard—but its factors appear to be workable for judges and lower court

---

[160] *See* Ohm, *supra* note 17, at 389.

[161] *See infra* Part III.B.

[162] *E.g.,* United States v. Trice, 966 F.3d 506, 519 (6th Cir. 2020) (holding that the brief use of a surveillance camera in an apartment hallway captured far less data, and less revealing data, than the prolonged cell phone tracking at issue in *Carpenter*); Standing Akimbo, LLC v. United States through Internal Revenue Serv., 955 F.3d 1146, 1164–65 (10th Cir. 2020) (holding in an IRS investigation case that a marijuana grower had no reasonable expectation of privacy in plant growth records that do not reveal any personal information and were voluntarily disclosed to a state regulator); United States v. Hood, 920 F.3d 87, 92 (1st Cir. 2019) (concluding that IP address information revealed far less than the data at issue in *Carpenter* and was automatically disclosed and accordingly finding no Fourth Amendment search); Commonwealth v. McCarthy, 142 N.E.3d 1090, 1104 (Mass. 2020) (concluding that license plate readers did not collect deeply revealing data in substantial amounts and did not effect a Fourth Amendment search); People v. Tafoya, 490 P.3d 532, 542 (Colo. Ct. App. 2019) (holding that the warrantless use of a telephone pole camera to observe the outside of a suspect's home for three months collected a substantial amount of revealing data and violated the Fourth Amendment).

[163] *See supra* note 85 and accompanying text; Ohm, *supra* note 17, at 389.

[164] Ohm, *supra* note 17, at 389; *see supra* Part I.A.

[165] *E.g.*, United States v. Diggs, 385 F. Supp. 3d 648 (N.D. Ill. 2019); State v. Eads, 154 N.E.3d 538, 541 (Ohio Ct. App. 2020).

[166] *E.g.*, United States v. Tolbert, 326 F. Supp. 3d 1211, 1225 (D.N.M. 2018); People v. Alexander, 2021 WL 912701 (Ill. App. Ct. 2021).

[167] *See supra* notes 129–134, 143.

[168] *See supra* notes 118, 129–134.

[169] *See supra* notes 117, 143.

complaints about *Carpenter* have been virtually nonexistent.[170]

Given *Carpenter*'s workability and universal reach, there is little reason to continue applying *Katz*'s vague reasonable expectation of privacy standard, except perhaps as a throat-clearing exercise at the beginning of a judicial opinion. To be clear, it matters little whether courts ignore *Katz* altogether or recite the *Katz* test before using *Carpenter* to determine whether an individual has a "reasonable expectation of privacy." The important thing is that *Carpenter* governs the analysis of whether a government action is a Fourth Amendment search, unencumbered by any *Katz*-related assessments of actual expectations, or public exposure, or positive law, or social norms, or any of the other conflicting conceptual models of the *Katz* test.[171]

It is telling that the *Carpenter* Court, addressing an especially difficult and significant Fourth Amendment question, did not actually apply the *Katz* test. It merely recited the test, noted that "no single rubric definitively resolves which expectations of privacy are entitled to protection," and quickly moved on to other topics.[172] *Katz* has little to offer even the most capable decisionmakers as a framework for concrete Fourth Amendment analysis.

This is not to say that the Supreme Court's myriad *Katz* precedents are valueless or need to be discarded when the *Carpenter* test is adopted. Indeed, another argument in favor of *Carpenter* is that its factors were not invented from whole cloth. Rather, they arose from decades of Supreme Court precedents grappling with difficult Fourth Amendment questions.[173] In this body of law, several principles gradually emerged that helped the Court identify when a government action required constitutional scrutiny.[174] Those same principles make up the *Carpenter* test. In this sense, *Carpenter* was more of an evolution than a sharp break from prior law. Its principles are firmly grounded in precedent and well-suited to assess the Fourth Amendment questions of the future.

B. *Carpenter* as Evolution

Carpenter was a case of potentially massive importance, establishing a new test that may come to dominate Fourth Amendment search law. But the decision, and the emerging

---

[170] Tokson, *supra* note 22 (manuscript at 36 & nn. 241–42).

[171] For a discussion of these models, *see supra* text accompanying notes 43–48.

[172] Carpenter v. United States, 138 S. Ct. 2206, 2213–14 (2018).

[173] *See, e.g.*, Dow Chem. Co. v. United States, 476 U.S. 227, 234–39 (1986); Florida v. Riley, 488 U.S. 445, 449–52 (1989); Oliver v. United States, 466 U.S. 170, 177–84 (1984); United States v. Place, 462 U.S. 696, 700–10 (1983); United States v. Knotts, 460 U.S. 276, 280–85 (1983); United States v. Miller, 425 U.S. 435, 442–47 (1976); Tokson, *supra* note 49, at 59 app. tbl.1.

[174] *See infra* Part III.B.

Carpenter test, is more continuous with past Fourth Amendment decisions than observers have recognized.[175] The factors that make up the *Carpenter* test can be traced to prior Supreme Court decisions spread out over several decades.

1. Revealing Nature

The *Carpenter* opinion emphasized that cell phone location data was deeply revealing of the details of a person's life.[176] It "provides an intimate window" into a person's life, potentially revealing their "familial, political, professional, religious, and sexual associations."[177] The Court's concern, in other words, was that intimate or sensitive information about an individual's life would be revealed to agents of the state.[178] Such data may be used for illegitimate purposes, give state agents undue power over a citizen, cause substantial privacy harms to data subjects, or simply compromise the security promised by the Fourth Amendment.[179]

The Supreme Court has looked to the revealing, intimate nature of government surveillance in numerous cases over the past several decades. For instance, the Court held that aerial surveillance of a commercial property was not a search because "the photographs here are not so revealing of intimate details as to raise constitutional concerns."[180] Observing the backyard of a home by helicopter was likewise not a search because "no intimate details connected with the use of the home or curtilage" were revealed.[181] And the Court justified its decision not to extend Fourth Amendment protections to open fields under *Katz* by stating that "open fields do not provide the setting for those intimate activities that the Amendment is intended to shelter from government interference or surveillance."[182] The revealing or

---

[175] *Cf.* Ohm, *supra* note 17, at 358 ("*Carpenter* works a series of revolutions in Fourth Amendment law, which are likely to guide the evolution of constitutional privacy in this country for a generation or more."); Kerr, *supra* note 135 (manuscript at 6) ("*Carpenter* signals a major break from the traditional understanding . . . [and] signals a new kind of expectation of privacy test . . . .").

[176] Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

[177] *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

[178] Kerr, *supra* note 135 (manuscript at 22); Ohm, *supra* note 17, at 403.

[179] *See* Rubenfeld, *supra* note 10, at 152 ("[The] data mining program [cast a] suspicionless, totally generalized net . . . —under which the government claimed in principle the power to know with whom each of us is communicating at every moment of our lives."); Kerr, *supra* note 135 (manuscript at 22) ("[T]he powers of the digital age [may allow police] to have unlimited access to embarrassing personal information about us—information such as personal associations, religious beliefs or sexual preferences . . . .").

[180] Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986).

[181] Florida v. Riley, 488 U.S. 445, 452 (1989).

[182] Oliver v. United States, 466 U.S. 170, 179 (1984).

intimate nature of surveillance is not always a definitive consideration.[183] But it has played a role in many Supreme Court Fourth Amendment cases—a role that has now been formalized in *Carpenter*.

2. Amount

The amount of data collected probably received more discussion in *Carpenter* than any other factor.[184] The Court described at length how cell phones track users constantly, everywhere they go, for long durations.[185] Large amounts of data such as those at issue in *Carpenter* increase the potential for invasions of the target's privacy.[186] Theoretically, the more personal data the government collects about an individual, the more they can exercise power over them, or learn about every aspect of their lives.[187]

The Supreme Court has often discussed the amount of data gathered by government officials in the decades prior to *Carpenter*. In ruling that the use of the drug-sniffing dog was not a search, the Court emphasized the limited quantity of information gathered by the dog.[188] The Court noted in an early location tracking case that, while short-duration location tracking was not a search, longer-duration searches were more constitutionally questionable.[189]

---

[183] *E.g.*, United States v. White, 401 U.S. 745, 752–54 (1971) (plurality opinion) (holding that the use of undercover informants with the suspect's unwitting consent was not a search despite the intimate and revealing nature of conversation); Arizona v. Hicks, 480 U.S. 321, 321 (1987) (holding that the Fourth Amendment protected non-revealing information, namely the serial numbers on the underside of stereo components).

[184] The Court detailed how the government could access cell phone company databases that typically go back five years, meaning that anyone of interest to the government "has effectively been tailed every moment of every day for five years." Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018). Cell phone tracking is "detailed [and] encyclopedic," *id.* at 2216, and provides "an all-encompassing record of the holder's whereabouts." *Id.* at 2217. The Court noted that "[T]his case is not about 'using a phone' or a person's movement at a particular time. It is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Id.* at 2220.

[185] *Id.* at 2218.

[186] *Id.* at 2220; Tokson, *supra* note 49, at 18. Stephen E. Henderson, *Fourth Amendment Time Machines (And What They Might Say About Police Body Cameras),* 18 U. PA. J. CONST. L. 933, 960–61 (2016); ABA Standards for Criminal Justice, Third Edition, Law Enforcement Access to Third Party Records, Commentary to Standard 25-4.1(b).

[187] Tokson, *supra* note 49, at 20; Renan, *supra* note 4, at 1056; David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 90 (2013). Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1112, 1154 (2002). Rubenfeld, *supra* note 10, at 151–52.

[188] United States v. Place, 462 U.S. 696, 707 (1983) (noting that "the information obtained [by a dog sniff] is limited").

[189] United States v. Knotts, 460 U.S. 276, 284 (1983) (deferring judgment on long-duration location monitoring, which remained hypothetical at the time of the instant case).

Moreover, in *United States v. Jones*, Justice Alito's concurrence recognized that long-term surveillance that "secretly monitor[ed] and catalogue[d] every single movement of an individual's car for a very long period" violated privacy in a way that briefer, lower-quantity methods of surveillance did not.[190] The concurrence was joined by three other Justices and endorsed by a fourth.[191]

The Court has also noted the importance of amount in privacy cases outside of Fourth Amendment law. In a 1977 case addressing the legality of a state database of prescription drug users, the Court noted "the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[192] In a later case, the Court held that FBI rap sheets compiling publicly available criminal conviction data could not be disclosed under FOIA, because the collection and storage of such a large quantity of information in one place raised substantial privacy concerns.[193] Like the revealing nature of data, amount is sometimes outweighed by other considerations.[194] But it appears surprisingly often in cases decided long before *Carpenter*.

3. Voluntary Disclosure to Others

The *Carpenter* Court discussed voluntary disclosure in its opinion as well, although perhaps not to the same extent as the other two factors.[195] The Court noted that cell phone data is not voluntarily shared with a cell phone company in any meaningful sense. Rather, a cell phone automatically transmits this data whenever it is powered on.[196] And declining to own a cellphone is hardly an option in modern America.[197] In theory, information that is not

---

[190] United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring). Accordingly, a search had occurred in a case involving twenty-eight days of tracking a car GPS. *Id.* at 403. Five Justices endorsed Justice Alito's concurrence, although Sotomayor did not officially join it. *See id. at* 413 (Sotomayor, J., concurring).

[191] *Id.* at 430 (Alito, J., concurring); *id*. at 413 (Sotomayor, J., concurring).

[192] Whalen v. Roe, 429 U.S. 589, 605 (1977). *See also id.* at 607 (Brennan, J., concurring) ("The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.").

[193] U.S. Dep't of Just. v. Reps. Comm. for Freedom of the Press, 489 U.S. 749, 764, 770 (1989).

[194] *E.g.*, Ferguson v. City of Charleston, 532 U.S. 67, 84–86 (2001) (holding that the collection of a small amount of medical data was a search); United States v. Karo, 468 U.S. 705, 720 (1984) (finding that collecting a substantial amount of non-specific location data was not a search).

[195] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

[196] *Id.*

[197] *Id*; *see also id.* at 2211 (noting that there were "396 million cell phone service accounts in the United States—for a Nation of 326 million people").

voluntarily disclosed to another is more private than information voluntarily disclosed to some other party or parties.[198]

This factor reflects the enduring influence of the Court's third-party doctrine precedents despite *Carpenter*'s new limitations on the doctrine. The Court's earliest third-party cases turned on suspects' voluntary (albeit uninformed) choice to share details of their crimes with undercover agents.[199] The Court held that the Fourth Amendment does not apply to an individual who "voluntarily confides his wrongdoing" to another.[200] Likewise, it does not apply to financial records "voluntarily conveyed to the banks,"[201] or to phone numbers "voluntarily conveyed…to the telephone company."[202] Similar concepts have been used in cases outside of the classic third-party disclosure context. The Court held, for instance, that an individual has no Fourth Amendment right in the trash they leave on the sidewalk for collection, which they expose to the public and convey to the trash collector.[203]

Many of these decisions have been justly criticized as leaning too heavily on third-party disclosure as a justification for withholding constitutional protection.[204] But the use of voluntary disclosure as a factor in the *Carpenter* test is more benign than its use in the classic third-party doctrine. Under the *Carpenter* test, voluntary disclosure is just one factor of three to be weighed in the calculus; it is not the definitive consideration it was prior to *Carpenter*. Courts applying *Carpenter* will still protect voluntarily disclosed data in many situations.[205] In addition, *Carpenter* makes clear that only truly voluntary disclosures will weigh against suspects, rather than the largely inescapable disclosures at issue in several of the Court's third-party doctrine cases.[206] Much of the criticism of these cases focuses on the Court's erroneous

---

[198] *See* Orin Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 588 (2009). A related theoretical point is that information widely disseminated to others is less private than information kept secret or disclosed only to a limited set of parties. Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 974 (2005). Thus far, despite its advantages, the social networks approach to assessing third-party disclosure has been largely confined to civil privacy cases. *See id.* at 973–75 (discussing the strengths of the social networks approach).

[199] United States v. White, 401 U.S. 745, 746–47 (1971) (plurality opinion); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427, 428–29 (1963).

[200] *White*, 401 U.S. at 749 (quoting *Hoffa*, 385 U.S. at 302).

[201] United States v. Miller, 425 U.S. 435, 442 (1976).

[202] Smith v. Maryland, 442 U.S. 735, 744 (1979).

[203] California v. Greenwood, 486 U.S. 35, 40–41 (1988).

[204] Ohm, *supra* note 56, at 1330–31; Bellovin et al., *supra* note 12, at 22–31; Leary, *supra* note 12, at 379.

[205] As an early example, see *In re* Google Location Hist. Litig., 514 F. Supp. 3d 1147, 1154–57 (2021) (finding a reasonable expectation of privacy under *Carpenter* for voluntarily disclosed data).

[206] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018). *See Smith*, 442 U.S. at 743–44; *Miller*, 425 U.S. at 442–43.

assumptions that the use of banks or telephones was somehow a voluntary choice.[207] *Carpenter*, while declining to correct these old errors, indicates that only truly voluntary disclosures will count going forward, while functionally unavoidable actions like owning a cell phone will not be held against suspects.[208]

In any event, the checkered past of the voluntary disclosure factor suggests that it should be considered the least important of the three *Carpenter* factors.[209] This factor has also been discussed far less often than the other two in lower court cases applying *Carpenter*.[210] And the Supreme Court itself has not always withheld protection from voluntarily disclosed data, even in the decades when the third-party doctrine supposedly mandated that outcome. The Court regularly protected third-party data long before *Carpenter* formally adopted that practice. It held, for instance, that a state hospital program of drug testing pregnant patients' urine for law enforcement purposes violated the Fourth Amendment, despite the fact that patients voluntarily turned over their urine to hospital employees.[211] In another case, the Court held that the police must obtain a warrant to enter a hotel room, despite the fact that the room was routinely exposed to "maids, janitors, or repairmen."[212] And in *Jones*, the exposure of Jones's car to the observation of the public was insufficient to eliminate Fourth Amendment protection in the car's GPS data.[213] The Court has experience in deemphasizing or ignoring voluntary disclosure when other considerations point the opposite way. It will continue to do so, especially now that voluntary disclosure has become only one consideration among several.

---

[207] Colb, *supra* note 11, at 155–59, 157 n.137; Rubenfeld, *supra* note 10, at 132–33; Leary, *supra* note 12, at 361.

[208] *Carpenter*, 138 S. Ct. at 2220.

[209] Tokson, *supra* note 60, at 425–26 (criticizing the concept of inescapability in Fourth Amendment law); Matthew Tokson, *Smart Meters as a Catalyst for Privacy Law*, 73 FLA. L. REV. (forthcoming 2022) (manuscript at 6–10) (critiquing the concept of voluntary disclosure in the context of smart utility meters).

[210] Tokson, *supra* note 22 (manuscript at 27–28). That study counted both cases that mentioned automatic disclosure and cases that mentioned inescapability. But cases that mentioned inescapability also tended to mention automatic disclosure, so in total there were only 66 cases that mentioned either of the two voluntariness concepts, compared to 93 mentions of the revealing nature of data and 116 mentions of the amount of data. *See id.*

[211] Ferguson v. City of Charleston, 532 U.S. 67, 84–85 (2001). The Court granted certiorari only on the issue of whether the testing was reasonable under the special needs doctrine and assumed a lack of patient consent. *Id.* at 76. However, the dissenting Justices noted that the patients' consent was obvious and provided a clear basis to resolve the case. *Id.* at 92–96 (Scalia, J., dissenting).

[212] Stoner v. California, 376 U.S. 483, 489–90 (1964).

[213] United States v. Jones, 565 U.S. 400, 410 (2012); *id.*. at 430 (Alito, J., concurring); *id.* at 413 (Sotomayor, J., concurring).

C. The *Carpenter* Test, with *Katz* Cases

Carpenter represents a significant evolution in Fourth Amendment law, not a sharp break with the past. Because of its advantages, it should come to govern new Fourth Amendment search questions.[214] Yet the more-than-forty Supreme Court cases applying the *Katz* test can still be used as valid precedents to guide courts, because several of the principles that drove them are the same principles embodied in the *Carpenter* test. Some of these cases may warrant reexamination or even reversal, to be sure.[215] But the guidance their holdings provide should not be lightly dismissed,[216] and they can often inform the new *Carpenter* paradigm in useful ways.

Indeed, the continuity of *Carpenter* with what came before will likely bolster the arguments of those judges, litigants, and scholars who wish to adopt it and phase out the *Katz* test. The Fourth Amendment is in a period of flux, and we cannot assume that courts will inevitably choose the optimal Fourth Amendment test. Those who wish to make Fourth Amendment law more coherent must advocate in favor of a more intelligible approach. But it is difficult to believe that the Supreme Court intended to radically revise Fourth Amendment law or to incorporate novel theoretical concepts into a revolutionary new test. It is far more likely that the Court, confronted with a difficult question posed by advanced technology, finally formalized some important considerations that it had been attentive to for decades.

CONCLUSION

As this Essay has detailed, Fourth Amendment law is in a transitional phase. The *Katz* and *Carpenter* tests coexist uneasily in the lower courts, as judges attempt to apply their overlapping and sometimes conflicting frameworks. There appear to be no effective metaprinciples to dictate which test should apply to a given set of facts.

Ultimately, as the above analysis shows, the *Carpenter* test is more coherent, specific, and predictable than the *Katz* test. It avoids *Katz*'s potential circularity problem and does not rely on randomly applied, conflicting conceptual models.[217] It is based on sound theoretical claims

---

[214] Specifically, it should govern at least those Fourth Amendment questions that do not involve clear physical trespasses. *See* Florida v. Jardines, 569 U.S. 1, 8 (2013) (applying a quasi-trespass test to determine that police entry onto a suspect's home's curtilage was a Fourth Amendment search).

[215] *See* Tokson, *supra* note 2, at 806–08.

[216] Allen & Rosenberg, *supra* note 6, at 1151–52, 1199–1201.

[217] *See supra* text accompanying note 40.

and grounded in decades of Supreme Court precedent.[218] Courts should adopt it and, at last, abandon the *Katz* paradigm that has caused so much confusion over the past several decades.

None of this is to say that the *Carpenter* test is flawless or always easy to apply. But it is a concrete test that produces clear answers. It can enable individuals to better understand when they will be protected against government surveillance. And it can provide courts with meaningful guidance, instead of the conceptual muddle of current law.

[218] *See supra* Part III.B.