2020

A Third-Party Doctrine for Digital Metadata

H. Brian Holland

A THIRD-PARTY DOCTRINE FOR DIGITAL METADATA

H. Brian Holland†

TABLE OF CONTENTS

† Professor of Law, Texas A&M University School of Law. Sincere thanks to the participants in the Internet Law Works-in-Progress conference as well as my colleagues at Texas A&M for the many helpful comments. And, as always, to Sarah, Will, and Ella, for the most important things.

INTRODUCTION

The law of search and seizure is built on flexible standards of reasonableness, transformed by courts into bright-line rules that balance the needs of law enforcement against the degree to which a particular police practice intrudes upon individual privacy interests. The third-party doctrine is one such rule, holding that police do not need a Fourth Amendment warrant to access information that an individual has voluntarily disclosed or conveyed to a third party, such as bank records or call histories. But the third-party doctrine is quite literally the product of another era—before ubiquitous networked computing, digital data, electronic communications, mobile technologies, and the commodification of information. Today, the digital devices that facilitate our daily participation in modern society are connected through automated infrastructures that are designed to generate vast quantities of data, nearly all of which are captured, utilized, and stored by third-party service providers. Under a plain reading of the third-party doctrine, however, the substantial majority of that data receives no Fourth Amendment protection—no matter how sensitive or revealing the information.

It is generally agreed that the balance struck in the third-party doctrine is no longer reasonable, as it fails to account for the far greater degree of privacy intrusion occasioned by warrantless government access to all of this personal data. Acknowledging that current approaches fail to adequately account for rapid advancements in information technology and analytics, the Supreme Court has responded in several recent cases by creating specific, narrow exceptions to the third-party doctrine for certain devices and data. But in the absence of a more generalized and coherent approach, lower courts have struggled to understand and apply these cases to other technologies and types of data, leading to uneven and often contradictory results.

This Article proposes a new analytical framework for adapting the third-party doctrine to the new-information environment. Drawing on the Court's recent decisions, this Article advances a three-step approach for the development of workable, bright-line rules governing the search and seizure of different categories of data. It identifies both guiding principles and

competing interests, as well as the specific factors to be considered in assessing the legitimacy and relative strength of those interests. It then explains the relationship between those factors and their role in the balancing process that produces appropriate and workable rules. The goal is to provide a consistent, practical framework to be applied more generally across the different categories of data generated by digital technologies and services.

This Article proceeds in three Parts. Part I identifies the public/private distinction as the dominant principle and primary limit on the scope of Fourth Amendment protections. I argue that the enduring and influential facet of *Katz v. United States*[1] is not Justice Harlan's "reasonable expectation of privacy" test[2] but rather the majority's distinction between that which "a person knowingly exposes to the public . . . [and] what he seeks to preserve as private."[3] I explore the origins of this public/private distinction in the "public exposure" and "third-party disclosure" cases, its use in subordination of property interests, and its consequential extension to the third-party doctrine. This discussion helps to establish the significance of the Court's recent decisions in *United States v. Jones* (2012),[4] *Riley v. California* (2014),[5] and *Carpenter v. United States* (2018).[6]

Part II argues that *Jones*, *Riley*, and *Carpenter* subvert the dominant role of the public/private distinction, with significant implications for the third-party doctrine. Third-party disclosure is transformed from a bright-line rule into a single element of a broader balancing test, in which an individual's privacy interest in a particular category of information is weighed against the diminishing effect of disclosure or conveyance. In some cases, those privacy interests will be weighty enough to overcome the third-party disclosure and the Fourth Amendment's protections will therefore apply.

In Part III, I propose an analytical framework to be applied by lower courts in developing workable, bright-line rules governing the search and seizure of the different categories of data. First, I identify four key factors to be applied in the analysis: pervasive devices and information services;

---

1 389 U.S. 347 (1967).

2 *Id.* at 360 (Harlan, J., concurring).

3 *Id.* at 351–52 (1967) (majority opinion) (citations omitted).

4 565 U.S. 400 (2012).

5 573 U.S. 373 (2014).

6 138 S. Ct. 2206 (2018).

automated data generation and collection; the nature of the metadata generated and collected; and the linking of that metadata to the "privacies of life."[7] Second, I propose a three-step analysis that begins by determining the strength and legitimacy of an individual's privacy interest in the information sought by the government. Here, the court examines both the possibility and probability that the category of data sought by the government will reveal sensitive information. Possibility simply refers to a direct and reliable link between the data and the sensitive information, i.e., the ability to derive information from the data. Probability is assessed on a sliding scale that considers both the precision/detail and amount/density of the data. In addition, individuals are likely to have a stronger privacy interest in large sets of historical, retrospective data. Next, the court determines the extent to which disclosure or conveyance of personal information to a third party diminishes that privacy interest. In making this determination, the court considers both the extent to which the device or service generating the data is a necessity to participation in a modern society and the user's practical ability to control the conveyance of data to a third party during the use of that device or service. Finally, the court balances the individual privacy interest against the diminishing effect of third-party disclosure, using fundamental Fourth Amendment principles to guide its evaluation. In the final Section of Part III, the proposed framework is tested by application to other automated technologies and metadata sets, using real-time cell phone location tracking and Internet Protocol (IP) addresses as examples.

I. THE PUBLIC/PRIVATE DISTINCTION: FROM *KATZ* TO THE THIRD-PARTY DOCTRINE

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause."[8] Reading the Amendment's substantive and procedural clauses as connected, the Supreme Court held that searches and seizures undertaken without first securing a warrant are presumptively

---

7 *Id.* (quoting *Riley*, 573 U.S. at 403).

8 U.S. CONST. amend. IV.

unreasonable.[9] This presumption may be overcome, however, in two common circumstances: first, on the front end, by demonstrating that no search or seizure occurred and thus no warrant was required;[10] or second, on the back end, by showing that a warrantless search or seizure was nevertheless reasonable because it "falls within a specific exception to the warrant requirement."[11]

In the first of these circumstances, the key question is how one determines whether a "search" has occurred within the meaning of the Fourth Amendment. For much of the twentieth century, the "liberty and privacy rights" secured by the Fourth Amendment "were understood largely in terms of property rights,"[12] but evolving societal practices and advancements in technology led the Court to adopt a more flexible standard intended to expand the concept of a Fourth Amendment search. In describing this shift, the conventional narrative focuses on two paradigmatic cases, *Olmstead v. United States*[13] and *Katz v. United States*.[14] In this simplified telling, the *Katz* decision is characterized as a fault line in Fourth Amendment jurisprudence—introducing an entirely new standard that replaces *Olmstead*'s rigid, property-based safeguards with more flexible, expansive, privacy-based protections.[15] These are mere caricatures, however, obscuring the emergence of a more demanding standard that, rather than

---

9 *See* Wayne D. Holly, *The Fourth Amendment Hangs in the Balance: Resurrecting the Warrant Requirement Through Strict Scrutiny*, 13 N.Y.L. SCH. J. HUM. RTS. 531, 541–43 (1997) (discussing the relationship between Fourth Amendment warrants and reasonableness, and the Supreme Court's asserted preference for the traditional warrant requirement); *see also Carpenter*, 138 S. Ct. at 2221 ("[W]arrantless searches are typically unreasonable . . . [unless they] fall[] within a specific exception to the warrant requirement." (citation omitted)).

10 *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 31 (2001) ("[T]he antecedent question whether or not a Fourth Amendment 'search' has occurred is not so simple under our precedent.").

11 *Riley*, 573 U.S. at 382 (citation omitted).

12 *Carpenter*, 138 S. Ct. at 2239 (quoting Morgan Cloud, *Property Is Privacy: Locke and Brandeis in the Twenty-First Century*, 55 AM. CRIM. L. REV. 37, 42 (2018)).

13 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

14 389 U.S. 347.

15 *See generally* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.1(b) (5th ed. 2019) (observing that "it is no overstatement to say, as the commentators have asserted, that *Katz* 'marks a watershed in fourth amendment jurisprudence' because the Court 'purported to clean house on outmoded fourth amendment principles' and moved 'toward a redefinition of the scope of the Fourth Amendment'" (internal citation omitted)).

expanding the concept of a Fourth Amendment search, sharply limits privacy protections for those engaged in modern information society.

A. Katz v. United States*: The Conventional Telling*

Throughout the first half of the twentieth century, the Supreme Court limited application of the warrant requirement to a narrow class of government actions constituting a "search" within the meaning of the Fourth Amendment. A search was said to occur only where enforcement officers "obtain[] information by physically intruding on a constitutionally protected area."[16] These protected areas were limited to property in which the targeted individual held an ownership or possessory interest, while physical intrusion required that officers commit common-law trespass upon property.[17] *Olmstead* provides the canonical example. In that case, the defendants spoke with one another using landline telephones located within the privacy of their respective homes[18]—an area at the "very core" of the Fourth Amendment.[19] Law enforcement officials intercepted these conversations by placing taps on telephone lines located immediately outside the homes on nearby streets.[20] The Court held that no Fourth Amendment search had occurred because placement of the taps did not require the officers to physically enter the defendants' homes—i.e., "without trespass upon any property of the defendants."[21] Moreover, the oral conversations transcribed by federal officers were not the type of tangible

---

16 United States v. Jones, 565 U.S. 400, 406 n.3 (2012); *see also Carpenter*, 138 S. Ct. at 2213.

17 *See Jones*, 565 U.S. at 405 (discussing the Fourth Amendment's "close connection to property"); *id.* ("[O]ur Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century." (citing Kyllo v. United States, 533 U.S. 27, 31 (2001))); *see also* Nita A. Farahany, *Searching Secrets*, 160 U. PA. L. REV. 1239, 1244–46 (2012) (observing that Fourth Amendment doctrine is grounded in property concepts); *Carpenter*, 138 S. Ct. at 2213–14 (referencing the historic connection between Fourth Amendment protections and trespass upon property).

18 *Olmstead*, 277 U.S. at 456.

19 Florida v. Jardines, 569 U.S. 1, 6 (2013) (citation omitted); *see also* Oliver v. United States, 466 U.S. 170, 178 (1984) (stating that "the Court since the enactment of the Fourth Amendment has stressed 'the overriding respect for the sanctity of the home that has been embedded in our traditions since the origins of the Republic.'" (quoting Payton v. New York, 445 U.S. 573, 601 (1980))).

20 *Olmstead*, 277 U.S. at 456–57.

21 *Id.* at 457, 466.

objects that are protected from search or seizure.[22] In the absence of a search, no warrant was required.[23]

Justice Brandeis, writing in dissent, recognized that such a rigid approach would create opportunities for evasion. He cautioned that technological advancement would bring "[s]ubtler and more far-reaching means of invading privacy" without physical intrusion and in the absence of trespass, the government would be able "to expose . . . the most intimate occurrences of the home" without implicating constitutional safeguards.[24]

In *Katz*,[25] the Court sought to rectify the shortcomings of the *Olmstead* approach by extending the concept of private spaces beyond formal property lines, to other areas and situations in which an individual enjoys a legitimate expectation of privacy.[26] The material facts of the case were fairly similar to those presented in *Olmstead*. Law enforcement agents had "attached an electronic listening and recording device to the outside of . . . [an enclosed] public telephone booth" commonly used by Katz to conduct a gambling operation.[27] Applying the *Olmstead* analysis, the court of appeals held that no search had occurred within the meaning of the Fourth Amendment because Katz's conversations had been obtained without law enforcement physically entering the area occupied by the defendant.[28] But the Supreme Court abruptly reversed course—rejecting *Olmstead*'s rigid, property-based approach in favor of a more flexible analysis of individual privacy interests.

It is commonly understood that the persistent standard to emerge from *Katz* came not from the majority opinion but from Justice Harlan's concurrence.[29] Building off the majority's holding that property interests no

---

22 *Id.* at 466.

23 *Id.*

24 *Id.* at 473–74 (Brandeis, J. dissenting).

25 389 U.S. 347 (1967).

26 United States v. Jones, 565 U.S. 400, 405–06 (2012) (describing the shift in Katz v. United States, 389 U.S. 347 (1967), from the "exclusively property-based approach" to the "reasonable expectation of privacy" approach).

27 *Katz*, 389 U.S. at 348.

28 *Id.* at 348–49.

29 *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2213–14 (2018) (discussing the reasonable expectation of privacy standard in *Katz*).

longer control the analysis,[30] Harlan concluded that a search instead occurs when government officials violate an individual's "reasonable expectation of privacy."[31] The latter interest requires "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 [objectively] 'reasonable.'"[32] Applying that standard, the Court found that "an enclosed telephone booth is an area where, like a home . . . a person has a constitutionally protected reasonable expectation of privacy."[33] Moreover, the Court held that a cognizable intrusion upon that privacy interest may occur "by electronic as well as physical invasion."[34] It was therefore immaterial that the electronic surveillance device used in this case did not penetrate the walls of the telephone booth.[35] Finally, the Court affirmed that Fourth Amendment protections are not limited to the seizure of tangible items but also apply to intangible interests, such as private oral conversations.[36]

When *Katz* was first decided, "commentators believed this formulation would expand the scope of the Fourth Amendment."[37] But the reality of post-*Katz* jurisprudence proved significantly more complex than this conventional narrative suggests. With the end of the Warren Court in the late 1960s, the Court's expansive understanding of *Katz* began almost immediately to erode on multiple fronts. Although the Court had apparently forsaken rigid, property-based rules in favor of more flexible standards, it had not abandoned its strong preference for workable, bright-line rules.[38]

30

> In his concurring opinion in *Katz*, Justice Harlan indicated that he "join[ed] the opinion of the Court," but then explained what he took that opinion to mean. Because lower courts attempting to interpret and apply *Katz* quickly came to rely upon the Harlan elaboration, as ultimately did a majority of the Supreme Court . . . .

LAFAVE, *supra* note 15.

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

32 *Id.* at 361.

33 *Id.* at 360.

34 *Id.* at 362.

35 *Id.* at 353 (majority opinion).

36 *Id.*

37 Christopher Slobogin, *Distinguished Lecture: Surveillance and the Constitution*, 55 WAYNE L. REV. 1105, 1111 (2009); *see* Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 330 (1998).

38 *See generally* 2 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 4.1(b) (5th ed. 2019); *see also* Orin S. Kerr, *The Fourth Amendment and New*

Amid this tension, the Court found it difficult to commit to the case-by-case, contextual approach suggested by *Katz*. The Court was unable to shake its conception of privacy as "a discrete commodity, possessed absolutely or not at all."[39]

It is now commonly argued that *Katz* effectively reframed the Fourth Amendment analysis but without significantly altering its substance. The Court, favoring clear guidelines, has continued to privilege property ownership and possessory interests in its analysis of privacy expectations.[40] And indeed, the Court has acknowledged as much, holding that "one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of this right to exclude."[41] But this observation, although generally correct as a matter of outcome, obscures a

Technologies: Constitutional Myths and the Case for Caution, 102 MICH. L. REV. 801, 861–62 (2004) (positing "rule clarity" as a goal of Fourth Amendment jurisprudence); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 581–82 (2009) ("The on/off switch of the suppression remedy demands clear Fourth Amendment rules on what police conduct triggers Fourth Amendment protection and what police conduct does not."); Wayne R. LaFave, *The Fourth Amendment in an Imperfect World: On Drawing "Bright Lines" and "Good Faith,"* 43 U. PITT. L. REV. 307, 325–27 (1982) (setting forth various factors to consider when determining whether to adopt bright-line rules in the Fourth Amendment context); Melanie D. Wilson, *The Return of Reasonableness: Saving the Fourth Amendment from the Supreme Court*, 59 CASE W. RES. L. REV. 1, 38–39 (2008) (arguing in favor of "clear rules" in Fourth Amendment jurisprudence).

39 Smith v. Maryland, 442 U.S. 735, 748–49 (1979) (Marshall, J., dissenting).

40 *See, e.g.*, Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978) ("Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society. One of the main rights attaching to property is the right to exclude others, and one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of this right to exclude. Expectations of privacy protected by the Fourth Amendment, of course, need not be based on a common-law interest in real or personal property, or on the invasion of such an interest. These ideas were rejected both in *Jones* and *Katz*. But by focusing on legitimate expectations of privacy in Fourth Amendment jurisprudence, the Court has not altogether abandoned use of property concepts in determining the presence or absence of the privacy interests protected by that Amendment." (citations omitted)); *see also* Oliver v. United States, 466 U.S. 170, 183–84 (1984). In *Carpenter*, the majority opinion and each of the four dissenting opinions reaffirmed the connection between Fourth Amendment protections and trespass-upon-property. *See Carpenter*, 138 S. Ct. at 2213–14; *id.* at 2227 (Kennedy, J., dissenting) ("*Katz* did not abandon reliance on property-based concepts."); *id*. at 2235–36 (Thomas, J., dissenting) (rejecting *Katz*, 389 U.S. 347, in favor of a property-based approach); *id.* at 2260 (Alito, J., dissenting) (characterizing United States v. Miller, 425 U.S. 435 (1976), and *Smith*, 442 U.S. 735, as turning on the defendants' lack of property rights in the property of another); *id.* at 2267–71 (Gorsuch, J., dissenting) (suggesting that a return to property concepts might resolve difficulties arising in regard to the third-party doctrine).

41 *Rakas*, 439 U.S. at 143 n.12.

more broadly significant and enduring facet of the *Katz* analysis: the central role of the public/private distinction in limiting the scope of Fourth Amendment protections.

B. *Revisiting* Katz*: The Public/Private Distinction*

The *Katz* analysis is best understood as an amalgam of the majority opinion and Justice Harlan's concurrence, read as an integrated whole. Four related points are particularly salient. First, a Fourth Amendment "search" occurs when the government (a) impermissibly intrudes (b) upon a legitimate privacy interest (c) in order to obtain information.[42] Second, legitimate privacy interests are not to be rigidly defined by property ownership or possessory interests, but rather by employing Harlan's two-pronged "reasonable expectation of privacy" standard.[43] Third, in applying this standard, both the majority opinion and Harlan's concurrence make an essential distinction between public exposure and the preservation of privacy. The majority holds that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[44] Harlan makes a similar distinction, differentiating between "a man's home . . . a place where he expects privacy" and "objects, activities, or statements that he exposes to the 'plain view' of outsiders."[45] Likewise, conversations that take place in "an enclosed telephone booth" away from "the uninvited ear" are protected, while "conversations in the open" are not.[46] Finally, as these examples suggest, the public/private distinction is often defined by reference to concealment within private areas or places.[47] This focus on concealment ensured that property interests, although not controlling, remain a significant consideration.

---

42 *See, e.g.*, United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring) (citing Silverman v. United States, 365 U.S. 505, 509–12 (1961)).

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

44 *Id.* at 351–52 (majority opinion) (citations omitted).

45 *Id.* at 361 (Harlan, J., concurring).

46 *Id.* at 352, 360–61 (majority opinion and then Harlan, J., concurring).

47 *Id.* at 361 (Harlan, J., concurring).

Viewed in isolation, *Katz* appeared at first to dramatically expand the concept of a Fourth Amendment search by decoupling individual privacy interests from the rigid limits of real and personal property. In place of this property approach, the Court adopted a contextual analysis of both an individual's subjective expectations and society's willingness to recognize those expectations as reasonable. This more flexible approach had the effect, in at least some cases, of extending protection beyond those areas enumerated in the Fourth Amendment and into the public sphere; here, a public telephone booth.[48]

But this new flexible, contextual approach proved difficult to apply. The "unjust"[49] certainty of *Olmstead* had merely been replaced with the impractical uncertainty of *Katz*. It is this uncertainty—so at odds with the Court's preference for workable, bright-line rules—that precipitated the emergence of the binary public/private distinction as a dominant limit on the scope of Fourth Amendment protections.

The public/private distinction is rooted in two distinct strands of pre-*Katz* case law. The first involves the exposure of evidence to the prying eyes and ears of the public, and by extension to law enforcement personnel (public exposure). The other addresses the disclosure of information to a particular third-party, such as an undercover officer or informant (third-party disclosure).

1. The Public Exposure Cases

The first strand of cases involves the exposure of acts, objects, or information to the public, even where an individual seeks to seclude himself within the bounds of property or through practical obscurity. In the first of the public exposure cases cited in *Katz*, *United States v. Lee*,[50] a Coast Guard patrol boat followed suspected bootlegger, Lee, to a rendezvous point twenty-four miles from land.[51] Using a searchlight to illuminate the deck of the bootlegger's boat, crew members spotted cases of illegal grain alcohol.[52]

---

48 *Id.* at 353 (majority opinion).

49 LAFAVE, *supra* note 15.

50 274 U.S. 559 (1927).

51 *Id.* at 560.

52 *Id.* at 560–61.

This led them to board the vessel and ultimately to Lee's arrest.[53] Despite the bootleggers' attempts to seclude their activities by retreating to the middle of the ocean, the Court held that no search had taken place within the meaning of the Fourth Amendment, because the contraband had been left exposed to observers.[54] In reaching its conclusion, the *Lee* court relied on *Hester v. United States*,[55] in which revenue officers crossed onto private land owned by the defendant's family for the purpose of conducting surveillance.[56] From their position in defendant's "open fields," the officers observed the defendant and an accomplice handling contraband in plain view.[57] The Court held, first, that the trespass itself did not constitute a search, because "the special protection accorded by the Fourth Amendment to . . . 'persons, houses, papers and effects,' is not extended to the open fields."[58] And second, as in *Lee*, the "defendant's own acts" exposed incriminating evidence to onlookers.[59]

The next case cited in *Katz*, *Rios v. United States*,[60] distinguishes these public exposure cases from those in which the individual seeks to conceal his conversations and property.[61] The underlying facts, although disputed, generally involved "[a] passenger who [let] a package drop to the floor of the taxicab in which he [was] riding."[62] Differentiating between concealment in a private vehicle on the one hand and exposure or abandonment on the other, the Court held that "[a]n occupied taxicab is not to be compared to an open field . . . or a vacated hotel room."[63] Finally, in *Ex parte Jackson*,[64] the Court drew a clear line between sealed letters and packages "intended to be kept free from inspection . . . except as to their outward form" and other types of printed matter "purposely left in a condition to be examined," such

---

53 *Id.* at 560.

54 *Id.* at 563 (holding that the use of a spotlight to inspect the boat was no different than "the use of a marine glass or a field glass").

55 *Id.* (citing Hester v. United States, 265 U.S. 57 (1924)).

56 *Hester*, 265 U.S. at 58–59.

57 *Id.*

58 *Id.*

59 *Id.* at 58.

60 364 U.S. 253 (1960).

61 *Id.* at 261–62, 262 n.6.

62 *Id.* at 261–62.

63 *Id.* at 262 n.6 (citations omitted).

64 *Ex parte* Jackson, 96 U.S. 727 (1877).

as newspapers and magazines.[65] In making this distinction, the Court analogized sealed letters and packages to the objects located within the senders' "own domiciles"[66]—safeguarding that which is concealed from both the public and government officials.

These cases illuminate a key aspect of the public/private distinction, drawing a line between seclusion and concealment. On the one hand, these cases affirm that "the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion" stands at "the very core" of the Fourth Amendment[67]—such that acts, objects, or information concealed within the home's interior remain protected. The same is true of certain other private areas, such as the taxicab in *Rios*,[68] provided that the relevant evidence remains concealed within that space and out of view of the public.[69] On the other hand, all that occurs outside of these concealed areas is deemed to have been "knowingly expos[ed] to the public" and "is not a subject of Fourth Amendment protection,"[70] even if, as in *Hester*, the home is secluded from the public by the operation of property law and a corresponding right to exclude.[71] An officer's trespass across open fields does not immunize that which is knowingly exposed and thus observed.[72] Moreover, even the most drastic efforts to physically isolate oneself or obscure illegal activity are generally insufficient to overcome the public exposure rule. What is visible—at night, by spotlight, on the open sea, miles from shore[73]—is said to be in plain view, exposed to the public. The apparent seclusion provided by private property rights in land or miles of open ocean bears little constitutional significance. Although concealment indoors or below decks may have been sufficient.

---

65 *Id.* at 733.

66 *Id.*

67 Silverman v. United States, 365 U.S. 505, 511 (1961).

68 *Rios*, 364 U.S. at 261–62.

69 *Id.* at 262.

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

71 Hester v. United States, 265 U.S. 57, 58-59 (1924).

72 *Id.*

73 United States v. Lee, 274 U.S. 559, 560–61 (1927).

2. The Third-Party Disclosure Cases

The second strand of cases supporting *Katz*'s public/private distinction are those in which an individual discloses information to a third party—e.g., to an undercover officer or informant. The *Katz* decision cites[74] specifically to *Lewis v. United States*,[75] in which an undercover narcotics agent was twice invited into the suspect's home to consummate a drug transaction.[76] The Court acknowledged that "the home is accorded the full range of Fourth Amendment protections,"[77] and that the agent gained entry to the home only by misrepresenting his identity.[78] Nevertheless, the Court found that no search had occurred within the meaning of the Fourth Amendment.[79] Key to this conclusion was that on "neither of his visits to petitioner's home did the agent see, hear, or take anything that was not contemplated, and in fact intended, by petitioner as a necessary part of his illegal business."[80] In other words, the suspect had voluntarily disclosed incriminating information and physical evidence to a government agent.

The *Lewis* Court compared[81] this result to its contrary conclusion in *Gouled v. United States*,[82] in which an informant secured by subterfuge an invitation to the suspect's office.[83] Once inside he "secretly ransacked the office and seized certain private papers of an incriminating nature."[84] The fundamental difference between *Lewis* and *Gouled* was the voluntariness of the suspect's disclosures. In *Lewis*, the suspect had chosen not only to admit the third party to his home, but to provide him with information and contraband. In *Gouled*, only the first of these conditions had been met. The suspect had freely admitted the informant to his office but had not willingly disclosed anything. It was the involuntary nature of the disclosure that established the Fourth Amendment violation.

---

74 *Katz*, 389 U.S. at 351.

75 385 U.S. 206 (1966).

76 *Id.* at 207–08.

77 *Id.* at 211.

78 *Id.* at 206–07.

79 *Id.* at 210–11.

80 *Id.* at 210.

81 *Id.* at 209–10.

82 255 U.S. 298 (1921), *abrogated by* Warden, Md. Penitentiary v. Hayden, 387 U.S. 294 (1967).

83 *Id.* at 304.

84 *Lewis*, 385 U.S. at 210 (describing the facts of *Gouled*, 255 U.S. 298).

The import of these third-party disclosure cases is best understood by revisiting the two basic rules that emerged from the public exposure cases. First, what is concealed from observation by its location within certain private areas (e.g., homes, taxicabs) is protected by the Fourth Amendment against search and seizure.[85] Second, although enforcement officers may trespass on certain forms of private property (e.g., open fields) to better observe acts, objects, or information in plain view, they may not physically intrude upon the private area itself in order to gain access to that which is concealed. Thus, these cases make clear that seclusion within the bounds of property[86] or through practical obscurity[87] is generally insufficient to protect oneself from government intrusion—a legitimate privacy interest instead requires physical concealment within a limited number of protected private areas.

The third-party disclosure cases maintain the distinction between seclusion and concealment, but effectively impose even more stringent requirements for legally effective concealment. Thus, an undercover officer or informant who is invited to enter an otherwise protected private area has not impermissibly intruded within the meaning of the Fourth Amendment—even where the invitation is obtained by misrepresentation.[88] Likewise, once the officer is permissibly located within that private area, the observation of acts, conversations, and objects in plain view does not constitute a search.[89] Moreover, the memorialization or recording of oral conversations occurring within the private area is not in itself a seizure of that communication.[90] In sum, the protections of the Fourth Amendment do not apply to the voluntary disclosure of incriminating information or physical evidence to any third party who is permissibly located (even if by deception) within an otherwise protected private area. Instead, the public/private distinction appears to demand absolute concealment within a protected private space, in near isolation and silence.

---

85 Rios v. United States, 364 U.S. 253, 261–62 (1960).

86 Hester v. United States, 265 U.S. 57, 58–59 (1924).

87 United States v. Lee, 274 U.S. 559, 560–63 (1927).

88 *Lewis*, 385 U.S. at 206–07.

89 United States v. Dunn, 480 U.S. 294, 304 (1987).

90 United States v. White, 401 U.S. 745, 751 (1971).

C. *After* Katz*: The Continued Subordination of Property*

This brings us back to the prevailing account of post-*Katz* Fourth Amendment jurisprudence. Although *Katz* reframes the analysis around an individual's reasonable expectation of privacy, critics argue that this standard remains stubbornly linked to an individual's interest in property. But this critique tends to overstate the correlation. Private property interests and the right to exclude are simply one mechanism by which an individual may "seek[] to preserve [that which is] private."[91] And it is the private/public distinction, rather than the bounds of property, that remains the central principle for determining the existence, scope, and degree of Fourth Amendment privacy interests. Indeed, a persistent thread running through the cases relied upon in *Katz* is the failure of personal property interests to secure privacy protections. A Fourth Amendment privacy interest might be created by physical concealment within one of a few select spaces, but retreat into seclusion—whether by the legal right to exclude, physical barriers to entry, or practical obscurity—fails to provide the same protection.

This point is exemplified by the Court's aerial surveillance decisions. In *California v. Ciraolo*,[92] for example, Ciraolo was suspected of maintaining a marijuana garden within the protected curtilage of his home.[93] The garden itself was surrounded by a ten-foot fence.[94] Ciraolo's entire yard was enclosed by a second, six-foot fence.[95] Unable to see the garden from ground level, police "secured a private plane and flew over [Ciraolo's] house at an altitude of 1,000 feet."[96] Officers visually identified the marijuana growing in Ciraolo's yard and photographed the area using "a standard 35mm camera."[97] In concluding that no search had occurred, the Court held that what an officer is able to observe "from a public vantage point where he has a right to be" has been "knowingly exposed to the public . . . . [It is] not a subject of Fourth Amendment protection"[98]—even where the suspect

---

91 Katz v. United States, 389 U.S. 347, 351 (1967).

92 476 U.S. 207 (1986).

93 *Id.* at 209.

94 *Id.*

95 *Id.*

96 *Id.*

97 *Id.*

98 *Id.* at 213 (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

conducts his activities within a constitutionally protected area and employs exceptional measures to shield those activities from public view. In practice, therefore, a legitimate expectation of privacy often requires absolute concealment within the interior of an enclosed, constitutionally protected area, effectively obscured from external observation.

The public/private distinction has also been applied to justify physical trespass upon private property interests. The "open-fields doctrine"[99] provides an example of this corrosive process. The Court has long held that a person's house stands at "the very core of the Fourth Amendment."[100] Likewise, certain lands immediately adjacent to the dwelling itself (referred to as curtilage) are considered to be part of the home for Fourth Amendment purposes.[101] Physical intrusion upon the house or its curtilage will thus likely constitute a search, triggering the presumptive need for a warrant.[102] But any privately-owned land beyond the narrow bounds of the curtilage is classified as open fields, left unprotected by the Fourth Amendment.[103] As such, physical trespass upon open fields is not considered to be a search,[104] and all observable acts, objects, and information located there are said to have been exposed to the public in plain view.

This open fields concept has been broadly applied to "any unoccupied or undeveloped area outside of the curtilage"[105]—including, for example, "wooded areas, desert, vacant lots in urban areas, open beaches, reservoirs, and open waters."[106] Individuals have no legitimate expectation of privacy within these areas, even when privately held, and may not create a legitimate expectation by secluding the land with fences, locked gates, and "no

---

99 *Open-Fields Doctrine*, BLACK'S LAW DICTIONARY (10th ed. 2014) (defining the open-fields doctrine as "[t]he rule permitting a warrantless search of the area outside a property owner's curtilage; the principle that no one has a reasonable expectation of privacy in anything in plain sight").

100 Payton v. New York, 445 U.S. 573, 589–90 (1980) (brackets omitted). "[T]he Court since the Enactment of the Fourth Amendment has stressed 'the overriding respect for the sanctity of the home that has been embedded in our traditions since the origins of the Republic.'" Oliver v. United States 466 U.S. 170, 178 (1984) (quoting *Payton*, 445 U.S. at 601).

101 *Oliver*, 466 U.S. at 180.

102 *Id.*

103 *Id.* at 176 (holding that the "special protection accorded by the Fourth Amendment to the people in their 'persons, houses, papers, and effects,' is not extended to the open fields." (quoting Hester v. United States, 265 U.S. 57, 59 (1924))).

104 *Id.* at 183.

105 *Id.* at 180 n.11.

106 LAFAVE, *supra* note 15, § 2.4(a).

trespassing" signs.[107] *United States v. Dunn*[108] provides a somewhat extreme example. Dunn owned a 198-acre ranch surrounded by a perimeter fence.[109]

> The property also contained several interior fences, constructed mainly of posts and multiple strands of barbed wire. The ranch residence was situated ½ mile from a public road. A fence encircled the residence and a nearby small greenhouse. Two barns were located approximately 50 yards from this fence. The front of the larger of the two barns was enclosed by a wooden fence and had an open overhang. Locked, waist-high gates barred entry into the barn proper, and netting material stretched from the ceiling to the top of the wooden gates.[110]

Officers entered Dunn's private property without a warrant, walking hundreds of yards to reach the out-buildings.[111] They crossed over the perimeter fence, two interior wooden fences, and two barbed wire fences.[112] Finally, standing at the locked gate of the larger barn, officers used a flashlight to illuminate the interior of the barn and observed what they believed to be a drug lab.[113]

Accepting for the sake of argument that the barn enjoyed Fourth Amendment protection, the Court nevertheless found that no search had taken place.[114] The Court determined that the area immediately in front of the barn gate was an "open field" outside the curtilage of the house.[115] It then held that "there is no constitutional difference between police observations conducted while in a public place and while standing in the open fields."[116]

The *Dunn* case illustrates two key points regarding post-*Katz* jurisprudence. First, although *Katz* eliminated the physical trespass requirement as a means of securing privacy against non-intrusive surveillance technologies, the practical effect has been to authorize government intrusion onto vast swaths of private property. Even the most

---

107 *Oliver*, 466 U.S. at 182.

108 480 U.S. 294 (1987).

109 *Id.* at 297.

110 *Id.*

111 *Id.* at 297–98.

112 *Id.*

113 *Id.*

114 *Id.* at 303–05.

115 *Id.* at 304.

116 *Id.*

extreme efforts to legally and physically seclude oneself within the bounds of real property often fail to create a legitimate expectation of privacy. Property interests are instead merely one factor to be considered in determining an individual's Fourth Amendment interests. Second, what an officer is able to observe while physically located in open fields or other unprotected areas of private property—i.e., outside the residential dwelling or its curtilage—is considered to be in plain view of the public (i.e., public exposure), including that which an officer is able to observe within the interior of dwellings using his natural senses. Thus, the officer's trespass to private property is equated to his presence on land that is open to the public or on to which he has been invited by the owner. Indeed, the Supreme Court recently affirmed that officers may even enter those areas of curtilage that are generally considered open to the public under prevailing social norms, provided that they do so for legitimate reasons,[117] and that observations made from that position using their natural senses may be treated as being in plain view.[118]

D. *A Third-Party Doctrine of Exposure and Disclosure*

As just described, *Katz* derives the public/private distinction from two distinct strands of pre-*Katz* jurisprudence: the public exposure cases and the third-party disclosure cases.[119] In public exposure cases, the Court emphasizes the material difference between effective concealment and efforts to seclude.[120] Seclusion relies primarily on private property interests and the legal right to exclude to establish a legitimate expectation of privacy, creating a buffer zone between individual and observer within which the individual is purportedly free to operate in the open.[121] Under *Katz* and its progeny, however, it is nearly impossible to establish a legitimate privacy

---

117 Florida v. Jardines, 569 U.S. 1, 9 (2013) (indicating that "the background social norms that invite a visitor to the front door do not invite [a police officer] there to conduct a search"); *see also id.* at 8 (discussing "the habits of the country," implied invitations, and licenses).

118 *Id.* at 7–9 (distinguishing between the observations of an officer who merely enters the curtilage as "any private citizen might do" and the introduction of a trained police dog for the purpose of investigating with heighted senses).

119 *See supra* Sections I.B.1, I.B.2.

120 *See supra* Section I.B.1.

121 *See supra* Section I.B.2.

interest solely through legal or physical seclusion.[122] Government officials are permitted, for example, to trespass upon open fields to observe objects, activities, or conversations occurring on or within private property[123] and to photograph from the air those areas of private property that cannot be seen from the ground.[124] As a result, a legitimate privacy interest must generally be established through effective and absolute concealment within a diminishing number of constitutionally protected areas—e.g., within the interior of a dwelling house, obscured from external observation.

As the third-party disclosure cases demonstrate, however, even these core concealment protections are subject to exception. Undercover officers and informants are permitted, for instance, to gain entrance to an individual's home under false pretenses.[125] Once in the home, many of the objects, activities, and conversations concealed within its interior and thus effectively obscured from external observation are now in plain view or hearing of the government's agent.[126] The suspect's legitimate expectation of privacy within the home—a stronghold of retreat and seclusion from public life—is no longer justified because he invited a third party into a protected space, voluntarily disclosed incriminating information, and assumed the risk that the invitee might in turn reveal that information to the government.[127] In the absence of effective concealment and absolute silence, no warrant is required to gather that information.[128] Moreover, the government is not required to obtain a subpoena or other formal process to compel production from these cooperating witnesses. They are free to disclose what they know.

The third-party doctrine[129] applies these same principles to personal information disclosed to a private individual or institution for the purpose of facilitating the provision of goods or services, as opposed to information gathered by a government agent or informant in the course of an investigation. At the time *Katz* was decided, these transactional disclosures

---

122 *See supra* Section I.C.

123 United States v. Dunn, 480 U.S. 294, 303–05 (1987).

124 California v. Ciraolo, 476 U.S. 207, 209–13 (1986).

125 *See supra* Section I.B.2.

126 *See supra* Sections I.B.2, I.C.

127 *See supra* Section I.B.2.

128 *See supra* Section I.C.

129 The third-party doctrine refers to the "principle that one has no reasonable expectation of privacy in information that one has voluntarily disclosed to one or more third parties." *Third-Party Doctrine*, BLACK'S LAW DICTIONARY (10th ed. 2014).

generally represented a small universe of confidential relationships in which sensitive information (e.g., health, financial) would be entrusted to a third-party professional (e.g., doctor, banker) for a limited purpose and then retained as a business record. Outside the context of the underlying confidential relationship, however, this same information might prove valuable to law and regulatory enforcement. To what extent is this information protected by the Fourth Amendment's warrant requirement? The Supreme Court addressed this precise question in the first of two principal cases establishing the third-party doctrine.

In *United States v. Miller*,[130] a criminal defendant challenged the use of a subpoena to compel the production of checks, deposit slips, and other records held by his bank.[131] Relying on *Katz*, Miller characterized the information obtained from his bank as "copies of personal records that were made available to the banks for a limited purpose . . . in which he ha[d] a reasonable expectation of privacy."[132] As such, Miller argued, enforcement officials were required to secure a warrant before seizing the records, rather than a mere subpoena. But the Court, relying on the public exposure rule enunciated by the *Katz* majority[133]—that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection"[134]—found no legitimate expectation of privacy in "information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[135] Drawing on principles from the informant cases, the Court held that an individual "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government," even where the information is disclosed for a limited purpose.[136] It made no difference that the information was gathered and held by a private institution, rather than an undercover agent or informant.

It was a shocking result that seemingly defied prevailing privacy expectations regarding the provision of sensitive financial information to a trusted professional or institution. Congress responded by passing the Right

130 425 U.S. 435 (1976).

131 *Id.* at 436.

132 *Id.* at 442.

133 *Id.*

134 Katz v. United States, 389 U.S. 347, 351 (1967).

135 *Miller*, 425 U.S. at 442.

136 *Id.* at 443.

to Financial Privacy Act (RFPA), which provided protections similar to those that would be required if the Fourth Amendment applied.[137] Nevertheless, the constitutional relevance of the third-party doctrine as a manifestation of the public/private distinction remained undisturbed.

Almost immediately, the third-party doctrine faced a technological challenge to its animating principle. Earlier cases had reasoned that individuals who voluntarily disclose information to another human being do not maintain a reasonable expectation of privacy in that information, because the recipient may choose to reveal it to the government. But what happens when you remove the human from the system? In the telephone industry, for instance, human operators were being replaced by automated switching equipment.[138] The data captured by that system was therefore highly unlikely to ever be observed by a living person with the capacity to assess the information, and to choose whether to convey it to the government. With no human involved in the process, there would seem to be little appreciable risk of disclosure[139]—unless, of course, enforcement officers were to compel the owner of an automated system to gather the relevant information and provide it to authorities.[140] The Court considered these issues in the second of these principal third-party doctrine cases.

In *Smith v. Maryland*,[141] the defendant claimed a reasonable expectation of privacy in the numbers dialed from his home phone,[142] a record of which had been collected by a pen register installed on the telephone company's automated switching system.[143] In rejecting this assertion, the Court adopted an even more expansive statement of the third-party doctrine that omits any reference to exposure, disclosure, or actual observation, instead focusing on conveyance and possession, holding that "a person has no legitimate expectation of privacy in information he

---

137 12 U.S.C. § 3401 (2018); *see* Presley v. United States, 895 F.3d 1284, 1292 (11th Cir. 2018); Dean Galaro, *A Reconsideration of Financial Privacy and* United States v. Miller, 59 S. TEX. L. REV. 31, 42 (2017); W. Faith McElroy, *Closing the Financial Privacy Loophole: Defining "Access" in the Right to Financial Privacy Act*, 94 WASH. U. L. REV. 1057, 1058 (2017).

138 *See generally* Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 586 (2011).

139 *Id.* at 585.

140 *Id.* at 589–96 (discussing governmental processes for accessing third-party data).

141 442 U.S. 735 (1979).

142 *See id.* at 742.

143 *See id.* at 741, 744–45.

voluntarily turns over to third parties."[144] Applying that standard to the automated dialing system, the Court concluded:

> [P]etitioner can claim no legitimate expectation of privacy here. When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.[145]

The Court thereby extends the exposure rationale of the third-party doctrine to the exchange of intangible information with an automated third-party processing system.[146] Human observation is irrelevant.[147] It is generally enough that the information is conveyed, captured, and stored in the ordinary course of business, and is therefore available for possible examination[148]—even if only at the direction of authorities.

Although application of the third-party doctrine to an automated system may strain the limits of the assumption-of-risk rationale, it is entirely consistent with a rigid public/private distinction that demands effective concealment and absolute silence. First, the Court has rejected as insufficient efforts to seclude information by retreating within legal and physical barriers.[149] As such, the contractual guarantees and data-security measures offered by a third-party service provider do not create a legitimate privacy interest. Second, the Court has held that a legitimate privacy interest generally requires information to be physically concealed within one of a limited number of constitutionally protected areas, such as a dwelling house.[150] And it would be difficult to argue that information exchanged with an external automated processing system owned and operated by a third-party service provider remains effectively concealed within a protected area. Third, in the absence of effective concealment, the Court has treated information as though it were exposed in plain view of the public and

---

144 *Id.* at 743–44.

145 *Id.* at 744.

146 *See id.* at 744–45.

147 *See id.* at 745.

148 *See id.* at 744.

149 *See infra* Part II.

150 *See supra* Section I.B.1.

government officials—no matter how unlikely their presence.[151] Thus, a legitimate privacy interest is not preserved because droplets of individual information is obscured in an ocean of data or because the potential for human observation of the data processed by an automated system is almost nonexistent. It is enough that the data is potentially within reach. Fourth, even where information remains within a protected area and out of plain view, the Court has consistently held that voluntary disclosure to a trusted third party vitiates any legitimate privacy interest.[152] Hence, even if the Court were to recognize automated processing as a secure system in which data is effectively concealed, the conveyance of personal information to a third-party with the ability to access that data—even if such access is contractually disclaimed—is treated as a disclosure.

The third-party doctrine is thus constructed upon a legal and factual artifice. The user of an automated processing system is said to assume the risk that the operator of that system will ignore all practical realities and legal obligations by targeting, gathering, and choosing to share specific information with government officials. In reality, however, this information remains practically obscured in automated systems awash in data. Human observation generally occurs only in the process of compliance with a request, subpoena, or court order compelling production.

It is not terribly difficult to imagine how application of the public/private third-party doctrine to automated systems impacts privacy protections in an age of ubiquitous digital networks, third-party Internet service providers and intermediaries, and cloud-based computing services—all driven by the enormous amounts of data that is provided, created, used, processed, stored, and transferred "in the course of carrying out mundane tasks."[153] Many of the computing resources previously operated and maintained by the user are now outsourced to third-party providers,[154] with data distributed across a vast network of privately-owned computing systems. By disclosing personal information to these automated systems and services, you abandon any legitimate expectation of privacy and assume the risk that it will be shared with the government without a warrant. It makes no difference that your service provider does not access your information

---

151 *See supra* Section I.B.1.

152 *See supra* Section I.B.2.

153 United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

154 *See* Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 985, 986 (2016); *supra* note 138, at 585.

and promises not to do so. Likewise, privacy guarantees made in your terms of service cannot create a legitimate privacy interest or defeat a subpoena for compelled production.

As Judge Beverly Martin recently observed,

> blunt application of the third-party doctrine threatens to allow the government access to a staggering amount of information . . . . [B]y allowing a third-party company access to our e-mail accounts, the websites we visit, and our search-engine history—all for legitimate business purposes—we give up any privacy interest in that information . . . . I am convinced that most [I]nternet users would be shocked by this.[155]

Supreme Court Justice Neil Gorsuch has lately expressed similar concerns.

> The problem isn't with the [lower court's] application of *Smith* and *Miller* but with the cases themselves. Can the government demand a copy of all your e-mails from Google or Microsoft without implicating your Fourth Amendment rights? Can it secure your DNA from 23andMe without a warrant or probable cause? *Smith* and *Miller* say yes it can—at least without running afoul of *Katz*. But that result strikes most lawyers and judges today—me included—as pretty unlikely.[156]

There is a growing sense that a majority of the Court agrees. In a series of recent cases, the Court has begun to crack open the rigid application of the public/private distinction—including the third-party doctrine. I explore these developments in the next Part.

II. SUBVERTING THE PUBLIC/PRIVATE DISTINCTION

The Court has consistently affirmed that a Fourth Amendment search occurs when three basic elements are satisfied: (a) an impermissible government intrusion (b) upon a legitimate privacy interest (c) in order to obtain information.[157] Following *Katz*, however, application of that standard

---

155 United States v. Davis, 785 F.3d 498, 535–36 (11th Cir. 2015) (Martin, J., dissenting).

156 Carpenter v. United States, 138 S. Ct. 2206, 2262 (2018) (Gorsuch, J., dissenting).

157 *See, e.g.*, United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring) (citing Silverman v. United States, 365 U.S. 505, 509–12 (1961)).

essentially collapsed into a single inquiry operationalizing the public/private distinction—whether the information sought by the government remained physically concealed within one of a limited number of constitutionally protected areas, neither exposed to plain view nor disclosed to a third party. In this Part, I discuss three recent Supreme Court cases with the potential to fundamentally reshape this inquiry: *United States v. Jones* (2012),[158] *Riley v. California* (2014),[159] and *Carpenter v. United States* (2018).[160] Taken together, these decisions threaten to subvert the dominant role of the public/private distinction and the need for effective concealment as a means of preserving one's legitimate privacy interest in personal information, with significant implications for the third-party doctrine.

Jones signaled the Court's initial willingness to depart from this rigid approach, holding that the government violates the Fourth Amendment when it trespasses upon an enumerated area (i.e., "persons, houses, papers, and effects") for the purpose of gathering information—even if the information itself had been exposed to the public or disclosed to a third party.[161] In *Riley*, the Court recognized that the immense amounts of personal information generated by and accessible through modern technologies might require it to reconsider the balancing of interests captured in certain categorical, bright-line rules of search and seizure law.[162] In reaching this conclusion, the Court recognized that information may itself constitute a distinct object of Fourth Amendment protection in which the individual maintains a legitimate privacy interest, independent of the space or thing in which it is held.[163] Thus, the fact that some of the personal information accessible through Riley's cell phone was stored on a third-party cloud server did not eliminate the individual's privacy interest in that information.[164] In *Carpenter*, the Court drew on many of these same principles to fashion a limitation on the third-party doctrine—effectively transforming a categorical application of the public/private distinction into a sort of balancing test in which the act of disclosure is measured against the

158 565 U.S. 400 (2012).

159 573 U.S. 373 (2014).

160 *Carpenter*, 138 S. Ct. 2206.

161 *See infra* Section II.A.

162 *See infra* Section II.B.

163 *See infra* Section II.B.

164 *See infra* Section II.B.

nature of the data sought.[165] This transformation required two key changes in the doctrine. The Court held: first, that the disclosure or conveyance of personal information to a third party significantly diminishes, rather than eliminates, the individual's legitimate privacy interest;[166] and second, that certain information is so revealing and sensitive that the degree of intrusion arising from a governmental search will outweigh the diminishing effects of that disclosure or conveyance.[167] This progressive subversion of the public/private distinction is discussed in the Sections that follow.

A. United States v. Jones

In *Jones*, police attached a Global Positioning System (GPS) tracking device to the undercarriage of a suspect's car and used that device to continuously monitor the vehicle's physical location and movements over a twenty-eight day period.[168] Prior to trial, Jones sought to suppress the evidence obtained, arguing that the government's actions constituted a warrantless search within the meaning of the Fourth Amendment.[169] The government countered that, under *Katz* and its progeny, Jones had no reasonable expectation of privacy in either the outer surface of the vehicle or its movements along public streets, as these areas and information were exposed to the public.[170] Thus, no search had occurred when police obtained information that was otherwise in plain view of the public and no warrant was required.

Somewhat surprisingly, the Supreme Court not only rejected the government's argument but found *Katz* to be altogether inapplicable in resolving the question.[171] Justice Scalia began his analysis with a basic proposition: that the Court was constitutionally bound to "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[172] And "for most of our history the

---

165 *See infra* Section II.C.

166 *See infra* Section II.C.

167 *See infra* Section II.C.

168 United States v. Jones, 565 U.S. 400, 402–03 (2012).

169 *Id.* at 403.

170 *Id.* at 406.

171 *Id.* at 406–07.

172 *Id.* at 406 (citations omitted).

Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates."[173] *Katz* should not therefore be read as eliminating or replacing these traditional protections, but instead as providing additional and more expansive safeguards.[174]

In defining the essential substance of these privacy protections, the Court reaffirmed that "a search within the meaning of the Fourth Amendment occurs, at a minimum, where . . . the Government [1] obtains information [2] by physically intruding [3] on a constitutionally protected area."[175] Thus, a minimalist version of the "common-law trespassory test" had survived the transition from *Olmstead* to *Katz*, safeguarding those areas specifically enumerated in the Fourth Amendment from impermissible physical intrusion. Applying this standard to *Jones*, Scalia concluded that monitoring a vehicle's location (obtaining information) by attaching the GPS tracking device (physical intrusion/trespass) to the suspect's vehicle (a constitutionally protected "effect"), constitutes an invalid warrantless search.[176]

Having restored these traditional minimum safeguards as a distinct theory of Fourth Amendment protection, the *Jones* Court was then left to address the public nature of the locational information gathered by the GPS device. The Court had previously held that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another," because that information is "voluntarily conveyed to anyone who wanted to look."[177] This reasoning is consistent with the basic premise of the public/private distinction, as applied through *Katz*, which treats the failure to conceal information as if it were exposed in plain view. Relying on these earlier cases, the government implicitly argued in *Jones* that a search producing only public information cannot violate the Fourth Amendment. But Scalia rejected that premise.

---

173 *Id.* at 406–07 (citations omitted).

174 *Id.* at 407–08, 409.

175 *Id.* at 413 (Sotomayor, J., concurring) (quotation marks and citations omitted); *see also id.* at 407 (majority opinion).

176 *Id.* at 404.

177 Carpenter v. United States, 138 S. Ct. 2206, 2215 (2018) (quoting United States v. Knotts, 460 U.S. 276, 281–82 (1983)).

In these earlier cases, the suspects' location information had been gathered without trespassing upon an enumerated area.[178] The Court had therefore applied the *Katz* standard, as developed through the public exposure cases, finding the suspects' privacy claims to be limited by the failure to conceal their location from public view.[179] In *Jones*, on the other hand, the government did commit trespass, both in the process of attaching the GPS device and when changing its battery.[180] Under these circumstances, the violation accrues at the moment of physical intrusion upon an enumerated area for the purpose of gathering information. The public nature of the information eventually gathered—in the sense that the suspects' location was exposed in plain view of the public—is therefore irrelevant to the legitimacy of the privacy interest infringed by the prior act of trespass.

Justice Alito, although concurring in the judgment, nevertheless criticized Scalia for returning to the now-discredited *Olmstead* rule that "a technical trespass followed by the gathering of evidence constitutes a search."[181] But this seems a mischaracterization of the decision. Scalia did not suggest that any trespass upon any private property is a search within the meaning of the Fourth Amendment. Instead, he created a more narrow exception to the public/private distinction for physical trespass upon certain enumerated areas—"persons, houses, papers, and effects"[182] —allowing that in such cases individuals may retain a legitimate expectation of privacy in information that has been exposed to the public or disclosed to a third party.

The *Jones* decision opened a crack in the public/private distinction by resurrecting the trespass doctrine as "Step Zero"[183] in the Fourth Amendment analysis and applying that doctrine beyond the special solicitude of the home. This Step Zero focuses on how police obtained the

---

178 *Jones*, 565 U.S. at 408–09 (discussing the beeper cases, *Knotts*, 460 U.S. 276, and United States v. Karo, 468 U.S. 705 (1984)).

179 *Id.* at 408–09 (citing *Knotts*, 460 U.S. at 281–82).

180 *Id.* at 403–04.

181 *Id.* at 421 (Alito, J., concurring).

182 *Id.* at 405 (majority opinion) (holding that the Fourth Amendment cannot be read to interpret the phrase "in their persons, houses, papers, and effects" as "superfluous"); *id.* at 406 (noting that "for most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates"); *id.* at 404 (finding Jones's vehicle to be an "effect" within the meaning of the Fourth Amendment).

183 The "Step Zero" formulation describes the initial inquiry into whether the governing legal framework—here, *Katz*'s "reasonable expectation of privacy standard"—applies at all. *See, e.g.*, Cass R. Sunstein, Chevron *Step Zero*, 92 VA. L. REV. 187, 191 (2006) (discussing the most famous "Step Zero").

relevant information, i.e., whether it was obtained by trespass upon an enumerated area. If so, the trespass itself constitutes an intrusion upon the individual's legitimate privacy interests. At that point, the public/private distinction drops out of the picture. The unconstitutional intrusion is not excused simply because the individual has no independent privacy interest in the information collected, either because the information was in plain view of the public or disclosed to a third party.

B. Riley v. California

In *Riley*, the Court addressed protections for personal information available on an individual's cell phone, whether that information resides locally on the phone itself[184] or on remote servers accessible through the use of phone-based applications.[185] Officers conducting a routine search incident to arrest found a cell phone in Riley's pants pocket.[186] An officer on the scene "accessed information on the phone" that he believed indicated Riley's involvement with a gang.[187] Following Riley's transfer to the station house, a detective "further examined the contents of the phone . . . looking for evidence."[188] Certain pictures and videos found in the course of that search provided key investigative information, with several being described and/or submitted at trial.[189] Riley challenged the warrantless search of the content of his cell phone as unreasonable.[190] The government, relying on *United States v. Robinson*,[191] responded that no warrant was required because the search fell within a specific exception to the warrant requirement[192]—permitting officers to examine the content of objects found in the course of a search incident to a custodial arrest.[193]

---

184 Riley v. California, 573 U.S. 373, 393–97 (2014).

185 *Id.* at 397.

186 *Id.* at 378–79.

187 *Id.* at 379.

188 *Id.* (citation omitted).

189 *Id.* at 379–80.

190 *Id.* at 379.

191 414 U.S. 218 (1973).

192 *Riley*, 573 U.S. at 383–84.

193 *Id.* at 382–85 (describing the search-incident-to-arrest exception).

Acknowledging *Robinson* as a "categorical rule,"[194] the Supreme Court nevertheless rejected its application to a search of data stored on and accessible by a cell phone.[195] The Court first held that in determining whether an exception to the warrant requirement is reasonable, it must balance the legitimate governmental interests served by the warrantless search against the intrusion upon an individual's personal privacy.[196] Applying this standard, the Court made a clear distinction between the device (cell phone) and the data (content). The Court found that the risks justifying the *Robinson* rule—harm to officers and destruction of evidence—although manifest in physical objects, are de minimis "when the search is of digital data."[197] Moreover, the degree of intrusion effected by a search of cell phone data, measured by the quantity and nature of the personal information revealed, "bears little resemblance" to a search of other physical objects.[198] The Court therefore "decline[d] to extend *Robinson* to searches of data on cell phones . . . hold[ing] instead that officers must generally secure a warrant before conducting such a search."[199]

In reaching this conclusion, the Court was careful to recognize that the functional relationship between the physical device and the digital data—i.e., that the device collects, uses, stores, shares, and provides access to data—should not obscure the distinct and independent significance of personal information in a Fourth Amendment analysis. Individuals may have a legitimate and significant interest in that information qua information. Certainly, cell phones are different from other "containers" discovered in the course of a search incident to arrest. They are "minicomputers" with "immense storage capacity,"[200] running multiple software programs (applications) that handle constant flows of varied and detailed information.[201] But it is the information itself that creates significant Fourth Amendment concerns.

---

194 *Id.* at 386.

195 *Id.*

196 *Id.* at 385–86.

197 *Id.* at 386.

198 *Id.*

199 *Id.*

200 *Id.* at 393.

201 *Id.* at 394–97.

The Court first draws this distinction between device and data in the context of the personal information residing in local storage—i.e., in the phone's memory.[202] As the Court observes, collecting vast quantities of "even just one type of information . . . convey[s] far more than previously possible."[203] And access to "many distinct types of information . . . reveal[s] much more in combination than any isolated record."[204] Moreover, that data is often retrospective, stretching back over long periods of time.[205] And it is this "revealing montage of the user's life,"[206] not the physical characteristics of the object itself, that distinguishes the search of a cell phone from the search of "a cigarette pack, a wallet, or a purse."[207]

The analytical distinction between the device and the data is fully realized, however, in the context of cloud computing. Many cell phones and software applications seamlessly integrate cloud computing services, allowing users to access "data stored on remote servers rather than on the device itself."[208] "Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference. Moreover, the same type of data may be stored locally on the device for one user and in the cloud for another."[209] This creates a particular challenge for the search incident to arrest exception, which is limited to "papers and effects in the physical proximity of an arrestee."[210] Applying that limit in *Riley*, the Court distinguishes between the cell phone, as a physical object located within the physical proximity of an arrestee, and the data located in remote storage outside the physical proximity of an arrestee.[211] The physical aspects of the phone may be examined,[212] for

---

202 *Id.* at 393–97.

203 *Id.* at 394.

204 *Id.*

205 *Id.* at 394–96.

206 *Id.* at 396.

207 *Id.* at 393.

208 *Id.* at 397.

209 *Id.* (citation omitted).

210 *Id.* at 398.

211 *Id.*

212 *Id.* at 387; *see also* People v. Ward, 169 A.D.3d 833, 835 (N.Y. App. Div. 2019) (finding that "a physical search of the phone, in which the police opened the back of the phone and looked under the battery to obtain the phone's serial number . . . did not implicate any of the aspects found to distinguish a digital search from a search of any other physical object").

example, to ensure that it cannot be used as a weapon.[213] But the exception "may not be stretched to cover a search of files accessed remotely—that is, a search of files stored in the cloud."[214]

This discussion of cloud-based data is particularly relevant to *Riley*'s significance as a subversion of the public/private distinction. Having acknowledged the unique nature of the personal information available on a cell phone, the Court rejected rote application of an existing categorical rule that would have permitted police to search the contents of a cell phone seized incident to arrest. Instead, the Court chose to revisit the balancing of interests intended to be captured by that categorical rule. The public's interest in protecting officers and evidence was weighed against the intrusion visited upon the individual's legitimate privacy interests. Had the Court rigidly applied the third-party doctrine to the cloud-based data accessible through Riley's cell phone, any legitimate privacy interest in that data would have been eliminated from this analysis. Instead, the Court found it noteworthy that police would have access to this data—stored remotely, outside the physical proximity of an arrestee. Thus, one categorical rule was exchanged for another, requiring a warrant prior to searching the content of a cell phone seized incident to arrest.

C. Carpenter v. United States

In *Carpenter*, the Court examined protections for metadata created by the automated processes associated with the use of a cell phone; specifically, cell-site location data (CSLI).[215] Officers suspected that Carpenter was involved in a series of nine robberies occurring over a four-month period.[216] Seeking to establish that Carpenter was in the vicinity at the time of each robbery, prosecutors obtained a statutory court order issued pursuant to the Stored Communications Act (SCA),[217] compelling Carpenter's wireless

---

213 *Riley*, 573 U.S. at 387.

214 *Id.* at 397 (citation omitted).

215 Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018) (stating the question presented as "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements"); *see also id.* at 2211–12 (describing CSLI and how it is generated).

216 *Id.* at 2212.

217 18 U.S.C. § 2703 (2018).

carriers to turn over four months of CSLI for his cellular telephone.[218] "Altogether the Government obtained 12,898 location points cataloging Carpenter's movements—an average of 101 data points per day."[219] Carpenter sought to suppress these records at trial,[220] arguing that the information sought by law enforcement was protected by the Fourth Amendment and that the government was therefore required to obtain a judicial warrant rather than a court order issued pursuant to the SCA.[221] The district court denied the motion[222] and the Sixth Circuit Court of Appeals affirmed, holding that Carpenter had no legitimate expectation of privacy in his location information because he had voluntarily shared it with his wireless carriers.[223]

This conclusion reflects the rigidity of the public exposure and third-party disclosure cases. Applying the public-exposure doctrine, Carpenter's physical proximity to the robberies had been "voluntarily conveyed to anyone who wanted to look,"[224] and information that "a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[225] Having failed to effectively conceal himself within a protected area, all of Carpenter's location information would be treated as though it were continuously exposed in plain view, observed, tracked, and recorded. Likewise, even if one might claim a privacy interest in public location information more generally, that claim is extinguished by the voluntary act of disclosure or conveyance to a third party[226]—here, Carpenter's wireless provider.[227] As explained in *Miller* and *Smith*, the third-party doctrine does not "distinguish between *kinds* of information disclosed to third parties and require courts to decide whether to 'extend' [the third-party doctrine] to particular classes of information, depending on their sensitivity."[228] Thus, the intensely personal and revealing nature of CSLI would be largely irrelevant to the Fourth Amendment analysis.

---

218 *Carpenter*, 138 S. Ct. at 2211–12.

219 *Id.* at 2212.

220 *Id.*

221 *Id.*

222 *Id.*

223 *Id.* at 2213.

224 *Id.* at 2215 (quoting United States v. Knotts, 460 U.S. 276, 281–82 (1983)).

225 Katz v. United States, 389 U.S. 347, 351 (citations omitted).

226 *Carpenter*, 138 S. Ct. at 2216.

227 *Id.* at 2212, 2220.

228 *Id.* at 2262 (Gorsuch, J., dissenting).

On review, however, the Supreme Court rejected this binary conception of privacy, marking a significant shift in application of the public/private distinction. Adopting a more flexible analysis, the Court transformed this bright-line rule into a balancing test, measuring the act of exposure and/or disclosure against both the manner of surveillance and the nature of the information sought. After *Carpenter*, exposure and/or disclosure of personal information to a third party does not eliminate the individual's legitimate privacy interest in that information—as was the case under the categorical approach—but is instead treated as merely diminishing the individual's expectation of privacy. In some cases, the surveillance will be so permeating and the information so sensitive that the individual's privacy interest and resulting degree of intrusion will outweigh the diminishing effects of exposure and/or disclosure, triggering the Fourth Amendment's warrant requirement.

Applying this new balancing test, the Court focused its analysis on the "unique"[229] and "deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection."[230] Unlike the limited locational data that could be gathered using traditional law enforcement methods,[231] CSLI is an exhaustive and "detailed chronical of a person's physical presence compiled every day, every moment, over several years."[232] Thus, the privacy implications of each locational data point cannot be viewed in isolation, but as an aggregated whole that "provides 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'"[233]—what the Court describes as the "privacies of life."[234] Measuring this unremitting collection of sensitive data against the act of disclosure, the Court observes that the information "is not truly 'shared' as one normally understands the term" but is rather automatically produced merely through the use of a device (cellphone) "indispensable to participation in modern society."[235] The diminishing effect

---

229 *Id.* at 2217, 2220 (majority opinion).

230 *Id.* at 2223.

231 *Id.* at 2217.

232 *Id.* at 2220.

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

234 *Id.* (quoting Riley v. California, 573 U.S. 373, 403 (2014)).

235 *Id.* at 2220.

of disclosure is therefore insufficient to outweigh Carpenter's legitimate privacy interest.

III. A NEW ANALYTICAL FRAMEWORK

In this Part, I propose a framework for analyzing a user's Fourth Amendment interests in the metadata generated by automated devices and systems; specifically, where that metadata is accessed, collected, and stored by third-party providers. Taken together, *Jones*, *Riley*, and *Carpenter* transform the third-party doctrine from a broad, technology-neutral standard into a differentiated and potentially technology-dependent balancing test. *Carpenter* provides one specific example, holding that law enforcement must obtain a warrant prior to obtaining seven or more days of historical CSLI metadata.[236] What these cases fail to provide, however, is a clear and thorough accounting of how this new approach can and should be applied to other metadata-intensive technologies. My proposed framework fills this gap, working within the basic structure of the *Carpenter* balancing test but identifying a series of factors and subfactors to be considered in evaluating each element. The result is a consistent, comprehensive, and generalized approach to the creation of technology-specific standards that effectuate the Court's strong preference for workable, bright-line rules in implementing the warrant requirement.

My proposal proceeds in four parts. First, I establish the basic structure of the *Carpenter* balancing test, as an adaption of the Fourth Amendment "reasonableness" analysis. Second, I describe the fundamental concerns and constitutional principles guiding development of the proposed framework. Third, I set forth the entirety of the proposed framework, identifying and categorizing the various factors to be considered in constructing a workable approach to the development of categorical rules for metadata generated by automated systems. Fourth, I explore multiple examples of how this framework might be applied to other technologies and metadata sets.

---

[236] *Id.* at 2217.

A. *The* Carpenter *Balancing Test*

Carpenter recognizes that new automated technologies require the Court to reassess the balancing of interests captured by the third-party doctrine. Although the public/private distinction remains a factor in the "reasonableness" analysis, it is not always determinative. Application of the third-party doctrine must reflect and be limited by "the basic purpose" of the Fourth Amendment: "safeguard[ing] the privacy and security of individuals against arbitrary invasion by government officials."[237] In effectuating this fundamental purpose, the Court is "informed by historical understandings 'of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted,'"[238] including general warrants authorizing "an unrestrained search"[239] of nearly anyone, at any time, with little suspicion or none at all.[240] Thus, the Fourth Amendment "reasonableness" standard must be applied so as to "secure 'the privacies of life' against 'arbitrary power.'"[241]

Guided by these basic principles, *Carpenter* measures the act of disclosure against the nature of the information sought. This balancing approach involves a three-step analysis. Step one determines the strength and legitimacy of an individual's privacy interest in the information sought by the government. Step two considers the extent to which disclosure or conveyance of personal information to a third party diminishes an individual's legitimate privacy interest in that information. Step three balances the individual privacy interest against the diminishing effect of third-party disclosure. In some cases, the information will be so sensitive and so revealing that the degree of intrusion arising from a governmental search will outweigh the diminishing effects of disclosure. In such cases, a warrant is generally required.

---

237 *Id.* at 2213 (citation omitted).

238 *Id.* at 2214 (punctuation omitted) (quoting Carroll v. United States, 267 U.S. 132, 149 (1925)).

239 *Id.* at 2213.

240 Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1194 (2016).

241 *Carpenter*, 138 U.S. at 2214 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

B. *Guiding Principles*

In constructing the proposed framework, I am guided by an overarching concern about the government's ability to derive sensitive personal information from seemingly innocuous metadata, and its implications for basic Fourth Amendment principles. An individual's legitimate privacy interest should effectuate constitutional restraints upon "a too permeating police surveillance"[242]—surveillance that "spread[s] through" an individual's life and is "present in every part of it."[243] This concern reflects the reality of modern technologies. The devices themselves are pervasive and persistent. So is the mechanism for producing, collecting, and sharing data. This process is so "remarkably easy, cheap, and efficient"[244] that the need for time, money, and resources provides little constraint. Nearly all of this data is "detailed, encyclopedic, and effortlessly compiled,"[245] where it essentially remains in permanent storage. It is an unremitting process so embedded in the fabric of our daily lives that "[o]nly the few [can] escape this tireless and absolute surveillance."[246]

The vast stores of metadata produced by this unrelenting surveillance are often "deeply revealing" in their breadth and comprehensive reach,[247] providing "an intimate window into a person's life, revealing . . . 'familial, political, professional, religious, and sexual associations'"[248]— what Chief Justice Roberts describes as "the privacies of life."[249] Providing the government with access to all of this privately held data would risk "arbitrary invasions" reminiscent of the "reviled general warrants and writs of assistance of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal

---

242 *Id.* at 2214 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

243 *Permeate*, CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/us/dictionary/english/permeate [https://perma.cc/P2DM-DU82] (defining "permeate" as "to spread through something and be present in every part of it"); *see also Permeate*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/permeate [https://perma.cc/SDW6-S6A2] (defining "permeate" as "to diffuse through or penetrate something").

244 *Carpenter*, 138 S. Ct. at 2217–18.

245 *Id.* at 2216.

246 *Id.* at 2218.

247 *Id.* at 2223.

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

249 *Id.* (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

activity."[250] Understanding that a search of this metadata will often expose "private aspects of identity,"[251] the absence of adequate safeguards "chills associational and expressive freedoms."[252] The question is not precisely how much or how many types of data are provided, but what that data can tell you.

It was these basic concerns about persistent and indiscriminate surveillance, access to immense databases, and the arbitrary exercise of government power that led the *Riley* Court to exempt cellphones from the search-incident-to-arrest exception, citing the degree of intrusion resulting from an unrestrained search of the device. The Court was troubled not only by the amount and variety of data accessible through a cellphone but also the retrospective nature of the data, enabling the government to reconstruct a "revealing montage of the user's life."[253] Likewise, in *Jones* and *Carpenter*, the Court held that "individuals have a reasonable expectation of privacy in the whole of their physical movements,"[254] because society does not "reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[255] As in *Riley*, CSLI surveillance runs against everyone all the time, creating a comprehensive dossier from which sensitive information can be derived and which therefore "implicates basic Fourth Amendment concerns about arbitrary government power."[256]

---

250 *Id.* at 2213 (quotations and citations omitted); *see also* Riley v. California, 573 U.S. 373, 403 (2014) (quotations and citations omitted).

251 *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring); *see also Carpenter*, 138 S. Ct. at 2216 (analogizing the nature of the information derived from the GPS data at issue in *Jones* to the CSLI records at issue in *Carpenter*).

252 *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

253 *Riley*, 573 U.S. at 396; *id.* at 403 (finding that cell phones "hold for many Americans 'the privacies of life'").

254 *Carpenter*, 138 S. Ct. at 2217.

255 *Jones*, 565 U.S. at 416 (Sotomayor, J. concurring); *see also id.* at 415 (expressing concern that "a precise, comprehensive record of a person's public movements . . . reflects a wealth of detail about her familial, political, professional, religious, and sexual associations").

256 *Carpenter*, 138 S. Ct. at 2222; *see also Jones*, 565 U.S. at 416–17 (Sotomayor, J. concurring).

C. *Proposed Framework*

The proposed framework fills significant analytical gaps left open by *Jones*, *Riley*, and *Carpenter*—identifying a series of factors and subfactors to be considered in evaluating each element of the new balancing test. My goal is to provide lower courts with a consistent, comprehensive, and generalized approach to the creation of technology-specific standards that effectuate the Court's strong preference for workable, bright-line rules.

Step (1): Defining the Privacy Interest

In determining the legitimacy and strength of the privacy interest in particular metadata, two factors are considered: (a) the nature of the metadata generated and collected, and (b) the ability to derive personal information from aggregated metadata.

(a) *Factor: Nature of the Metadata Generated and Collected*. Courts should consider the following: (i) government access to comprehensive dossiers of historical metadata and (ii) undifferentiated collection and long-term storage of metadata.

i. *Subfactor: Comprehensive Dossiers of Historical Metadata*. Metadata-intensive technologies—such as Internet browsers, cellphones, and smart-home appliances—are now a pervasive part of modern society. These automated technologies are continually generating, collecting, and storing vast amounts of metadata. Unlike the information that could be gathered using traditional law enforcement methods, these exhaustive stores of metadata are "compiled every day, every moment, over several years."[257] A court should consider that the very existence of a comprehensive dossier of sensitive metadata constitutes the type of inescapable surveillance that creates a significant risk of arbitrary government invasion.

ii. *Subfactor: Undifferentiated Collection and Long-Term Storage of Metadata*. This pervasive surveillance runs against nearly everyone, all the time, so police need not know who they want to follow in advance. In the case of

---

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

CSLI metadata, for instance, the government "can now travel back in time [and] . . . whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years."[258] A court should therefore consider whether the metadata sought by the government is so broadly collected and stored that a retroactive search, even where individualized, exceeds society's expectations.

(b) *Factor: Ability to Derive Personal Information from Aggregated Metadata*. This factor is primarily concerned with the degree to which the metadata sought by the government is likely to reveal the privacies of life, generally defined by reference to eight categories of sensitive information.[259]

1. Finances—e.g., budgeting, commercial transactions.[260]
2. Legal matters—e.g., meeting with a criminal defense attorney.[261]
3. Physical and mental health—e.g., meeting with a psychiatrist, plastic surgeon, abortion clinic, or AIDS treatment center;[262] treatment for an alcohol, drug, or gambling addition;[263] tracking pregnancy symptoms;[264] web searches related to a certain disease or condition.[265]
4. Sexual orientation, associations, and activities[266]—e.g., trips to a strip club, by-the-hour motel, or gay bar;[267] dating applications.[268]
5. Familial associations[269]—e.g., trips to a private residence.[270]

---

258 *Id.* at 2218.

259 *See supra* Section II.C.

260 Riley v. California, 573 U.S. 373, 396 (2014).

261 People v. Weaver, 909 N.E.2d 1195, 1199–200 (N.Y. 2009) (cited with approval in United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J. concurring)).

262 *Id.*

263 *Riley*, 573 U.S. at 396.

264 *Id.*

265 *Id.* at 395–96.

266 *Jones*, 565 U.S. at 415, 416 (Sotomayor, J. concurring); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

267 *Weaver*, 909 N.E.2d at 1199–200.

268 *Riley*, 573 U.S. at 396.

269 *Carpenter*, 138 S. Ct. at 2217; *Jones*, 565 U.S. at 415.

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

6. Professional associations[271]—e.g., union meetings.[272]
7. Political beliefs, affiliations, and activities[273]—e.g., following political party news,[274] trips to political headquarters.[275]
8. Religious beliefs and affiliations[276]—e.g., trips to a mosque, synagogue, or church;[277] sharing prayer requests.[278]

Assessing the government's ability to derive this type of sensitive information from aggregated metadata requires a two-part inquiry, examining both the possibility and probability that the category of data sought by the government will reveal sensitive information.

i. *Subfactor: The Possibility of a Reliable Linkage*. Possibility requires simply that a court find it abstractly possible that there is some reliable linkage between the metadata generated and personal information that might be derived from its collection. Here, the Court has not indicated that attenuation is a concern, but only that a direct linkage is possible. CSLI records provide a good example. Generally speaking, the data provided to law enforcement consists of cell-site registration data, indicating the cell-site to which a particular phone was connected at a particular time. Law enforcement also has access to a list of cell-site locations, indicating where each cell site is located (longitude and latitude) and the geographical sector served by each of the various antennas located on that cell site. By mapping the cell-site registration data onto the list of cell-site locations, law enforcement is able to derive a fairly accurate approximation of where a user's cell phone was located at various times of the day, as well as their movements. It is this geographical location data "that enables the

---

271 *Id.* at 2217; *Jones*, 565 U.S. at 415.

272 *Weaver*, 909 N.E.2d at 1199–200 (cited with approval in *Jones*, 565 U.S. at 415).

273 *Carpenter*, 138 S. Ct. at 2217; *Jones*, 565 U.S. at 415–16.

274 *Riley*, 573 U.S. at 396 (discussing "apps for Democratic Party news and Republican Party news").

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

276 *Id.* at 2217; *Jones*, 565 U.S. at 415–16.

277 *Weaver*, 909 N.E.2d at 1199–200.

278 *Riley*, 273 U.S. at 396.

Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[279]

ii. *Subfactor: The Probability of a Reliable Linkage*. The probability analysis considers two aspects of the metadata sought to determine whether and under what circumstances a particular category of data is likely to reveal sensitive information: precision and/or detail and amount and/or density.

- *Precision and/or Detail*. First, a court should examine the level of data precision and detail; including, in some cases, whether the data is time-stamped.[280] For instance, in *Jones*, Justice Sotomayor found that GPS systems using multiple satellites had the ability to "establish[] the vehicle's location within 50 to 100 feet."[281] The Court reached a similar result in *Carpenter*, even though the accuracy of CSLI was less than that of GPS data.[282]
- *Amount and/or Density*. Second, a court should consider the amount and/or density of data within that category. This is perhaps the most difficult aspect of the analysis. It is clear, however, that the longer the period of time and the more data points collected (i.e., sustained density), the more likely it is that the data will reveal sensitive information. But it is equally apparent that the amount and/or density of data required may vary based on the precision and detail of that data. In *Carpenter*, for example, the Court found that obtaining 127 days of location tracking data with an average of 101 data points per day was sufficient to establish the government's ability to ascertain sensitive

---

279 *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

280 The Court also appears to require in all cases that the data be recorded and aggregated by the service provider. *Id.*

281 *Id.* at 403 (majority opinion).

282 Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

> information, even where the accuracy of CSLI was less than that of GPS data.[283] Justice Sotomayor posited, however, that "even short-term monitoring" that produces a "precise, comprehensive record" may be sufficiently likely to reveal sensitive information.[284] This conclusion is supported by *Carpenter*, which held that a warrant was required for each of two distinct CSLI record requests—one covering 152 days from MetroPCS, the other just seven days from Sprint (which ultimately produced only two days of records).[285]

Step (2): Diminishing Effects of Disclosure

The third-party doctrine holds that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[286] Framed through the lens of the public/private distinction, this analysis remained primarily focused on the individual's ability to proactively conceal information.[287] In the absence of active and effective concealment it was assumed that information had been voluntarily disclosed.[288] In the context of automated systems, the choice to utilize a particular service or device was itself a failure to conceal all associated data, which is therefore said to have been voluntarily disclosed to the provider.

In *Carpenter*, the Court concludes that this categorical rule cannot be mechanically extended to automated, data-intensive technologies. In some cases, disclosure diminishes an individual's privacy interest in information but does not eliminate it. Not all acts of "voluntary exposure" impose the same degree of diminution.[289] In determining the degree of diminution, the

---

283 *Id.* at 2212.

284 *Jones*, 565 U.S. at 415.

285 *Carpenter*, 138 S. Ct. at 2212–13.

286 Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

287 *See* discussion *supra* Section I.D.

288 *See* discussion *supra* Section I.D.

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

Court focuses on the voluntariness of that disclosure to determine whether the data was "truly 'shared' as one normally understands the term."[290]

Drawing from *Carpenter* and *Riley*, I identify two key factors in assessing the degree to which metadata is truly and voluntarily shared with the third-party provider: (a) the extent to which the device or service generating the metadata is a necessity to participation in a modern society, and (b) the user's practical ability to control the automated generation and conveyance of metadata to a third party during the use of that device or service.

(a) *Factor: Necessity of the Device or Service to Participation in a Modern Society*. The necessity analysis acknowledges that certain data-intensive devices and services are now essentially "indispensable to participation in modern society."[291] Here, a court should consider the role of the device or service in society—both personal and professional—as well as structural adaptions that increasingly require always-on connectivity. Studies indicate, for instance, that ninety percent of Americans use the Internet[292] and ninety-six percent own a cellphone (eighty-one percent of which are smartphones).[293] It is worth noting that these pervasive and persistent devices are more likely to be present in private places and situations, producing, collecting, and sharing immense amounts of data from which sensitive information is likely to be derived.[294] Cellphones, for instance, are "such a pervasive and insistent part of daily life"[295] that people "compulsively carry" them at all times"[296]—"beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing

---

290 *Id.*

291 *Id.*

292 *Internet/Broadband Fact Sheet*, PEW RES. CTR.: INTERNET & TECH. (Feb. 5, 2018), https://www.pewresearch.org/internet/fact-sheet/internet-broadband [https://perma.cc/QGS7-MKTR].

293 *Mobile Fact Sheet*, PEW RES. CTR.: INTERNET & TECH. (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/mobile [https://perma.cc/H6SM-7U33].

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

295 Riley v. California, 573 U.S. 373, 385 (2014).

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

locales."[297] Almost like a feature of human anatomy,[298] "nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower."[299]

(b) *Factor: Ability to Control Automated Metadata Generation and Collection*. In assessing the user's ability to control the conveyance of metadata to a third party during the use of that device or service, courts should consider three subfactors: first, whether the category of data sought by the government is automatically generated, "without any affirmative act on the part of the user beyond powering up;"[300] second, which and what percentage of activities carried out through the device or service generate the category of data sought;[301] and third, whether it is possible to lessen or eliminate the conveyance of the category of data sought without abandoning the device or service.[302]

Step (3): Balancing

In the final step of the analysis, the individual's privacy interest is balanced against the diminishing effect of third-party disclosure to determine whether she enjoys a reasonable expectation of privacy in the metadata sought by the government. If so, and assuming no exception applies, access to that data constitutes a Fourth Amendment search and a warrant is presumptively required. In making this assessment, a court should be guided by the basic purposes of the Fourth Amendment: protecting the privacies of life against arbitrary invasion and too permeating police surveillance.

In the absence of additional guidance, *Carpenter* provides a single point of comparison for future cases. *Carpenter* holds that individuals have a legitimate privacy interest in the whole of their physical movements, primarily because access to those records is likely to reveal sensitive information. CSLI metadata provides a precise and detailed accounting of

297 *Id.*

298 *Riley*, 573 U.S. at 385.

299 *Id.* at 395.

300 *Carpenter*, 138 S. Ct. 2206, 2220.

301 *Id.*

302 *Id.*

an individual's location and movements, establishing a reliable linkage to the privacies of life. Given the sustained density of CSLI metadata collection, there is a high probability that government access to even a short period of CSLI metadata will reveal sensitive information. Moreover, this comprehensive metadata is collected on nearly everyone and stored for long periods, creating the risk of arbitrary retroactive surveillance. An individual therefore has a legitimate and significant privacy interest in her CSLI metadata. *Carpenter* then determines that CSLI metadata is not truly shared and thus that third-party disclosure does little to diminish an individual's privacy interest. This reflects both the necessity of a cellphone to participation in modern society and the user's inability to adequately control the disclosure of CSLI metadata without giving up the cellphone itself. The practical inability to escape this constant and revealing surveillance creates a reasonable expectation of privacy and demands Fourth Amendment protection.

D. *Using the Proposed Framework to Derive Bright-Line Rules*

In this Section, I explore how this proposed framework could be applied to other automated technologies and metadata sets.

Real-Time CSLI. "Prospective, or real-time, CSLI permits police to determine the phone's current location as it registers with each tower."[303] Police may seek current records or ask the cellular provider to "ping" the cellphone to determine its current location—for instance, when searching for a fugitive.[304] As relevant to the proposed framework, a request for real-time CSLI differs from historical CSLI in three key ways. First, although cellular providers compile comprehensive dossiers of historical CSLI, a request for real-time CSLI does not involve a substantially retroactive search of that database. Second, in most cases these requests will produce far fewer data points over a very limited period of time.[305] Third, police will often request that the cellular provider actively initiate collection of CSLI by

---

303 Christian Bennardo, Note, *The Fourth Amendment, CSLI Tracking, and the Mosaic Theory*, 85 FORDHAM L. REV. 2385, 2392 (2017).

304 *See, e.g.*, Sims v. State, 569 S.W.3d 634, 636–37 (Tex. Crim. App. 2019).

305 *See, e.g.*, *id.* at 646 (addressing a Fourth Amendment challenge to police access of just three hours of real-time CSLI records, in which the suspect's cellular provider pinged his phone fewer than five times).

"pinging" the individual's cellphone—as opposed to tracking the cellphone's attempt to connect with the network.

As applied in step one of the proposed framework, these distinctions weaken the individual's privacy interest in particular metadata. Although real-time CSLI draws upon the metadata generated by persistent surveillance, a targeted request for a limited amount of current information does not implicate concerns of undifferentiated collection and retroactive tracking to the same degree, lessening the risk of arbitrary government invasion. Moreover, narrow metadata requests—limited in amount and density—are less likely to reveal the privacies of life sought to be secured by the Fourth Amendment. It is worth noting, however, that repeated and proximate requests for real-time CSLI will, at some point, begin to take on many of the same characteristics and concerns of historical CSLI. As Justice Sotomayor observed in *Jones*, "even short-term monitoring" that produces a "precise, comprehensive record" may be sufficiently likely to reveal sensitive information,[306] strengthening the individual's privacy interest.

In step two, certain methods of acquiring real-time CSLI may diminish an individual's privacy interest in that metadata to an even lesser degree than historical CSLI. *Carpenter* recognized that a cellphone user has little practical ability to control the conveyance of metadata to a third-party, in part because CSLI is automatically generated by the cellphone itself "by dint of its operation, without any affirmative act on the part of the user."[307] When a cellular provider initiates the exchange of metadata at the government's request—pinging an otherwise inactive phone—the act of disclosure is entirely involuntary and the third-party doctrine has minimal diminishing effect.

The structured approach of the proposed framework bears fruit in the final step of the analysis, in which the individual's privacy interest is balanced against the diminishing effects of third-party disclosure. A case comparison helps illustrate this point. In *Sims v. State*,[308] police located a suspect by initiating the exchange of real-time CSLI metadata. The court concluded that Sims "did not have a legitimate expectation of privacy in his physical movements or his location as reflected in the less than three hours

---

306 United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

307 *Carpenter*, 138 S. Ct. at 2220; *see also id.* (observing that "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data").

308 569 S.W.3d 634.

of real-time CSLI records accessed by police by pinging his phone less than five times."[309] In reaching this result, the court focused almost exclusively on the amount of metadata requested.

Under the *Sims* approach, the search analysis does not turn on the content of the CSLI records but instead on whether the government searched or seized "enough" information that it violated a legitimate expectation of privacy. There is no bright-line rule for determining how long police must track a person's cellphone in real time before it violates a person's legitimate expectation of privacy in those records. Whether a person has a recognized expectation of privacy in real-time CSLI records must be decided on a case-by-case basis.[310]

The *Sims* court's approach suffers from two key deficiencies. First, it fails to account for both the commonalities and differences between historical and real-time CSLI. Second, it precludes the use of a balancing test for the creation of workable, bright-line rules.

The proposed framework remedies both concerns. As described above, the multi-factor analysis identifies three key distinctions between real-time and historical CSLI—retroactivity, amount or density, and control over the act of disclosure—each of which potentially impacts the outcome of the balancing test. They also provide a principled basis for the formulation of bright-line rules. In the *Sims* case, for instance, police sought a limited amount of current data targeting a specific individual. The suspect's privacy interest was therefore significantly weaker than that recognized in *Carpenter*. It was the police, however, that initiated the metadata exchange by pinging Sims's cellphone, minimizing any diminishing effects of third-party disclosure. Balancing these competing elements, a court might conclude that these distinctions are immaterial and that a warrant is therefore required for both historical and real-time CSLI. On the other hand, it might find the retroactive nature of the data request to be determinative and conclude that no warrant is required for real-time CSLI. Alternatively, it could draw a line at control over the act of disclosure, requiring police to obtain a warrant only before initiating a ping of the suspect's cellphone. In each case, the court would be engaging in the principled development of workable rules that effectuate the basic purposes of the Fourth Amendment.

---

309 *See, e.g.*, *id.* at 646.

310 *See, e.g.*, *id.*

IP Addresses.

> Each time a customer connects [to the Internet], the ISP [Internet Service Provider] assigns a unique identifier, known as an IP address, to the customer's computer terminal. Depending on the ISP, a customer's IP address can change each time he logs on to the Internet. ISPs retain . . . records of the IP addresses that they assign to customers [for up to ninety days].[311]

In many cases, a user's physical location can be derived from the IP address.

An ISP's IP address records share several common characteristics with CSLI. First, these records provide a comprehensive historical database of a user's points of Internet access, gathered on nearly every American.[312] Second, IP addresses "convey location information with similar degrees of specificity" as CSLI.[313] Third, Internet access is "indispensable to participation in modern society"[314] and IP addresses are automatically generated and collected as part of that process. Nevertheless, most courts to consider the application of *Carpenter* to IP address records "have adopted a categorical approach"[315] that essentially ignores these key differences; it is enough that IP addresses weren't CSLI.

Recognizing that the concerns expressed in *Carpenter* are implicated by other automated technologies, the proposed framework provides a more structured and principled basis for this distinction. As relevant to the identified factors, IP address records do not provide the amount or sustained density of locational metadata as CSLI, and that metadata is retained for a much shorter period. Hardwired and wireless broadband access is generally limited to certain locations, while cellular access is essentially identical to that of CSLI. Moreover, it can be argued that IP addresses are not automatically generated "without any affirmative act on the part of the user beyond powering up"[316] but requires the user to open an Internet browser or other network application. Each of these discrepancies' maps to a relevant

---

311 United States v. Christie, 624 F.3d 558, 563 (3d Cir. 2010).

312 *Supra* note 292.

313 United States v. Kidd, 394 F. Supp. 3d 357, 365 (S.D.N.Y. 2019).

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

315 *Kidd*, 394 F. Supp. 3d at 362.

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

factor in the proposed framework, potentially tilting the outcome of the balancing test and supporting a different bright-line rule.

Focusing exclusively on the potential for IP addresses to provide location information, the ultimate question remains whether this metadata is the type of "detailed and comprehensive record of a person's movements" that is likely to reveal the privacies of life.[317] A court might conclude, for instance, that Internet browsing will never provide the necessary amount or sustained density of locational data to provide that linkage. Courts may reach a different result, however, where the IP address is generated by software applications that automatically connect to the Internet even when not in use. Alternatively, a court might draw a line between stationary technologies (e.g., desktop, connected appliance) and mobile devices (e.g., laptop, smartphone) that "automatically connects to the wireless internet of his . . . subway, local coffee shop, or park."[318] As this discussion demonstrates, the proposed framework avoids the ham-handed division between CSLI and everything else. Instead, courts are able to draw principled distinctions between automated technologies and metadata sets.

CONCLUSION

In this Article, I have sought to do four things. First, I have attempted to demonstrate that the conventional narrative of modern Fourth Amendment doctrine obscures the dominant and broadly significant role of the public/private distinction in limiting privacy protections, even to the point of subordinating property rights. Second, I have framed the third-party doctrine as an application of the public/private distinction, eliminating an individual's legitimate privacy interest in personal information disclosed or conveyed to service providers. Third, I have explored how three recent Supreme Court cases promise to subvert the dominant role of the public/private distinction, applying a more flexible, balancing approach that contemplates Fourth Amendment protection for certain categories of data, independent of physical location. Fourth, I have proposed an analytical framework that brings structure and clarity to the Court's new approach.

Lower courts have struggled to understand and apply the Supreme Court's recent Fourth Amendment jurisprudence to other technologies. In

---

317 *Id.* at 2217.

318 *Kidd*, 394 F. Supp. 3d at 368.

the absence of clear guidance from the Court, most have narrowly confined these new cases to their precise facts, returning instead to a misconceived *Katz* analysis. Others have persevered but the results have been uneven and often contradictory.

This Article brings coherence to the difficult process of developing workable rules that adequately capture the Court's intended approach to difficult questions of digital privacy. It begins by reframing modern Fourth Amendment jurisprudence so as to illuminate the significance of recent cases. These cases are explored in depth, drawing out the basic structure of the Court's analysis and identifying those factors relevant to its balancing approach. Situating those factors in the broader analysis, a three-step framework is then proposed—to be used by lower courts as they develop bright-line rules for each of the different categories of data generated by digital technologies and services.