A DESCRIPTIVE ANALYSIS OF THE FOURTH AMENDMENT AND THE THIRD-PARTY DOCTRINE IN THE DIGITAL AGE

Peter C. Ormerod[†]

Lawrence J. Trautman[*]

[†] B.A. (magna cum laude), The George Washington University; J.D., The George Washington University Law School. Mr. Ormerod is an adjunct professor of business law at Western Carolina University. He may be contacted at ormerod.peter@gmail.com.

[*] B.A., The American University; MBA, The George Washington University; J.D., Oklahoma City University School of Law. Mr. Trautman is Assistant Professor of Business Law and Ethics at Western Carolina University. He may be contacted at Lawrence.J.Trautman@gmail.com.

The authors wish to extend particular thanks to Orin Kerr and Stephen Henderson. All errors and omissions are our own.

ABSTRACT

There are few areas of constitutional law that raise scholars' ire and trouble jurists like the Fourth Amendment's third-party doctrine. Making sense of the Court's distinctions between content and metadata and between personal communications and business records was already difficult with physical documents and analog technologies. But the proliferation of digital technologies has rendered obsolete the factual predicates underpinning those distinctions, and courts have struggled mightily with adapting third-party rules forged over thirty years ago to new technologies.

At the same time, the Supreme Court has become more explicit in fashioning distinct Fourth Amendment rules for digital

technologies. In a trio of 21st-century decisions, the Court has made clear—often by overwhelming votes—that the old rules no longer suffice.

These two strains of Fourth Amendment law are on a collision course—a collision scheduled for the Court's October 2017 Term. In June 2017, the Court granted certiorari in *Carpenter v. United States*, and the question presented is whether the government needs a probable cause warrant to obtain voluminous records about a cell phone's location—data termed cell site location information (CSLI)—from a wireless provider.

In this article, we first review the Court's 21st-century digital Fourth Amendment jurisprudence to tease out the Court's differential treatment of digital technologies. We then turn to the existing third-party doctrine and attempt to make sense of the doctrine's distinctions between content and metadata and between personal communications and business records. We examine how our understanding of the existing doctrine applies to digital information like the CSLI at issue in *Carpenter*. We conclude by reviewing some types of sensitive digital information that potentially lack Fourth Amendment protection under current doctrine.

Keywords: browsing history, Carpenter v. United States, cell phones, cell phone search, cell site locational information (CSLI), cloud computing, constitutional law, digital data, Fourth Amendment, Internet, iPhone, United States v. Jones, Katz v. United States, Kyllo v. United States, location data, metadata, United States v. Miller, privacy, Riley v. California, search incident to arrest, Smith v. Maryland, Stored Communication Act, Supreme Court, third-party doctrine, United States v. Wurie

JEL Classifications:

A DESCRIPTIVE ANALYSIS OF THE FOURTH AMENDMENT AND THE THIRD-PARTY DOCTRINE IN THE DIGITAL AGE

INTRODUCTION

On June 5, 2017, the U.S. Supreme Court granted a writ of certiorari in *Carpenter v. United States*.[1] *Carpenter* asks whether the government needs a probable cause warrant to obtain voluminous records of a cell phone's location data, which is known as cell site location information (CSLI).[2] According to Professor Orin S. Kerr, a foremost expert on the Fourth Amendment, the Court's grant in *Carpenter* is "a momentous development," because "the future of surveillance law hinges on how the Supreme Court rules."[3]

The government currently does not need a probable cause warrant to obtain CSLI from a telecommunication provider. Section 2703(d) of the Stored Communications Act (SCA) provides that the government may compel disclosure of CSLI whenever the government offers "specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation."[4]

And the government uses this authority: In 2016 alone, AT&T Wireless received over 50,000 requests for historic cell phone location data.[5] The facts of *Carpenter* starkly demonstrate the scope of information the government has authority to compel without a warrant—in this case, 127 days of the defendant's CSLI,

---

[1] 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (No. 16–402) (2017).

[2] Petition for Writ of Certiorari at i, 6, *Carpenter v. United States*, 137 S. Ct. 2211 (No. 16-402) [hereinafter *Carpenter* Cert. Petition].

[3] Orin S. Kerr, *Supreme Court agrees to hear 'Carpenter v. United States,' the Fourth Amendment historical cell-site case*, THE WASHINGTON POST (June 5, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/06/05/supreme-court-agrees-to-hear-carpenter-v-united-states-the-fourth-amendment-historical-cell-site-case/.

[4] Required Disclosure of Customer Communications or Records, 18 U.S.C.A. § 2703 (West, Westlaw through P.L. 115-117 approved 1/12/18).

[5] *See* AT&T FEBRUARY 2017 TRANSPARENCY REPORT 4 (2017) (showing the data for cell towers for January-June and July-December periods).

about four months.[6]

Carpenter implicates the third-party doctrine—the rule that people lack a reasonable expectation of privacy in information that third parties possess or know.[7] The third-party doctrine is one of the most widely disparaged constitutional rules still in force,[8] and not a single member of the current Court has participated in a decision that expressly applied the doctrine.[9] Making sense of the Court's distinctions between content and metadata and between personal communications and business records was already difficult with physical documents and analog technologies. The rapid proliferation of digital technology has made the task Herculean—rendering the rule's factual predicates obsolete and creating a vast cache of sensitive information only a subpoena away.

While the Court has studiously avoided addressing the viability of the third-party doctrine in the 21st century, the Court has become more explicit in fashioning distinct Fourth Amendment rules for digital technologies like thermal imaging cameras, GPS trackers, and smartphones seized incident to arrest. In this article, we first examine this digital Fourth Amendment jurisprudence and then try to make sense of how the third-party doctrine applies to data like Timothy Carpenter's CSLI. With the Court poised to address the constitutional contours of electronic surveillance law, we seek to provide helpful context about one of the most important cases of the Court's October 2017 term—and raise questions about the Fourth Amendment status of other types of sensitive digital data.

This article has six parts. In part one, we describe the Court's traditional approach to Fourth Amendment searches. In the second part, we discuss the Court's recent decisions that suggest the Fourth Amendment applies differently to digital technologies. In part three, we describe the third-party doctrine. In the fourth section, we explain the Stored Communications Act's statutory

---

[6] *Carpenter* Cert. Petition, *supra* note 2, at i; *16-402 Carpenter v. United States* (2017), https://www.supremecourt.gov/qp/16-00402qp.pdf.

[7] Daniel J. Solove, *A Taxonomy of Privacy*, 154(3) U. PA. L. REV. 477, 526 (2006).

[8] *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563–64 (2009) [hereinafter Kerr, *Third-Party Doctrine*] (reflecting that many scholars and state courts have begun rejecting this doctrine).

[9] Stephen E. Henderson, *Carpenter v. United States and the Fourth Amendment: The Best Way Forward*, WM. & MARY BILL RTS. J. (forthcoming) [hereinafter Henderson, *The Best Way Forward*].

framework. In part five, we relate the facts and the Sixth Circuit's opinions in *Carpenter* case, and we review other cases addressing how the Fourth Amendment applies to CSLI. Part six is our descriptive analysis: We explain how we interpret the current third-party doctrine and how the Court might apply that standard to CSLI. We conclude with a brief survey of other types of data that current doctrine does not protect.

I. TRADITIONAL FOURTH AMENDMENT SEARCH ANALYSIS

This section describes the traditional approach to the Fourth Amendment. We begin by discussing the ways the government conducts a search and then review how the Court responded to pre-digital technological advances in the 20th century.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[10] The current understanding of the two ways the government performs a Fourth Amendment search is based on the 2012 case *United States v. Jones*:[11] First, by physically trespassing on a suspect's property for the purpose of obtaining information, and second, by violating the "reasonable expectation of privacy" standard from Justice Harlan's concurrence in *Katz v. United States*.[12]

A. The Trespass Test

The *Jones* majority made clear that Justice Harlan's *Katz* test did not extinguish the pre-*Katz* rule: "The *Katz* reasonable-expectations test 'has been *added to*, not *substituted for*,' the traditional property-based understanding of the Fourth

---

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

[11] *United States v. Jones*, 565 U.S. 400 (2012).

[12] 389 U.S. 347 (1967); *see also* Nita A. Farahany, *Searching Secrets*, 160(5) U. PA. L. REV. 1239, 1246 (2012) (defining the "two-pronged privacy test"); Aya Gruber, *Garbage Pails and Puppy Dog Tails: Is that What* Katz *is Made of?,* 41 U.C. DAVIS L. J. 781, 785–86 (2008) (describing whether a search and seizure implicates the Fourth Amendment); Mary G. Leary, *Katz on a Hot Tin Roof—Saving the Fourth Amendment from Commercial Conditioning by Reviving Voluntariness in Disclosures to Third Parties,* 50 AM. CRIM. L. REV. 341, 342 (2013) (describing the *Katz* tests); Katherine J. Strandburg, *Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 101 (2011) (discussing *Katz*); Marc J. Blitz, *Stanley in Cyberspace: Why the Privacy Protection of the First Amendment Should Be More Like that of the Fourth*, 62 HASTINGS L.J. 357, 363 (2010) (further discussing Justice Harlan's rationale).

Amendment."[13] Under this property-based approach, the government performs a Fourth Amendment search when its agents physically intrude on a suspect's private property for the purpose of obtaining information.[14] Hence, in 1928's *Olmstead v. United States*,[15] the Court held that the government did not perform a search when agents attached wiretaps to telephone wires on public streets because "[t]here was no entry of the houses or offices of the defendants."[16] And in *Jones* itself, where government agents physically placed a GPS tracker on the underside of the suspect's automobile, the Court said: "The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."[17]

The Court also applied the trespass test in 2013's *Florida v. Jardines*.[18] In *Jardines*, law enforcement brought a drug-sniffing dog onto the porch of the defendant's home.[19] The dog indicated that it detected an illegal substance after sniffing the base of the defendant's front door.[20] On that basis, the officers obtained a search warrant for the defendant's home, which revealed marijuana plants.[21]

The Court held that the use of a drug-sniffing dog on the defendant's porch was a warrantless search because the "officers were gathering information . . . in the curtilage of the house, which we have held enjoys protection as part of the home itself,"[22] and

---

[13] *Florida v. Jardines*, 569 U.S. 1, 11 (2013) (quoting *Jones*, 565 U.S. at 409).

[14] *See Jones*, 565 U.S. at 420–21. In response to Justice Alito's concurrence, Justice Scalia is explicit that a trespass alone does not suffice: "Trespass alone does not qualify, but there must be conjoined with that what was present here: an attempt to find something or to obtain information." *Id.* at 408 n.5. Similarly, Justice Scalia distinguishes the curtilage of a home from an open field: "[T]he Government's position gains little support from our conclusion in *Oliver v. United States*, 466 U. S. 170 . . . (1984), that officers' information-gathering intrusion on an 'open field' did not constitute a Fourth Amendment search even though it was a trespass at common law . . . . Quite simply, an open field, unlike the curtilage of a home . . . is not one of those protected areas enumerated in the Fourth Amendment." *Id.* at 410–11.

[15] 277 U.S. 438 (1928).

[16] *Id.* at 464.

[17] *Jones*, 565 U.S. at 404–05.

[18] 569 U.S. 1 (2013).

[19] *Id.* at 3–4.

[20] *Id.* at 4.

[21] *Id.*

[22] *Id.* at 5–6.

because the officers "gathered that information by physically entering and occupying the area to engage in conduct not explicitly or implicitly permitted by the homeowner."[23]

Justice Scalia's majority opinion explicitly premised its conclusion on *only* trespass grounds: "[W]e need not decide whether the officers' investigation of [the defendant's] home violated his expectation of privacy under *Katz*. . . . That the officers learned what they learned only by physically intruding on [the defendant's] property to gather evidence is enough to establish that a search occurred."[24]

B. The Katz Reasonable Expectation of Privacy Test

Far murkier than the bright-line trespass test is Justice Harlan's two-factor standard from *Katz*. There, government agents placed listening devices on the top of public pay phones to eavesdrop on the defendant's conversations.[25] While no physical trespass occurred, the Court nonetheless held that the government had violated the defendant's Fourth Amendment rights.[26] In his concurrence, Justice Harlan provided what has since become the rule: "[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[27] Or as the Court put it in *Bond v. United States*[28]: "First, we ask whether the individual, by his conduct, has exhibited an actual expectation of privacy; that is, whether he has shown that he sought to preserve something as private. . . . Second, we inquire whether the individual's expectation of privacy is one that society is prepared to recognize as reasonable."[29]

The touchstone for determining whether the government has

---

[23] *Id.* at 6.

[24] *Jardines*, 569 U.S. at 11. In contrast, Justice Kagan's concurring opinion—which Justice Ginsburg and Justice Sotomayor joined and whose three votes were all necessary to Justice Scalia's five-vote majority—argued that the police violated *both* the trespass test and *Katz*'s reasonable expectation of privacy test: "Was this activity a trespass? Yes, as the Court holds today. Was it also an invasion of privacy? Yes, that as well. The Court today treats this case under a property rubric; I write separately to note that I could just as happily have decided it by looking to Jardines' privacy interests. A decision along those lines would have looked . . . well, much like this one." *Id.* at 13 (Kagan, J., concurring).

[25] *Katz*, 389 U.S. at 348.

[26] *Id.* at 353.

[27] *Id.* at 361 (Harlan, J., concurring).

[28] 529 U.S. 334 (2000).

[29] *Id.* at 338 (internal quotation marks omitted).

conducted a Fourth Amendment search is the point at which the government exposes or obtains information that someone has reasonably sought to keep private.[30] Fourth Amendment searches, in short, often contain an element of surprise. The Court has held that the government conducts a Fourth Amendment search when its agents expose or obtain information from inside a home,[31] a car,[32] a package,[33] and a person's pockets.[34] In contrast, the government does not conduct a search when its agents merely observe the outside of property,[35] observe something in plain view,[36] or observe something from a perspective frequented by the public.[37]

C. Pre-Digital Technologies: Airborne Observation Cases

This latter example is worth further exploration. In three cases from the 1980s, the Court considered how technology-enabled human flight has impacted Fourth Amendment expectations of privacy.[38] We term these decisions the "airborne observation cases," and they have particular relevance in our discussion of *Kyllo*, *infra*.

In *California v. Ciraolo*,[39] the police received an anonymous tip that the defendant was growing marijuana in his backyard.[40] Unable to confirm the tip from the ground level due to a tall fence encasing the backyard, two officers "secured a private plane and flew over [the defendant's] house at an altitude of 1,000 feet, within navigable airspace."[41] From this perspective, the officers identified marijuana plants growing in his backyard and photographed the area with a 35mm camera.[42] The defendant

---

[30] Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111(3) MICH. L. REV. 311, 316–17 (2012) [hereinafter Kerr, *Mosaic Theory*].

[31] *See, e.g.*, *Silverman v. United States*, 365 U.S. 505, 511 (1961).

[32] *See, e.g.*, *United States v. Ross*, 456 U.S. 798, 807–09 (1982).

[33] *See, e.g.*, *United States v. Jacobsen*, 466 U.S. 109, 114 (1984).

[34] *See, e.g.*, *Minnesota v. Dickerson*, 508 U.S. 366, 378 (1993).

[35] *See, e.g.*, *New York v. Class*, 475 U.S. 106, 114 (1986).

[36] *See, e.g.*, *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (explaining that the government has not violated a reasonable expectation of privacy when discovering what a person has "expose[d] to the 'plain view' of outsiders").

[37] *See, e.g., California v. Ciraolo*, 476 U.S. 207, 213–14 (1986); *Florida v. Riley*, 488 U.S. 445, 450 (1989).

[38] *California v. Ciraolo*, 476 U.S. 207; *Dow Chemical v. United States*, 476 U.S. 227 (1986); *Florida v. Riley*, 488 U.S. 445.

[39] 476 U.S. 207 (1986).

[40] *Id.* at 209.

[41] *Id.*

[42] *Id.*

challenged a warrant issued on the basis of the airborne observations, but the Court rejected his arguments that the Fourth Amendment forbade evidence collection by technologically-enabled human flight: "The observations . . . took place within public navigable airspace . . . in a physically nonintrusive manner [and] . . . [a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed."[43]

In *Dow Chemical v. United States*,[44] federal regulators—denied access to inspect an industrial complex—employed a commercial aerial photographer, who used a "standard floor-mounted, precision aerial mapping camera, to take photographs of the facility from altitudes of 12,000, 3,000, and 1,200 feet."[45] As in *Ciraolo*, the aircraft was at all times lawfully within navigable airspace.[46] Relying on *Ciraolo*, the Court rejected the complex owner's Fourth Amendment challenge.[47] The Court suggested that "surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant."[48] But, the Court held, the technology employed here did not cross that threshold: "[T]he photographs here are not so revealing of intimate details as to raise constitutional concerns."[49]

In *Florida v. Riley*,[50] the police received a tip that the defendant was growing marijuana in a partially-enclosed greenhouse behind his home.[51] When an investigating officer discovered it was not possible to see inside the greenhouse from the ground level, he circled twice over the property in a helicopter at an altitude of 400 feet.[52] From that perspective, the officer made naked-eye observations of marijuana plants inside the greenhouse, and a subsequent search—executed pursuant to a search warrant obtained on the basis of the officer's observations—revealed

---

[43] *Id.* at 213–14.
[44] 476 U.S. 227 (1986).
[45] *Id.* at 229.
[46] *Id.*
[47] *Id.* at 234–36, 239.
[48] *Id.* at 238.
[49] *Id.*
[50] 488 U.S. 445 (1989).
[51] *Id.* at 448. We refer to this 1989 case as "*Florida v. Riley*," and we refer to 2014's *Riley v. California*, 134 S. Ct. 2473 (2014), as merely "*Riley*."
[52] *Id.*

marijuana plants growing inside the greenhouse.[53] Justice White's plurality opinion held: "Here, the inspection was made from a helicopter, but as is the case with fixed-wing planes, 'private and commercial flight [by helicopter] in the public airways is routine' in this country, and there is no indication that such flights are unheard of in [the defendant's jurisdiction]."[54]

Justice O'Connor's concurring opinion—which was necessary to the judgment—explained that the defendant in *Ciraolo* did not have a reasonable expectation of privacy "not because the airplane was operating where it had a 'right to be,' but because public air travel at 1,000 feet is a sufficiently routine part of modern life that it is unreasonable" to expect that property "will not be observed from the air at that altitude."[55] Note that her framing of the issue differs from Chief Justice Burger's in both *Ciraolo* and *Dow Chemical*: The government's aircrafts in those cases were "lawfully within navigable airspace" under local law.[56] Here, however, Justice O'Connor argued that "[i]f the public rarely, if ever, travels overhead at such altitudes, the observation cannot be said to be from a vantage point generally used by the public and [the defendant] cannot be said to have 'knowingly exposed' his greenhouse to public view."[57] Indeed, Justice Blackmun's dissent recognized that five justices agreed "the reasonableness of [the defendant's] expectation depends, in large measure, on the frequency of nonpolice helicopter flights at an altitude of 400 feet."[58]

D. Fourth Amendment Searches: The Element of Surprise and the Probabilistic Model

Justice O'Connor's approach was later adopted by a seven-justice majority in *Bond v. United States*.[59] In *Bond*, the defendant was riding a Greyhound bus from California to Arkansas.[60] At a required checkpoint stop in Texas, a federal border patrol agent

---

[53] *Id.* at 448–49.

[54] *Id.* at 450 (quoting *Ciraolo*, 476 U.S. at 215).

[55] *Id.* at 453 (O'Connor, J., concurring).

[56] *Dow Chemical v. United States*, 476 U.S. at 229; see also *Ciraolo*, 476 U.S. at 213 ("The observations . . . in this case took place within public navigable airspace.").

[57] *Florida v. Riley*, 488 U.S. at 455 (O'Connor, J., concurring) (internal quotation marks and alterations omitted).

[58] *Id.* at 467 (Blackmun, J., dissenting).

[59] *Bond v. United States*, 529 U.S. 334.

[60] *Id.* at 335.

boarded the bus to check the immigration status of the passengers.[61] Satisfied the passengers were lawfully in the country, the agent began to exit the bus, and along the way, he began squeezing the soft luggage that passengers had placed in the overhead storage compartments.[62] The agent squeezed a soft canvas bag above the defendant's seat and felt a "brick-like" object.[63] The defendant admitted the bag was his and agreed to allow the agent to open it; this further inspection led the agent to discover a "brick" of methamphetamine inside.[64]

The defendant argued that the government had violated a reasonable expectation of privacy when the agent manipulated his bag to ascertain information about its contents, and the government responded by arguing it was objectively unreasonable to expect that other people would not touch his bag.[65] The Court ruled for the defendant, reasoning:

> [A] bus passenger clearly expects that his bag may be handled. He does not expect that other passengers or bus employees will, as a matter of course, feel the bag in an exploratory manner. But this is exactly what the agent did here. We therefore hold that the agent's physical manipulation of petitioner's bag violated the Fourth Amendment.[66]

Importantly, the Court's formulation of a reasonable expectation of privacy did not hinge on what other passengers or bus employees *could do* or what they *might do*—but rather what they *might actually do*.[67] Or, as articulated by D.C. Circuit Judge

---

[61] *Id.*

[62] *Id.*

[63] *Id.* at 336.

[64] *Id.*

[65] *Bond v. United States*, 529 U.S. at 336–37.

[66] *Id.* at 338–39.

[67] *But see Illinois v. Caballes*, 543 U.S. 405 (2005) (holding that the use of a drug-sniffing dog to ascertain whether the trunk of the defendant's car contained marijuana was not a Fourth Amendment search). Some of the language in *Caballes* is indeed difficult to reconcile with *Bond*. In his majority opinion, Justice Stevens suggests that the likelihood that police would discover the drugs in the trunk was irrelevant to the Fourth Amendment analysis: "[T]he expectation that certain facts will not come to the attention of the authorities is not the same as an interest in privacy that society is prepared to consider reasonable." *Id.* at 408–09 (internal quotation marks omitted) (quoting *Jacobsen*, 466 U.S. at 122 ("The concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation, however well justified, that certain facts will not come to the attention of the authorities.")).

Ginsburg in *Jones*, the GPS tracking case: "[W]hether something is 'expose[d] to the public,' . . . depends not upon the theoretical possibility, but upon the actual likelihood, of discovery by a stranger."[68]

Professor Kerr has termed this method of search analysis the "probabilistic model,"[69] one of four different Fourth Amendment models the Court routinely picks and chooses between.[70] The probabilistic inquiry "is descriptive rather than normative: it tries to assess the likelihood that a person will be observed or a place investigated based on prevailing social practices."[71] More precisely, Professor Kerr explains, the probabilistic model "protects citizens against unexpected invasions of privacy," because when the government "collects evidence in a way that interferes with customs and social expectations, revealing what a reasonable person might expect would remain hidden, it violates a reasonable expectation of privacy."[72]

II. THE COURT'S ARPROACH TO THE FOURTH AMENDMENT AND DIGITAL TECHNOLOGIES

In several 21st-century decisions, the Court has suggested that distinct Fourth Amendment rules apply to digital technologies.[73]

---

[68] *United States v. Maynard*, 615 F.3d 544, 560 (D.C. Cir. 2010) (quoting *Katz*, 389 U.S. at 351), *aff'd sub nom. Jones*, 565 U.S. 400.

[69] *See* Kerr, *Mosaic Theory*, *supra* note 30, at 348–49 (citing Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60(2) STAN. L. REV. 503, 508–12 (2007) [hereinafter Kerr, *Four Models*]).

[70] *See* Kerr, *Four Models*, *supra* note 69, at 506–07 ("Scholars and students of Fourth Amendment law find the current approach frustrating because the courts routinely mix and match the four models. Most Supreme Court opinions feature multiple models to varying degrees, and they often switch from model to model without recognizing the change"). Professor Kerr's other three models are the private facts model, the positive law model, and the policy model. *See id.* at 506. The private facts model "asks whether the government's conduct reveals particularly private and personal information deserving of protection" and "focuses on the information the government collects rather than how it is collected." *Id.* The positive law model "considers whether the government conduct interferes with property rights or other legal standards outside the Fourth Amendment." *Id.* The positive law model has effectively been codified in recent Supreme Court decisions—namely, *Jones* and *Jardines*—which have established that physical trespass is its own, free-standing standard for Fourth Amendment searches, independent of *Katz*'s reasonable expectation of privacy standard. The policy model is a direct inquiry into "whether the police practice should be regulated by the Fourth Amendment." *Id.*

[71] *Id.* at 508.

[72] *Id.* at 509.

[73] We do not purport to offer a comprehensive accounting of every digital

We discuss three decisions in this section: warrantlessly aiming a thermal imaging camera at a home in 2001's *Kyllo v. United States*;[74] the warrantless Global Positioning System (GPS) tracking of a suspect's automobile for 28 days in 2012's *United States v. Jones*;[75] and warrantlessly searching a defendant's cell phone incident to his arrest in 2014's *Riley v. California*.[76]

A. Kyllo v. United States (2001)

The Court decided *Kyllo v. United States* in 2001, which asked whether aiming a thermal imaging camera at a home was a Fourth Amendment search.[77] Below, we relate the facts and then discuss the Court's opinion.

1. Facts of *Kyllo*

In 1991, federal agents began to suspect that Danny Kyllo was growing marijuana inside his home.[78] Growing marijuana plants

---

technology and how the Fourth Amendment may or should apply differently to that digital technology vs. some comparable physical, mechanical, or analog technology. For our purposes, "analog technologies" are those technologies that (at least when they were first invented or implemented) convey or transmit information in a physically measurable, continuous waveform, such as through electric voltage. *See Analog Computer*, AMERICAN HERITAGE DICTIONARY, https://www.ahdictionary.com/word/search.html?q=analog+computer&submit.x=0&submit.y=0 ("A computer in which numerical data is represented by measurable physical variables, such as electric voltage or the position of an indicator."). Telephones, fax machines, vinyl records, VHS tapes, and radio transmitting beepers—such as the one at issue in *Knotts*—are prime examples of analog technologies. "Digital technologies" are those technologies that convey or transmit information in a discrete, binary format: ones and zeros. With digital technologies, information is counted, rather than measured. *See Digital*, AMERICAN HERITAGE DICTIONARY, https://www.ahdictionary.com/word/search.html?q=digital&submit.x=0&submit.y=0 ("Relating to or being a device that can generate, record, process, receive, transmit, or display information that is represented in discrete numerical form."). VoIP calls, scanners, CDs, DVDs, and GPS trackers are just a few examples of digital technologies, which correspond to the aforementioned analog technologies. And throughout the discussion that follows, we take "physical" to mean "[o]f or relating to material things: *a wall that formed a physical barrier*; *the physical environment*." *Physical*, AMERICAN HERITAGE DICTIONARY, https://www.ahdictionary.com/word/search.html?q=physical&submit.x=0&submit.y=0.

[74] 533 U.S. 27, 29 (2001).

[75] *Jones*, 565 U.S. at 403.

[76] 134 S. Ct. 2473 (2014), *decided together with, United States v. Wurie* (No. 13-212).

[77] *Kyllo v. United States*, 533 U.S. at 29.

[78] *Id.* at 29. *See also* Joel R. Reidenberg, *Privacy in Public*, 69 U. MIAMI L. REV. 141, 145 (2014); Richard Henry Seamon, *Kyllo v. United States and the Partial*

indoors typically requires high-intensity lamps, so the federal agents trained an Agema Thermovision 210 thermal imaging camera at Kyllo's home on one night in January 1992.[79] Thermal imaging cameras "detect infrared radiation, which virtually all objects emit but which is not visible to the naked eye,"[80] and converts that radiation "into images based on relative warmth—black is cool, white is hot, shades of gray connote relative differences; in that respect, it operates somewhat like a video camera showing heat images."[81] The agents' thermal imaging scan of Kyllo's home "took only a few minutes and was performed from the passenger seat of [one agent's] vehicle across the street from the front of the house and also from the street in back of the house."[82]

The scan revealed that portions of Kyllo's home were significantly warmer than his neighbors' homes.[83] A federal magistrate judge issued a search warrant for Kyllo's home based on informants' tips, utility bills, and the thermal imaging results.[84] Execution of the search warrant revealed that Kyllo's home hosted an indoor marijuana-growing operation with more than 100 plants.[85] After the district court denied Kyllo's suppression motion, he entered a conditional guilty plea and appealed.[86]

The U.S. Court of Appeals for the Ninth Circuit initially remanded for an evidentiary hearing about the intrusiveness of the agents' thermal imaging scan of Kyllo's home.[87] The district court upheld the validity of the warrant after finding that the Agema 2010 "is a non-intrusive device" that "did not show any people or activity within the walls of the structure," that it "cannot penetrate walls or windows to reveal conversations or human activities," and that "[n]o intimate details of the home were observed."[88] A divided panel of the Ninth Circuit eventually

---

Ascendance of Justice Scalia's Fourth Amendment, 79 WASH. U. L. Q. 1013, 1016 (2001); David A. Sklansky, *Back to the Future: Kyllo, Katz, and Common Law,* 72 MISS. L.J. 143, 169–70 (2002) (for further discussion).

79 *Kyllo*, 533 U.S. at 29.

80 *Id.*

81 *Id.* at 29–30.

82 *Id.* at 30.

83 *Id.*

84 *Id.*

85 *Kyllo*, 533 U.S. at 30.

86 *Id.*

87 *Id.*

88 *Id.*

affirmed.[89] The Supreme Court ruled in favor of Kyllo, 5-4, holding that use of the thermal imaging camera was an unreasonable warrantless Fourth Amendment search.[90]

2. The Court's Opinion

The analysis portion of Justice Scalia's majority opinion begins by observing that technological advances have undoubtedly affected the degree of privacy secured by the Fourth Amendment.[91] In support of that proposition, Justice Scalia cites *Ciraolo*, discussed above, which recognized that "technology enabling human flight has exposed to public view (and hence, we have said, to official observation) uncovered portions of the house and its curtilage that once were private."[92] Justice Scalia frames the issue in *Kyllo* in terms of "what limits there are upon this power of technology to shrink the realm of guaranteed privacy."[93]

Within the framework of *Katz*'s reasonable-expectation-of-privacy test, Justice Scalia's majority opinion held: "We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' . . . constitutes a search—at least where (as here) the technology in question is not in general public use."[94] The Court rejected arguments advanced by the government and the dissent that sought to downplay the intrusiveness of this particular thermal imaging scan: A contrary holding "would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home. While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development."[95]

Perhaps the narrowest reading of *Kyllo* focuses on two aspects of how this case is distinct from *Dow Chemical*. The first aspect is the police's target: In *Kyllo*, the government used technology to obtain otherwise inaccessible information about the inside of a

---

89 *United States v. Kyllo*, 190 F. 3d 1041, 1047 (9th Cir. 1999).
90 *Kyllo*, 533 U.S. at 40.
91 *Id.* at 33–34.
92 *Id.* at 34.
93 *Id.*
94 *Id.* (quoting *Silverman v. United States.*, 365 U.S. at 512).
95 *Kyllo*, 533 U.S. at 35–36.

home,[96] whereas the information in *Dow Chemical* was "an industrial complex, which does not share the Fourth Amendment sanctity of the home."[97] The Court pointedly noted: "In the home, our cases show, all details are intimate details, because the entire area is held safe from prying government eyes."[98]

The second aspect is the familiarity and availability of the technology used to obtain that information: In *Dow Chemical*, the government used a fixed-wing aircraft and a precise camera.[99] These are undoubtedly significant technological advancements since the Founding, but they are quite familiar and common to twenty-first century Americans.[100] In *Kyllo*, however, the government used a thermal imaging camera, which Justice Scalia repeatedly described as "technology . . . not in general public use."[101]

To be sure, these two aspects are probably enough to explain the different result in the three airborne observation cases and *Kyllo*. But Justice Scalia's opinion goes further, highlighting a concern that digital technologies may eventually eradicate any and all semblance of privacy—both inside the home and elsewhere.[102] The beginning of Justice Scalia's analysis provides: "This [conclusion] assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[103] A broader reading focuses the Court's appreciation that technology potentially poses an existential threat to Fourth Amendment privacy.[104] The government argued that the thermal imaging did

---

[96] *Id.* at 29.

[97] *Id.* at 37.

[98] *Id.* The emphasis on the sanctity of the home—and the government's interference with an individual's property interests—was later confirmed through the revival of the trespass test in *Jones* and in the trespass test's application in *Jardines*.

[99] *Dow Chemical v. United States*, 476 U.S. at 229.

[100] The most obvious issue with this narrower interpretation is that it seems unlikely that Justice Scalia's analysis of Fourth Amendment protection would hinge on how common and familiar the information-gathering technology is. Put another way, we don't think the result of *Kyllo* would be any different if, at some point in the near future, the general public use of thermal imaging cameras became common.

[101] *Kyllo*, 533 U.S. at 34, 40 ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant.").

[102] *Id.* at 28.

[103] *Id.* at 34.

[104] *Id.* at 35–36 n.3. There can be little doubt Justice Scalia found potential future technological advances vexing, demonstrated by a footnote that notes the

not significantly compromise Kyllo's privacy, but the Court said it didn't matter: "While it is certainly possible to conclude from the videotape of the thermal imaging that occurred in this case that no 'significant' compromise of the homeowner's privacy has occurred, we must take the long view, from the original meaning of the Fourth Amendment forward."[105]

The Court's conclusion suggests that technologically-enhanced searches are not just different as a matter of degree, but they are different as a matter of kind: Here, the government used digital technology to obtain information "that would previously have been unknowable without physical intrusion."[106] The Court is thus explicitly treating a digital, technologically-enhanced search differently from a physical search. The concern animating this distinction is circumvention—that the government should be prohibited from using technology in a manner that undermines Fourth Amendment restrictions on physical information-gathering techniques.

Justice Scalia also hints that he would not limit this line of analysis to only prohibit obtaining information digitally that could not have otherwise been constitutionally collected.[107] Responding to the dissent in footnote No. 2, Justice Scalia contends it is "quite irrelevant" that similar information about the relative heat inside Kyllo's home could potentially have been gleaned through constitutionally permissible alternative means, such as "by observing snowmelt on the roof."[108] Justice Scalia argues: "The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment."[109] This suggestion takes on new importance in the case discussed next.

B. United States v. Jones (2012)

The Court decided a second case about digital information-gathering in 2012's *United States v. Jones*, which concerned long-term GPS tracking of the suspect's automobile.[110] Below, we relate

---

"ability to 'see' through walls and other opaque barriers is a clear, and scientifically feasible, goal of law enforcement research and development."

105 *Id.* at 40.

106 *Id.*

107 *See Kyllo*, 533 U.S. at 40 (discussing a bright-line Fourth Amendment rule).

108 *Id.* at 35 n.2.

109 *Id.*

110 *Jones*, 565 U.S. at 402.

the facts, discuss a relevant precedent, examine the D.C. Circuit's opinion, and then analyze the Court's two concurring opinions.

1. Facts of *Jones*

In 2004, the FBI began to suspect Antoine Jones of trafficking in narcotics.[111] Government agents placed Jones under investigation, using techniques that included visual surveillance of the nightclub he owned and operated, installation of a camera focused on the nightclub's front door, and a pen register and wiretap on Jones's cell phone.[112] Based on information gleaned from these investigatory techniques, FBI agents applied to the U.S. District Court for the District of Columbia for a warrant authorizing the use of a Global Positioning System (GPS) tracking device on the automobile that Jones used.[113]

A warrant was issued, which required installation of the GPS tracker inside the District of Columbia and within 10 days.[114] On the eleventh day and in Maryland, agents installed a GPS tracking device on the undercarriage of Jones's car while it was parked in a public lot.[115] In the litigation that followed, the government conceded that its agents had not complied with the terms of the warrant and argued that a warrant was not required.[116]

Over the 28 days that followed installation of the GPS tracker, the government tracked the vehicle's every movement.[117] "By means of signals from multiple satellites, the device established the vehicle's location within 50 to 100 feet, and communicated that location by cellular phone to a Government computer. It relayed more than 2,000 pages of data over the 4-week period."[118] At his

---

[111] *Id.* S*ee generally* Peter P. Swire & Erin E. Murphy, *How to Address Standardless Discretion After Jones*, OHIO STATE PUBLIC LAW WORKING PAPER NO. 177 (2012); Susan Freiwald, *The Davis Good Faith Rule and Getting Answers to the Questions Jones Left Open,* 14 N.C. J.L. & TECH. 341 (2013); Mary Leary, *The Missed Opportunity of United States v. Jones: Commercial Erosion of Fourth Amendment Protection in a Post-Google Earth World*, 15 U. PA. J. CONST. L. 331 (2012); Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning,* 36 S. ILL. U. L.J. 475 (2012) (for further discussion).

[112] *Jones*, 565 U.S. at 402.

[113] *Id.* at 402–03.

[114] *Id.*

[115] *Id.* at 403. This was not the sole instance of government agents physically touching Jones's car: Agents "once had to replace the [GPS] device's battery when the vehicle was parked in a different public lot in Maryland." *Id.*

[116] *Id.* at 403 n.1.

[117] *Id.* at 403.

[118] *Jones*, 565 U.S. at 403.

trial, the government introduced GPS-derived location data that connected Jones to a stash house that contained $850,000 in cash, 97 kilograms of cocaine, and 1 kilogram of cocaine base.[119] The District Court denied most of Jones's suppression motion for the GPS-derived location data.[120] Jones was convicted, sentenced to life in prison, and appealed.[121]

2. The Applicability of the Court's Decision in *Knotts*

The District Court relied on the Court's holding in *United States v. Knotts*[122] in its denial of Jones's suppression motion.[123] The differences between *Knotts* and *Jones* are particularly illuminating for our purposes of distinguishing between analog and digital technologies.

In *Knotts*, the police were investigating the defendant for manufacturing methamphetamine.[124] Upon learning that one of Knotts's coconspirator would purchase a five-gallon drum of chemicals, the police obtained the consent of the chemical vendor to place a radio beeper inside the drum.[125] As the Court explained, "[a] beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver."[126] The police followed the coconspirator's car containing the drum from where it was purchased in Minneapolis, Minnesota, to a secluded cabin near Shell Lake, Wisconsin, a journey of about 100 miles.[127] For most of the drive, agents maintained visual contact with the coconspirator's vehicle, but exclusive use of the beeper became necessary near the end of the drive.[128]

The Court held that no search occurred:

> A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the

---

[119] *Id.* at 403–04.

[120] *Id.* at 403. "The District Court granted the motion only in part, suppressing the data obtained while the vehicle was parked in the garage adjoining Jones's residence. It held the remaining data admissible."

[121] *Id.* at 404.

[122] 460 U.S. 276 (1983).

[123] *United States v. Jones*, 451 F. Supp. 2d 71, 88 (D.D.C. 2006), *aff'd in part, rev'd in part sub nom. Maynard*, 615 F.3d 544, *aff'd Jones*, 565 U.S. 400.

[124] *United States v. Knotts*, 460 U.S. at 277.

[125] *Id.* at 278.

[126] *Id.* at 277.

[127] *Id.*

[128] *Id.* at 278–79.

> coconspirator] traveled over the public streets, he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.[129]

The District Court reasoned that the same analysis applied to monitoring using a GPS device.[130]

3. The D.C. Circuit and the Supreme Court Majority's Opinions

A panel of the U.S. Court of Appeals for the District of Columbia Circuit unanimously reversed on the GPS Fourth Amendment issue.[131] Judge Douglas H. Ginsburg concluded that *Knotts* was inapplicable because the Court "explicitly distinguished between the limited information discovered by use of the beeper—movements during a discrete journey—and more comprehensive or sustained monitoring of the sort at issue in this case."[132] Specifically, Judge Ginsburg cited the following passage from *Knotts* to argue that the Court had specifically reserved the question of how the Fourth Amendment applies to the more comprehensive type of surveillance implicated by the GPS tracker: "[I]f such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[133]

After finding the Court's holding in *Knotts* inapplicable, Judge Ginsburg's Fourth Amendment inquiry asked two questions: First, did Jones actually expose to the public his every movement in the car over the 28-day tracking period? Second, did Jones constructively expose to the public his every movement in the car over the 28-day tracking period?[134]

In addressing whether Jones's movements were actually exposed, Judge Ginsburg first discussed many of the same precedents reviewed above in section I.C—namely, *Ciraolo*, *Florida v. Riley*, and *Bond*.[135] In discussing these particular cases,

---

129 *Id.* at 281–82.
130 *United States v. Jones* (D.D.C.), 451 F. Supp. 2d at 88.
131 *Maynard*, 615 F.3d at 568.
132 *Id.* at 556 (citing *Knotts*, 465 U.S. at 283).
133 *Knotts*, 465 U.S. at 84.
134 *Maynard*, 615 F.3d at 558–59.
135 *Id.* at 559.

Judge Ginsburg asked whether the totality of Jones's movements *might actually* be observed by a member of the public.[136] Judge Ginsburg answered:

> [W]e hold the whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil. It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's hitherto private routine.[137]

Judge Ginsburg similarly concluded that Jones's movements were not constructively exposed:

> The whole of one's movements over the course of a month is not constructively exposed to the public because . . . that whole reveals far more than the individual movements it comprises. The difference is not one of degree but of kind, for no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life, nor the departure from a routine that, like the dog that did not bark in the Sherlock Holmes story, may reveal even more.[138]

Further, Judge Ginsburg explained why the whole was more than merely the sum of its parts:

> Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a

---

[136] *See id.* ("In considering whether something is 'exposed' to the public as that term was used in Katz we ask not what another person can physically and may lawfully do but rather what a reasonable person expects another might actually do.").

[137] *Id.* at 560.

[138] *Id.* at 562.

> month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.[139]

Considered as a collective whole, Judge Ginsburg held the 28 days of GPS monitoring was a Fourth Amendment search because it revealed "an intimate picture of the subject's life that he expects no one to have—short perhaps of his spouse."[140]

The D.C. Circuit denied the government's petition for rehearing over the dissent of four judges.[141] Judge Brett Kavanaugh's dissent from the denial for rehearing en banc argued the government's interference with Jones's property interests—when agents warrantlessly installed the GPS tracker and changed its batteries—constituted a Fourth Amendment search.[142]

A majority of the U.S. Supreme Court later adopted Judge Kavanaugh's suggestion.[143] As discussed above in section I.A, a five-justice majority held that the government conducted an unreasonable, warrantless search when its agents physically placed the GPS tracker on the underside of Jones's vehicle.[144] Justice Alito wrote an opinion concurring in the judgment, which was joined by Justice Ginsburg, Justice Breyer, and Justice Kagan.[145] Justice Sotomayor joined Justice Scalia's majority opinion, but she also filed a separate concurring opinion.[146] We discuss the two concurring opinions in detail below because a close reading suggests there are five votes to significantly alter how the Court analyzes digitally-aggregated information that was physically exposed to third parties.

---

139 *Id.*

140 *Maynard*, 615 F.3d at 563.

141 *United States v. Jones*, 625 F.3d 766, 767 (D.C. Cir. 2010), *denying reh'g en banc to Maynard*, 615 F.3d 544, *aff'd sub nom. Jones*, 565 U.S. 400.

142 *United States v. Jones*, 625 F.3d at 769–71 (Kavanaugh, J., dissenting).

143 *See Jones*, 565 U.S. at 413 (for holding).

144 *Id.*

145 *Id.* at 418 (Alito, J., concurring).

146 *Id.* at 413 (Sotomayor, J., concurring).

4. Justice Alito's Opinion

Most of Justice Alito's opinion criticizes the majority's revival of the trespass test.[147] At the end of his opinion, however, Justice Alito argues that the 28 days of monitoring constituted a violation of *Katz*'s reasonable-expectation-of-privacy test.[148] Justice Alito's analysis is significantly shorter than Judge Ginsburg's, but both jurists seem to agree that the proper subject for the *Katz* inquiry was the entire 28-day monitoring period, rather than analyzing each individual trip in a vacuum.[149]

But importantly, Justice Alito and Judge Ginsburg differ on precisely what expectation of privacy the government violated here. Judge Ginsburg's probabilistic analysis asked whether the totality of Jones's movements over 28 days might actually be observed by a member of the public; he answered that question no because "the likelihood a stranger would observe all those movements is not just remote, it is essentially nil."[150] Justice Alito's focus is instead what society expects *the police to do*: "[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not secretly monitor and catalogue every single movement of an individual's car for a very long period."[151] Professor Kerr's discussion of Justice Alito's opinion explains that Justice Alito "shift[ed] the probabilistic inquiry from what a person might expect the public to *see* to what a person might expect that police to *do*."[152] And Justice Alito argues—excepting "extraordinary offenses" and "investigation[s] of unusual importance"—

---

147 *See id.* at 424–25 (Alito, J., concurring).

> [T]he Court's reasoning largely disregards what is really important (the *use* of a GPS for the purpose of long-term tracking) and instead attaches great significance to something that most would view as relatively minor (attaching to the bottom of a car a small, light object that does not interfere in any way with the car's operation). Attaching such an object is generally regarded as so trivial that it does not provide a basis for recovery under modern tort law.

148 *Id.* at 430–31 (Alito, J., concurring).

149 *Jones*, 565 U.S. at 430 (Alito, J., concurring) ("[R]elatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."). *See also* Kerr, *Mosaic Theory*, *supra* note 30, at 327. ("Like the D.C. Circuit, Justice Alito concluded that long-term GPS monitoring constituted a search while short-term monitoring did not.").

150 *Maynard*, 615 F.3d at 558.

151 *Jones*, 565 U.S. at 430 (Alito, J., concurring).

152 Kerr, *Mosaic Theory*, *supra* note 30, at 327.

comparable physical tracking and visual surveillance is "difficult and costly and therefore rarely undertaken" because "constant monitoring of the location of a vehicle for four weeks . . . would have required a large team of agents, multiple vehicles, and perhaps aerial assistance."[153]

Justice Alito thus implicitly echoes an important aspect of *Kyllo*—that digitally-enhanced searches are distinct from physical searches. In *Kyllo*, Justice Scalia was perturbed that the government used digital technology to obtain information "that would previously have been unknowable without physical intrusion."[154] But there is an important point of divergence between *Kyllo* and Justice Alito in *Jones* on this issue: The crux of the physical/digital distinction in *Kyllo* was that the police used a digital technology to obtain information that they could not have otherwise physically collected, because the information was about the inside of the suspect's home.[155] In *Jones*, however, Justice Alito seems to extend the point: It was theoretically possible the police could use physical means that did not run afoul of the Fourth Amendment to collect all of the same information about the suspect's movements.[156] It would be costly and difficult, but possible and constitutional. And yet Justice Alito seems prepared to treat the digitally-enhanced, effortless collection of Jones's movements differently as a matter of kind, rather than degree.

Justice Alito's opinion concludes by noting that it was unnecessary to "identify with precision the point at which the tracking of this vehicle became a search," because "the line was surely crossed before the 4-week mark."[157] In short, Justice Alito's opinion endorses drawing a line between traditional surveillance and digitally-aggregated information, but it does not determine where, exactly, that line lies.

5. Justice Sotomayor's Opinion

Justice Sotomayor joined Justice Scalia's majority opinion, but she also wrote a separate concurrence.[158] At bottom, Justice Sotomayor agreed with both Justice Scalia and Justice Alito: This was a search twice over—both a trespass and a violation of a

---

153 *Jones*, 565 U.S. at 429, 431 (Alito, J., concurring).
154 *Kyllo*, 533 U.S. at 50.
155 *Id.* at 34.
156 *Jones*, 565 U.S. at 422 (Alito, J., concurring).
157 *Id.* at 430 (Alito, J., concurring).
158 *Id.* at 413 (Sotomayor, J., concurring).

reasonable expectation of privacy.[159]

Justice Sotomayor's opinion is particularly notable in two respects. First, Justice Sotomayor explicitly says the time has come to revisit and alter how the third-party doctrine applies in the digital age:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year.[160]

Justice Sotomayor calls for the Court to "cease[] . . . treat[ing] secrecy as a prerequisite for privacy."[161] And she goes on to endorse a distinct approach to the third-party doctrine first raised by Justice Marshall's dissent in *Smith v. Maryland*[162]—that the scope of disclosure of information to third parties should be limited to the specific purpose for which it was disclosed:

> I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth

---

[159] *See id.* at 414–15 (Sotomayor, J., concurring).

> I join the Court's opinion because I agree that a search within the meaning of the Fourth Amendment occurs, at a minimum, where, as here, the Government obtains information by physically intruding on a constitutionally protected area. . . . I agree with Justice Alito that, at the very least, longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.

(Internal quotation marks and alterations omitted).

[160] *Id.* at 417–18 (Sotomayor, J., concurring) (citing *Smith v. Maryland*, 442 U.S. 735, 742 (1979) (superseded by statute); *United States v. Miller*, 425 U.S. 435, 443 (1976) (superseded by statute)). *See infra* section III for an in-depth discussion of the third-party doctrine.

[161] *Id.* at 418 (Sotomayor, J., concurring).

[162] 442 U.S. 735 (1979) (superseded by statute).

> Amendment protection. See *Smith*, 442 U.S., at 749 (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes"); see also *Katz*, 389 U.S., at 351–352 ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected").[163]

The second notable aspect of Justice Sotomayor's opinion is how she frames the *Katz* inquiry. Citing the unique aspects of GPS monitoring—its effortless and comprehensive precision—Justice Sotomayor argued:

> I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people 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.[164]

This focus is slightly distinct from both Judge Ginsburg's approach and Justice Alito's approach. Judge Ginsburg asked what a person expects other people might actually see;[165] Justice Alito asked what a person expects the police to do;[166] and Justice Sotomayor's approach asked "whether police conduct collected so much information that it enabled the government to learn about a person's private affairs more or less at will."[167]

But most important for our purposes is that Justice Sotomayor—more directly than Justice Scalia in *Kyllo* and Justice Alito here—seems prepared to adopt a distinction between physical and digitally-enhanced information gathering. She wrote: "I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques."[168] In support of this assertion, Justice

---

163 *Jones*, 565 U.S. at 418 (Sotomayor, J., concurring).
164 *Id.* at 416 (Sotomayor, J., concurring).
165 Kerr, *Mosaic Theory*, *supra* note 30, at 324.
166 *Id.* at 328.
167 *Id.* (internal quotation marks omitted).
168 *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (citing *Kyllo*, 533 U.S. at

Sotomayor cites footnote two of Justice Scalia's *Kyllo* opinion—that it was "quite irrelevant" that constitutionally permissible observation could potentially have revealed the same information as was obtained with a digitally-enhanced technique.[169]

The takeaway is that members of the Court are increasingly adopting the position that digitally-enhanced techniques are distinct from traditional, physical information-gathering techniques. Justice Scalia's concern in *Kyllo* on this point was primarily about preventing circumvention—that the police should not be able to obtain information through digital means that they could not have permissibly physically collected.[170] Justice Alito here seems prepared to draw a line between constitutionally permissible physical surveillance methods and digitally-enhanced ones, a distinction premised on society's expectations of the logistical difficulties of old-fashioned surveillance.[171] And Justice Sotomayor goes further, seizing on the suggestion from *Kyllo* that the simple fact the police may permissibly collect information through physical means does not, categorically, render the digital collection of that same information constitutional.[172]

The Court's adoption of a bright-line distinction between the physical and the digital becomes most explicit in the cases discussed next.

C. Riley v. California and United States v. Wurie[173] (2014)

The Court confronted a common question in *Riley* and *Wurie*: "[W]hether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested."[174] Below, we first provide the facts of each case, relate

---

35 n.2).

169 *Id.*

170 *Kyllo*, 533 U.S. at 34.

171 *See id.* (discussing further the digital and physical search dichotomy).

172 *See Jones*, 565 U.S. at 411 (making the point that a *Katz* analysis would still apply).

173 728 F.3d 1 (1st Cir. 2013), *aff'd sub nom*. *Riley*, 134 S. Ct. 2473.

174 *Riley*, 134 S. Ct. at 2480; *cf.* Clark D. Cunningham, *Apple and the American Revolution: Remembering Why We Have the Fourth Amendment*, 126 YALE L.J. 216 (2016) (deriving underlying principles from the history of the Fourth Amendment and examining modern-day practices given these principles); Adam M. Gershowitz, *Password Protected? Can a Password Save Your Cell Phone from the Search Incident to Arrest?*, 96 IOWA L. REV. 1125 (2011) (considering the legal protection offered by a password lock on an arrestee's cell phone); Adam M. Gershowitz, *Seizing a Cell Phone Incident to Arrest: Data Extraction Devices, Faraday Bags, or Aluminum Foil as a Solution to the Warrantless Cell Phone*

the search-incident-to-arrest (SITA) rule from three precedents, and then discuss Chief Justice Roberts's majority opinion.

1. Facts of *Riley* and *Wurie*

In the first case, the police stopped David Riley for a traffic violation, which eventually led to his arrest for possession of concealed and loaded firearms.[175] A search of Riley incident to his arrest revealed a smartphone in a pants pocket, and an officer who accessed information on the phone noticed repeated use of a term associated with the "Bloods" street gang.[176] The Court described Riley's smartphone as "a cell phone with a broad range of other

Search Problem, 22 WM. & MARY BILL RTS. J. 601 (2013) (suggesting that cell phones only be seized incident to arrest and preserved pending a search warrant); JENNIFER KING & CHRIS J. HOOFNAGLE, RESEARCH REPORT: A SUPERMAJORITY OF CALIFORNIANS SUPPORTS LIMITS ON LAW ENFORCEMENT ACCESS TO CELL PHONE LOCATION INFORMATION (2008) (reporting the preferences of Californians regarding the use of retrospective location data from cell phones by law enforcement); Matthew E. Orso, *Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence,* 50 SANTA CLARA L. REV. 183, 185 (2010) (proposing a different standard for searching cell phones incident to arrest and distinguishing between smartphones and older devices); JENNIFER M. URBAN ET AL., MOBILE PHONES AND PRIVACY (2012) (reporting the results of a survey concerning the type of data stored on cell phones and attitudes on privacy of this data); Thomas K. Clancy, *Fourth Amendment Satisfaction — The "Reasonableness" of Digital Searches*, 48 TEX. TECH L. REV. 37 (2015) (discussing the impact of *Riley* on Fourth Amendment jurisprudence and suggesting that traditional rules of search and seizure need rethinking).

[175] *Riley*, 134 S. Ct. at 2480. *Cf.* Alan Butler, *Get a Warrant: The Supreme Court's New Course for Digital Privacy Rights after* Riley v. California, 10 DUKE J. CONST. L. & PUB. POL'Y 83 (2014) (discussing the impact of *Riley* on Fourth Amendment jurisprudence and considering its effects on related constitutional questions); Adam M. Gershowitz, *The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69(3) VAND. L. REV. 585 (2016) (discussing the impact of *Riley* on lower court decisions and criticizing the widespread practice of issuing overbroad search warrants); Matthew B. Kugler & Lior J. Strahilevitz, *The Myth of Fourth Amendment Circularity*, 84 U. CHI. L. REV. 1747 (2017) (reporting that changes in Fourth Amendment jurisprudence has little impact on the public's expectations of privacy); Adam Lamparello & Charles E. MacLean, Riley v. California*: Privacy Still Matters, but How Much and in What Contexts?,* 27 REGENT U.L. REV. 25 (2014) (hypothesizing how the Court's rationale in *Riley* will affect the Court's analysis in later cases concerning digital privacy); Richard H. McAdams, Riley*'s Less Obvious Tradeoff: Forgoing Scope-Limited Searches*, 48 TEX. TECH L. REV. 97 (2015) (examining the possibility of a warrant exception that would allow "scope-limited" search of cell phones incident to arrest); Leslie A. Shoebotham, *The Strife of Riley: The Search-Incident Consequences of Making an Easy Case Simple,* 75 LA. L. REV. 29 (2014) (criticizing *Riley*'s failure to address or reinforce the evidence-gathering justification of the search-incident doctrine).

[176] *Riley*, 134 S. Ct. at 2480.

functions based on advanced computing capability, large storage capacity, and Internet connectivity."[177]

Later, a detective specializing in street gangs further examined the contents of Riley's smartphone.[178] The detective's investigation revealed "photographs of Riley standing in front of a car they suspected had been involved in a shooting a few weeks earlier."[179] Riley was eventually convicted on three charges connected to that earlier shooting.[180] Before his trial, Riley argued "that the searches of his phone violated the Fourth Amendment, because they had been performed without a warrant and were not otherwise justified by exigent circumstances."[181] The trial court rejected that argument, the California Court of Appeal affirmed, and the California Supreme Court denied Riley's petition for review.[182]

In the second case, the police arrested Brima Wurie after observing him engage in an apparent drug sale.[183] The police confiscated two cell phones from Wurie's body in a search incident to arrest; unlike the smartphone at issue in the companion case, the mobile phone implicated here was a "flip phone," which the Court described "as a kind of phone that is flipped open for use and that generally has a smaller range of features than a smart phone."[184]

Shortly after arriving at the police station, "officers noticed that the phone was repeatedly receiving calls from a source identified as 'my house' on the phone's external screen."[185] The officers navigated through several menus to ascertain the phone number associated with the "my house" contact and used an online phone directory to trace the number to an apartment building.[186] A search of that address, executed pursuant to a warrant, revealed narcotics, firearms, and cash.[187] Wurie was indicted on several charges and "moved to suppress the evidence obtained from the search on his apartment, arguing it was the fruit of an unconstitutional search of his cell phone."[188] The district court

---

177 *Id.*
178 *Id.*
179 *Id.* at 2481.
180 *Id.*
181 *Id.*
182 *Riley*, 134 S. Ct. at 2481.
183 *Id.*
184 *Id.*
185 *Id.*
186 *Id.*
187 *Id.*
188 *Riley*, 134 S. Ct. at 2482.

denied his motion and Wurie was convicted.[189] A divided panel of the First Circuit reversed.[190]

The Court unanimously ruled in favor of both defendants in an opinion by Chief Justice Roberts.[191]

2. Search Incident to Arrest Precedents

As Chief Justice Roberts relates in his opinion, the search incident to arrest (SITA) rule is an exception to the warrant requirement. The government has the right, "always recognized under English and American law, to search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime."[192] Litigation about the SITA rule has since focused on the scope of the rule, "the extent to which officers may search property found on or near the arrestee."[193] There are three relevant Supreme Court precedents about the scope of the SITA rule.

The first is *Chimel v. California*.[194] The defendant was arrested inside his three-bedroom home, and the police proceeded to search the entire house, including the attic, the garage, and through the contents of drawers.[195] The Court articulated two rationales for the SITA rule and held that neither rationale justified the scope of the officers' search of the defendant's entire house.[196] The first rationale is the arresting officers' safety: "[I]t is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape."[197] The second rationale is preventing the destruction of evidence: "[I]t is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or

189 *Id.*
190 *Id.*
191 *Id.* at 2479.
192 *Weeks v. United States*, 232 U.S. 383, 392 (1914). *Cf.* Wayne A. Logan, *An Exception Swallows a Rule: Police Authority to Search Incident to Arrest,* 19 YALE L. & POL'Y REV. 381 (2001) (attempting to distinguish custodial arrests from other police encounters as a limit to the applicability of the search incident to arrest exception); Ric Simmons, *The Missed Opportunities of* Riley v. California, 12 OHIO ST. J. CRIM. L. 253 (2014) (discussing flaws and missed opportunities in *Riley*'s majority opinion).
193 *Riley*, 134 S. Ct. at 2482–83.
194 395 U.S. 752 (1969).
195 *Id.* at 753–54.
196 *Id.* at 762–63, 768.
197 *Id.* at 763.

destruction."[198]

Together, these two rationales provided the scope of the SITA rule: "There is ample justification, therefore, for a search of the arrestee's person and the area 'within his immediate control'—construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence."[199]

The second case is *United States v. Robinson*.[200] The defendant, Robinson, was arrested for driving with a revoked license.[201] The arresting officer conducted a patdown and felt an object in Robinson's pocket that he could not initially identify.[202] The officer removed the object, which was a crumpled up cigarette package, and when the officer opened it, he found narcotics inside.[203] The court below held that the search violated the Fourth Amendment because "Robinson was unlikely to have evidence of the crime of arrest on his person, and because it believed that extracting the cigarette package and opening it could not be justified as part of a protective search for weapons."[204]

The Supreme Court reversed, explaining that:

> [t]he authority to search the person incident to a lawful custodial arrest, while based upon the need to disarm and to discover evidence, does not depend on what a court may later decide was the probability in a particular arrest situation that weapons or evidence would in fact be found upon the person of the suspect.[205]

The Court did not distinguish between a search of Robinson's person and the officer's further inspection of the contents of an object found during the search of his person. Only later, in *United States v. Chadwick*,[206] did the Court qualify this aspect of the SITA rule: It was unreasonable and unconstitutional for the police to search a 200-pound footlocker incident to arrest because it was not "personal property . . . immediately associated with the person of the arrestee."[207]

---

198 *Id.*
199 *Id.*
200 414 U.S. 218 (1973).
201 *Id.* at 220.
202 *Id.* at 223.
203 *Id.*
204 *Riley*, 134 S. Ct. at 2483.
205 *Robinson*, 414 U.S. at 235.
206 433 U.S. 1 (1977).
207 *Id.* at 4, 15, *abrogated on other grounds by California v. Acevedo*, 500 U.S. 565 (1991).

The third and final case is *Arizona v. Gant*.[208] *Gant* concerned the scope of the SITA rule within the context of a vehicle.[209] The police had searched the passenger compartment of the vehicle after having handcuffed and secured the defendants in patrol cars.[210] The Court held that *Chimel* authorized a search of a vehicle "only when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search."[211] But the Court added an additional justification for the more thorough search here: A warrantless search of the vehicle's passenger compartment is permissible "when it is 'reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle.'"[212] This exception flows not from *Chimel* but rather from "circumstances unique to the vehicle context."[213]

3. The Court's Opinion

Chief Justice Roberts's analysis begins with the general Fourth Amendment proposition that the Court "generally determine[s] whether to exempt a given type of search from the warrant requirement 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'"[214] The Chief Justice notes that "a mechanical application of *Robinson* might well support the warrantless searches at issue here," but argues that digital searches are distinct from physical ones: "[W]hile *Robinson*'s categorical rule strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones."[215]

On the government interest side of the equation, the Court asked "whether application of the search incident to arrest doctrine to this particular category of effects would 'untether the

---

[208] 556 U.S. 332 (2009).

[209] *See generally id.* (finding that searching an arrestee's vehicle after he has been secured and the vehicle is outside his reach violates the Fourth Amendment SITA exception).

[210] *Id.* at 336, 344.

[211] *Id.* at 343.

[212] *Id.* (quoting *Thornton v. United States*, 541 U.S. 615, 632 (2004) (Scalia, J., concurring)).

[213] *Id.*

[214] *Riley*, 134 S. Ct. at 2484 (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)).

[215] *Id.*

rule from the justifications underlying the *Chimel* exception.'"[216] The Court answered that question no.[217] First, the Court reasoned that with respect to an officer's safety, "[d]igital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape."[218] As for the second justification for SITA—preventing the destruction of evidence—the government argued that digital data on a cell phone may be "vulnerable to two types of evidence destruction unique to digital data—remote wiping and data encryption."[219] The Court rejected this argument.[220] It reasoned that "in situations in which an arrest might trigger a remote-wipe attempt or an officer discovers an unlocked [and unencrypted] phone, it is not clear that the ability to conduct a warrantless search would make much of a difference."[221]

The Court then turned to the privacy interests at stake. The opinion notes that, while *Robinson* is the only Supreme Court decision approving of a search of the contents of an item found on an arrestee's person, the Court was aware of many other cases from Circuit Courts of Appeal, which include searches incident to arrest of billfolds, address books, wallets, and purses.[222] The government had argued that "a search of all data stored on a cell phone is materially indistinguishable from searches of these sorts of physical items."[223] The Court flatly rejected that assertion: "That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together."[224]

---

[216] *Id.* at 2485 (quoting *Gant*, 556 U.S. at 343).

[217] *See id.* at 2483–94 (explaining that *Chimel*'s SITA exception is to be used to protect the safety of the police officer or preserve evidence at risk of being destroyed when still within a defendant's reach, and that in the present case, the cell phone data posed no threat to the police officer and was no longer within reach of Defendant).

[218] *Id.* at 2485.

[219] *Id.* at 2486.

[220] *Riley*, 134 S. Ct. at 2486 (stating that the issues of remote wiping and data encryption are neither prevalent nor would they allow for sufficient searches to be made).

[221] *Id.* at 2487.

[222] *See id.* at 2488 (citing *United States v. Carrion*, 809 F. 2d 1120, 1123, 1128 (5th Cir. 1987); *United States v. Watson*, 669 F.2d 1374, 1383–84 (11th Cir. 1982); *United States v. Lee*, 501 F. 2d 890, 892 (D.C. Cir. 1974)).

[223] *Id.* (internal quotation marks omitted).

[224] *Id.* "The term 'cell phone' is itself misleading shorthand; many of these devic es are in fact minicomputers that also happen to have the capacity to be used as a telephone." *Id.* at 2489.

The Court then dedicated considerable space to explaining why digital searches are categorically different from physical ones—and make no mistake, the Court expressly held that digital searches "differ in both a quantitative and a qualitative sense" from searches of physical objects.[225]

On the quantitative differences, Chief Justice Roberts noted that "[o]ne of the most notable distinguishing features of modern cell phones is their immense storage capacity," [226] and that modern smart phones have a dizzying array of features, including camera, video player, rolodex, calendar, tape recorder, library, diary, albums, television, maps, and newspapers.[227] This quantitative difference in the amount of storage makes a cell phone much more similar to the 200-pound footlocker disallowed in *Chadwick* than the cigarette package permitted in *Robinson*.[228]

Chief Justice Roberts argued that the storage capacity of modern cell phones has four interrelated consequences for privacy, and his list is remarkable because each item suggests a bright-line distinction between what was previously physically feasible and what is now digitally possible.[229] First, a cell phone's collection of many different types of information "reveal much more in combination than any isolated record."[230] Second, the sheer amount of storage makes a cell phone's collection of any one type of information far more revealing than would have been physically possible: "The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet."[231]

Third, the amount of data contained on a cell phone has an unprecedented temporal scope. For example, "[a] person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone."[232] Fourth and finally, Chief Justice Roberts remarked on the proliferation and pervasiveness of these devices: "[M]any of the more than 90% of American adults who own a cell phone keep on

---

225 *Id.*at 2489.
226 *Riley*, 134 S. Ct. at 2489.
227 *Id.*
228 *Id.* at 2484–85.
229 *Id.*at 2489–90.
230 *Id.* at 2489.
231 *Id.*
232 *Riley*, 134 S. Ct. at 2489.

their person a digital record of nearly every aspect of their lives—from the mundane to the intimate," and "[a]llowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case."[233]

On the qualitative differences, Chief Justice Roberts discussed how two types of extremely revealing data logged by modern cell phones have changed the Fourth Amendment privacy equation: Internet browsing history and location data. Browsing history, he says, "could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of a disease, coupled with frequent visits to WebMD."[234] And "[h]istoric location information is a standard feature on many smart phones and can reconstruct specific movements down to the minute, not only around town but also within a particular building."[235]

Chief Justice Roberts, concluding the section of the opinion about qualitative differences, makes explicit that digital technology has fundamentally altered the Fourth Amendment calculus. Quoting Learned Hand in 1926—"that it is 'a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him'"[236]—Chief Justice Roberts concludes:

> If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.[237]

There are two additional noteworthy issues that Chief Justice Roberts's decision discusses. The first concerns cloud computing, which he explains "is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself."[238] An aspect that becomes important for our analysis below

---

[233] *Id.* at 2490.

[234] *Id.*

[235] *Id.*

[236] *Id.*at 2490–91 (quoting *United States v. Kirschenblatt*, 16 F.2d 202, 203 (2nd Cir. 1926)).

[237] *Id.* at 2491.

[238] *Id. See, e.g.*, Primavera De Filippi & Smari McCarthy, *Cloud Computing: Centralization and Data Sovereignty*, 3(2) EUR. J. L. & TECH. 1 (2012) (defining

is that the government conceded, and the Court implicitly agreed, that the SITA exception to the warrant requirement "may not be stretched to cover . . . a search of files stored in the cloud," because that would be akin to "finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house."[239] Professor Kerr explains that the Court's "special concern that allowing a cell phone search could accidentally allow a cloud search, too" can "only make[] sense as a concern if there is Fourth Amendment protection in stored contents in the cloud, too."[240]

The final noteworthy aspect of the Court's opinion comes in discussion of the government's proposed limiting principle—that "officers could search cell phone data if they could have obtained the same information from a pre-digital counterpart."[241] In rejecting this suggestion, the Court reiterated just how different digital data is:

> [T]he fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery. The fact that someone could have tucked a paper bank

---

and describing cloud computing); URS GASSER, CLOUD INNOVATION AND THE LAW: ISSUES, APPROACHES, AND INTERPLAY (Research Publication No. 2014-7 2014) (discussing the benefits of cloud computing); Paul Ohm, *The Fourth Amendment in a World Without Privacy,* 81 MISS. L.J. 1309 (2012) (describing a third-party rule); RANDAL C. PICKER, COMPETITION AND PRIVACY IN WEB 2.0 AND THE CLOUD (John M. Olin Law & Economics Working Paper No. 414 (2d series) 2008) (discussing cloud computing and computers in general); Paul M. Schwartz, *Information Privacy in the Cloud,* 161 U. PA. L. REV. 1623 (2013); Laurie B. Serafino, *'I Know My Rights, So You Go'n Need a Warrant for That:' The Fourth Amendment, Riley's Impact, and Warrantless Searches of Third-Party Clouds,* 19 BERKELEY J. CRIM. L. 154 (2014) (considering if third-party Internet service providers should not be denied Fourth Amendment protections); Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era,* 8 J. TELECOMM. & HIGH TECH. L. 359 (2010) (discussing cloud computing); Peter Swire, *From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud*, 2 INT'L DATA PRIV. L. 200 (discussing law enforcement's ability to access the cloud); CHRISTOPHER S. YOO, CLOUD COMPUTING: ARCHITECTURAL AND POLICY IMPLICATIONS (U. of Penn., Inst. for Law & Econ. Research Paper No. 11-15 2011) (describing "[c]loud computing's growing salience"); Jennifer C. Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326 (2015) (discussing generally how cloud computing works); John G. Palfrey, *The Public and the Private at the United States Border with Cyberspace*, 78(2) MISS. L. J. 241, 243 (2008) (discussing innovation in the U.S.).

[239] *Riley*, 134 S. Ct. at 2491.

[240] Orin S. Kerr, *The Significance of Riley*, THE WASHINGTON POST (June 25, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/25/the-significance-of-riley/.

[241] *Riley*, 134 S. Ct. at 2493.

> statement in a pocket does not justify a search of every bank statement from the last five years.[242]

The Court's opinion is very explicit that digital searches implicate quantitatively and qualitatively distinct privacy interests. And, critically, the Court held that the government's justifications for physical searches must have their own merit before the same rules will be applied to digital searches.[243] We do not seek to belabor the point. There is a significant amount of language in the Court's decision that suggests SITA is just "the tip of the iceberg" because "[w]e're now in a 'digital age,' and quantity of data and the 'qualitatively different' nature of at least some digital records changes how the Fourth Amendment should apply."[244]

In sum, the Court's evolution on digital searches began in *Kyllo*, progressed in *Jones*, and, as *Riley* suggests, appears to be accelerating further.

III. THE THIRD-PARTY DOCTRINE

The "third-party doctrine" is the name courts and scholars have given to the general rule that "if information is possessed or known by third parties, then, for purposes of the Fourth Amendment, an individual lacks a reasonable expectation of privacy in the information."[245] "By disclosing to a third party, the subject gives

---

[242] *Id.*

[243] *Id.*

[244] *The Significance of Riley*, *supra* note 240.

[245] Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 526 (2006). *See also*, *e.g.*, Jane R. Bambauer, *Other People's Papers*, 94 TEX. L. REV. 205 (2015) (discussing third parties and private individuals' information); William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment,* 129(7) HARV. L. REV. 1821 (2016) (discussing the Fourth Amendment and privacy); Steven M. Bellovin et al., *It's Too Complicated: How the Internet Upends* Katz, Smith, *and Electronic Surveillance Law*, 30(1) HARV. J. L. & TECH. 1 (2016) [hereinafter Bellovin, et al., *It's Too Complicated*] (considering metadata and privacy); Bernard Chao et al., *Why Courts Fail to Protect Privacy: Race, Age, Bias, and Technology*, 106 CAL. L. REV. __ (2018) (reflecting that average citizens do not fully understand the amount of access police have to their information); Thomas P. Crocker, *The Political Fourth Amendment,* 88(2) WASH. U. L. REV. 303 (2010) (describing the "third party" doctrine); David A. Harris, Riley v. California and *the Beginning of the End for the Third-Party Search Doctrine*, 18 U. PA. J. CONST. L. 895 (2016) (considering the application of the third-party doctrine to cloud computing); Olivier Sylvain, *Failing Expectations: Fourth Amendment Doctrine in the Era of Total Surveillance,* 49 WAKE FOREST L. REV. 485 (2014) (discussing warrant requirements); Joseph T. Thai, *Is Data Mining Ever a Search Under Justice Stevens' Fourth Amendment?,* 74 FORDHAM L. REV. 1731, 1733 (2006) ("the Court held decades ago that when we convey information to a third party, we give

up all of his Fourth Amendment rights in the information revealed."[246] Hence, under the third party doctrine, the government does not perform a Fourth Amendment search when it acquires previously-shared information from the third party.

A. Origins: Informants, Miller, and Smith

The third-party doctrine has its origins in cases involving confidential informants. In *On Lee v. United States*,[247] the defendant sold opium from his store, and he made incriminating statements to a friend who was—unbeknownst to him—a criminal informant wearing a recording device that captured the defendant's incriminating statements.[248] The Court rejected the defendant's argument that having an informant wear a wire was akin to placing a listening device in the store without a warrant: "The presence of a radio set is not sufficient to suggest more than the most attenuated analogy to wiretapping. Petitioner was talking confidentially and indiscreetly with one he trusted, and he was overheard."[249] The Court would go on to reaffirm this basic holding in cases decided both before[250] and after[251] *Katz*.

But it wasn't until after *Katz*, when the Court considered several cases about business records, that the broadest contours of the third-party doctrine took shape.[252] In *United States v. Miller*,[253] the government issued subpoenas to two banks where the defendant

---

up all constitutionally protected privacy in that information"). *But see* Monu S. Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54(1) B.C. L. REV. 1, 5 (2013) (considering "the concept of interpersonal privacy to examine how to extend Fourth Amendment protection to Facebook communications").

246 Kerr, *Third-Party Doctrine*, *supra* note 8, at 563.

247 343 U.S. 747 (1952).

248 *Id.* at 749.

249 *Id.* at 753–54.

250 *See, e.g.*, *Lopez v. United States*, 373 U.S. 427, 440 (1963) (finding no violation of the Constitution); *Lewis v. United States*, 385 U.S. 206, 212 (1966) (affirming a conviction); *Hoffa v. United States* 385 U.S. 293, 312 (1966) (holding that "the Constitution does not require us to upset the jury's verdict.").

251 *See, e.g.*, *United States v. White*, 401 U.S. 745, 752 (1971). "Inescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police."

252 *See, e.g.*, *Couch v. United States*, 409 U.S. 322 (1973) (finding that there are no protections after the records have been handed over to a tax accountant); *United States v. Payner*, 447 U.S. 727 (1980) (finding a violation of one's Fourth Amendment rights only occurs when one's own legitimate expectation of privacy is invaded).

253 425 U.S. 435 (1976).

had accounts.[254] The subpoenas required the banks to produce "all records of accounts, i.e., savings, checking, loan or otherwise,"[255] which the Court described as "negotiable instruments to be used in commercial transactions."[256] The defendant later sought to suppress the incriminating bank records on Fourth Amendment grounds.[257] The Court ruled against him:

> The [bank] depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[258]

The Court noted that all the bank records and documents "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[259]

Three years later, in *Smith v. Maryland*, the Court confronted the issue of pen registers.[260] "A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed."[261] In *Smith*, the police had a telephone company put a pen register on the home phone of a man they suspected was responsible for robbing the victim and then harassing her by making anonymous phone calls.[262] The pen register revealed the man was making the harassing calls.[263]

---

[254] *Id.* at 437.
[255] *Id.*
[256] *Id.* at 442.
[257] *Id.* at 440.
[258] *Id.* at 443 (citing *White*, 401 U.S. at 752; *Hoffa*, 385 U.S. at 302; *Lopez*, 373 U.S. at 427).
[259] *Miller*, 425 U.S. at 442.
[260] *Smith v. Maryland*, 442 U.S. 735. *See also* Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 991 (2007) (discussing Justice Marshall's dissent in *Smith*).
[261] *Smith*, 442 U.S. at 736 n.1 (internal quotation marks omitted) (quoting *United States v. New York Tel. Co.*, 434 U.S. 159, 161 n.1 (1977)).
[262] *Id.* at 737.
[263] *Id.*

The Court rejected the defendant's Fourth Amendment argument by applying the third-party doctrine from *Miller*: "When he used his phone, [the defendant] voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, [he] assumed the risk that the company would reveal to police the numbers he dialed."[264] The Court recognized that the phone company recorded the numerical information at issue "for a variety of legitimate business purposes."[265]

The defendant conceded "that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy."[266] Because the "switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber,"[267] the Court refused "to hold that a different constitutional result is required because the telephone company . . . decided to automate."[268] Again, the Court premised its conclusion on the fact the defendant voluntarily conveyed this information to a third party, and he assumed the risk the third party could disclose: The defendant "*voluntarily conveyed* to [the phone company] information that it had facilities for recording and that it was free to record."[269]

The third-party doctrine is among the most maligned constitutional doctrines still in force. Professor Wayne R. LaFave's treatise on the Fourth Amendment argues the Court's application of the third-party doctrine is "dead wrong"[270] and that "[s]uch a crabbed interpretation of the *Katz* test makes a mockery of the Fourth Amendment."[271] Professor Solove has argued, "The third-party doctrine presents one of the most serious threats to privacy in the digital age."[272] More than a dozen state Supreme Courts have either rejected the doctrine in whole or in part under their state constitutions.[273]

---

[264] *Id.* at 744.
[265] *Id.* at 743.
[266] *Id.* at 744.
[267] *Smith*, 442 U.S. at 744.
[268] *Id.* at 744–45.
[269] *Id.* at 745 (emphasis added).
[270] WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT 747 (4th ed. 2004).
[271] *Id.* at 736.
[272] Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74(2) FORDHAM L. REV. 747, 753 (2005).
[273] *See* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from*

Indeed, Professor Kerr has observed that "even the U.S. Supreme Court has never offered a clear argument in its favor."[274] Even the justification put forth by the *Smith* majority—that you assume the risk when you disclose to a third party[275]—is "a result rather than a rationale: A person must assume a risk only when the Constitution does not protect it. Exactly *why* the Constitution does not protect information disclosed to third parties has been left unexplained."[276]

B. Limits to the Third-Party Doctrine with Physical Spaces and Materials

Yet, as other scholars have argued, the third-party doctrine may not be as wide-ranging and all-encompassing as the Court suggested in *Miller*. There are several U.S. Supreme Court cases that suggest, without necessarily framing the analysis as implicating the third-party doctrine, that there are limits to the general maxim that people lack a reasonable expectation of privacy in anything and everything disclosed to or possessed by another. Below, we discuss three limitations on the broadest interpretation of the third-party doctrine—that people retain a reasonable expectation of privacy in physical spaces owned by a third party, in physical things left with another party, and in at least one type of information conveyed to a third party.

First, physical spaces. In *Stoner v. California,*[277] which predates *Katz*, the Court held that a search of the defendant's hotel room violated the Fourth Amendment.[278] The government had obtained the consent of the hotel clerk to search the defendant's room and argued nothing more was required.[279] The Court rejected the government's argument, holding that the police's reliance on the hotel clerk's expression of consent was not "a reasonable basis for the belief that the clerk had authority to consent to the search."[280]

Unreasonable Search, 55 CATH. U. L. REV. 373, 394–96 (2006) (listing and discussing the states that have rejected the doctrine).

[274] Kerr, *Third-Party Doctrine*, *supra* note 8, at 564.

[275] *See Smith*, 442 U.S. at 744 ("When . . . petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the normal course of business . . . [he] assumed the risk that the company would reveal to police the numbers he dialed.")

[276] Kerr, *Third-Party Doctrine*, *supra* note 8, at 564.

[277] 376 U.S. 483 (1964).

[278] *Id.* at 490.

[279] *Id.* at 487–88.

[280] *Id.* at 488.

Citing cases that held that a hotel guest[281] and an occupant of a room in a boarding home[282] retained reasonable expectations of privacy, the Court concluded that Fourth Amendment "protection would disappear if it were left to depend upon the unfettered discretion of an employee of the hotel."[283]

Second, lower courts have repeatedly held that people retain a reasonable expectation of privacy in physical items that are temporarily possessed by third parties. Professor Stephen Henderson has argued that *Miller* and *Smith* only support a "limited" third-party doctrine: "But if it is right to assert Fourth Amendment protection for the contents of telephone conversations even if obtained via the provider . . . then we have a 'limited' third party doctrine that only removes constitutional protection from information provided for a third party's use."[284] To support this interpretation, Professor Henderson has explained that courts "in other contexts have recognized a reasonable expectation of privacy in something left with a bailee"[285]—including a bag left with a store clerk,[286] luggage left with an airline,[287] and a briefcase left with a friend.[288]

Finally, the Court recognized a limitation specifically about information disclosed to a third party in *Ferguson v. City of Charleston*.[289] In that case, a state hospital adopted a policy in which pregnant patients suspected of drug use had their urine screened for narcotics; those who tested positive were referred to the local police for prosecution on drug offenses, child neglect, or both.[290] Despite the fact that pregnant patients provided their incriminating urine to third-party medical personnel—and the third-party medical personnel provided evidence to the government—the Court held that "[t]he reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared

---

281 *See Johnson v. United States*, 333 U.S. 10 (1948).

282 *See McDonald v. United States*, 335 U.S. 451 (1948).

283 *Stoner*, 376 U.S. at 490. *See also Lustig v. United States*, 338 U.S. 74 (1949); *United States v. Jeffers*, 342 U.S. 48 (1951).

284 Stephen E. Henderson, *After* United States v. Jones*, After the Fourth Amendment Third Party Doctrine*, 14(2) N.C. J. L. & TECH. 431, 437 (2013) [hereinafter Henderson, *After* Jones].

285 *Id.* at 437 n.36.

286 *See United States v. Most*, 876 F.2d 191, 198 (D.C. Cir. 1989).

287 *See United States v. Barry*, 853 F.2d 1479, 1481–84 (8th Cir. 1988).

288 *See United States v. Presler*, 610 F.2d 1206, 1213–14 (4th Cir. 1979).

289 532 U.S. 67 (2001).

290 *Id.* at 70–73.

with nonmedical personnel without her consent."[291] The majority opinion did not explicitly discuss the third-party doctrine.[292]

Justice Scalia's dissent, however, recognized the inconsistency between the majority's holding and *Miller*'s broad characterization of the third-party doctrine:

> Until today, we have *never* held—or even suggested—that material which a person voluntarily entrusts to someone else cannot be given by that person to the police, and used for whatever evidence it may contain. Without so much as discussing the point, the Court today opens a hole in our Fourth Amendment jurisprudence, the size and shape of which is entirely indeterminate. . . . I would adhere to our established law, which says that information obtained through violation of a relationship of trust is obtained consensually, and is hence not a search.[293]

Justice Scalia argued this case was not materially different than several confidential-informant cases: "[T]he Fourth Amendment does not protect a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it. . . . [F]or however strongly a defendant may trust an apparent colleague, his expectations in this respect are not protected by the Fourth Amendment when it turns out that the colleague is a government agent."[294]

C. Content Versus Metadata and Personal Communications Versus Business Records

The most important limitation on the third-party doctrine is the Court's long-recognized distinction between content and non-content information, which flows from *Katz*. In *Katz*, the defendant made calls from inside a public phone booth and government agents recorded his conversations by placing microphones outside

---

[291] *Id.* at 78.

[292] *See id.* at 69–86 (for J. Stevens' majority opinion).

[293] *Id.* at 95–96 (Scalia, J., dissenting) (footnotes omitted).

[294] *Id.* at 94 (Scalia, J., dissenting) (citing *Hoffa*, 385 U.S. at 302; *citing White*, 401 U.S. at 749) (internal quotation marks and citations omitted). To be sure, the majority reserved for remand whether the patients were coerced into providing the incriminating urine. But Justice Scalia persuasively argued the same amount of coercion is present in similar laws, meaning the "Fourth Amendment would invalidate those many state laws that require physicians to report gunshot wounds, evidence of spousal abuse, and (like the South Carolina law relevant here) evidence of child abuse." *Id.* at 97 (internal footnotes and citations omitted).

the booth.[295] In *Berger v. New York*,[296] the Court invalidated a New York state statute that allowed the police to wiretap and record a person's telephone conversations in real-time, pursuant to a court order that required less than probable cause.[297] In both cases a defendant disclosed incriminating information to a third party by way of a telephone, and in both cases the Court held that the police violated a reasonable expectation of privacy when they recorded the content of those conversations while the conversational content was in transit from the speaker's mouth to a third party's ear.[298]

As Justice Stewart recognized in his dissent in *Smith*, the Court's distinction between the content of conversations and non-content information (metadata) can hardly be justified on the rationale of the third-party doctrine alone:

> Nevertheless, the Court today says [Fourth Amendment] safeguards do not extend to the numbers dialed from a private telephone, apparently because when a caller dials a number the digits may be recorded by the telephone company for billing purposes. . . . The telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment. Yet we have squarely held that the user of even a public telephone is entitled "to assume that the words he utters into the mouthpiece will not be broadcast to the world."[299]

Justice Stewart identifies a significant limitation on the scope of the third-party doctrine—that people retain a reasonable expectation of privacy in the content of their conversations when speaking on the phone.

This, of course, raises an additional issue: Why do phone conversations receive more protection than, say, a conversation unwittingly had with a confidential informant? This tension between confidential informants and wiretaps is best explained in terms of consent: The Court's third-party jurisprudence recognizes a distinction between a conversation recorded with the consent of one of the conversation's participants—the confidential

---

[295] *Katz*, 389 U.S. at 348.
[296] 388 U.S. 41 (1967).
[297] *Id.* at 43–44.
[298] *Katz*, 389 U.S. at 353–54; *Berger*, 388 U.S. at 44–45.
[299] *Smith*, 442 U.S. at 746–47 (Stewart, J., dissenting) (quoting *Katz*, 389 U.S. at 352).

informant[300]—and a conversation recorded during transmission and without the consent of any participant—the wiretap.[301]

The Court's differential treatment of content and metadata is rooted in the historical realities of the physical transmission of letters. In the physical realm—viz., the U.S. Postal Service's transmission of a sealed letter—the Court long ago recognized a bright-line distinction between the plainly visible exterior and the sealed interior's contents: "[A] distinction is to be made between . . . what is intended to be kept free from inspection, such as letters, and sealed packages subject to letter postage; and what is open to inspection, such as newspapers, magazines, pamphlets, and other printed matter purposely left in a condition to be examined."[302]

Fourth Amendment protection thus applies to the contents of letters and sealed packages in the mail, but there is no Fourth Amendment protection "as to their outward form and weight,"[303] which includes the metadata required to effectuate transmission and delivery.[304] The Court reaffirmed this approach more than a century later: "Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable."[305] Even in circumstances where the government may "lawfully seize such a package to prevent loss or destruction of suspected contraband, the Fourth Amendment requires that they obtain a warrant before examining the contents of such a package."[306]

But not *all* content is protected. The documents submitted to the bank in *Miller* can hardly be categorized as non-content information. The Court held the contents of those documents were not protected by the Fourth Amendment because they were "negotiable instruments" that were "to be used in commercial transactions."[307] The third-party doctrine thus recognizes two distinctions—one between content and non-content and one between personal communications and business records. To be

---

300 *See, e.g.*, *On Lee*, 343 U.S. at 753–54.
301 *See, e.g.*, *Berger*, 388 U.S. at 45, 64.
302 *Ex parte Jackson*, 96 U.S. 727, 733 (1877).
303 *Id.*
304 *See id.* (following that the means required to effectuate delivery is not protected).
305 *Jacobsen*, 466 U.S. at 114.
306 *Id.*
307 *Miller*, 425 U.S. at 442.

sure, the content/metadata and communications/records distinctions are related concepts that overlap. *Katz* and *Smith* are prime examples: The dialing information in *Smith* was both metadata and a business record, while the phone conversation in *Katz* was both content and a personal communication. The difficulties arise when a piece of information is unprotected under one category but protected under the other. For example, in *Miller* the bank deposit slips and other documentation was both content and a business record.[308] The Court held there was no Fourth Amendment protection because it was clear the documents were business records and the defendant had exposed their contents to bank employees.[309] But what happens when it's not clear whether the content of a communication is a business record or not? And what about when it's unclear whether a defendant has consented to exposing contents to a third-party service provider?

Digital technologies have exacerbated the tensions with how the Court treats content and metadata and with how the Court treats personal communications and business records.[310] When you communicate with a computer—say, typing a URL into your browser—how do courts characterize that communication? Is it content or metadata? And is it a business record or a personal communication? Or how about when an email service provider scans the contents of your emails in order to facilitate advertisement targeting? Do the contents of your emails become business records? These are difficult issues, and courts have struggled to apply the Fourth Amendment tests from physical and analog technologies to digital ones. We explore these and related issues in detail in our analysis section, *infra*, section VI.

---

[308] *Id.* at 440.

[309] *Id.* at 442.

[310] *See* Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 628 (2003). Professor Kerr has explained that these difficulties were present, albeit "latent," in *Smith*. In *Smith*, the Court analogized dialing a phone number to contacting an operator and asking the operator to connect the call. Because disclosing the number to an operator would eliminate the speaker's reasonable expectation of privacy in the information, so did disclosing the information to the phone company's computer. So far, so good. The difficulty is that if a speaker calls the operator and places that request, then that request constitutes the *contents* of the communication between the speaker and the operator. The contents of the conversation between the speaker and the operator becomes the addressing information for the ensuing conversation between the speaker and the person he wishes to call. As a result, it is difficult in the abstract to say whether that initial communication should be considered addressing information or contents.

IV. THE STORED COMMUNICATIONS ACT

The Stored Communications Act (SCA) is a federal law that provides procedures for, among other things, compelling certain types of internet service providers ("ISPs" or "service providers") to disclose historical electronic data and records—content and non-content alike.[311] This section first provides an overview of the SCA and then addresses the procedures law enforcement must follow to compel metadata and content records.

A. Overview of the SCA

President Ronald Reagan signed the SCA into law on October 21, 1986, three years before the fall of the Berlin Wall, before one of the authors of this article was born, and when an extremely primitive new computer cost about $6,000, adjusted for inflation.[312] As others have noted, the statute "remains poorly understood" and is "dense and confusing."[313]

At the outset, it is important to understand that the SCA is not a comprehensive statute—it does not apply to real-time collection of electronic records, nor are its procedures necessarily consistent with the Fourth Amendment.[314] We do not undertake a comprehensive review of this esoteric and byzantine statute here.[315]

The SCA defines "content" in the same way that the Wiretap Act[316] (WTA) and Pen Register Statute[317] (PRS) do: "when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or

---

311 18 U.S.C.A. § 2703.

312 *Macintosh Plus*, WIKIPEDIA, https://en.wikipedia.org/w/index.php?title=Macintosh_Plus&oldid=777273019.

313 Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72(6) GEO. WASH. L. REV. 1208, 1208 (2004) [hereinafter Kerr, *SCA*].

314 *See id.* at 1214. ("The narrow scope of the SCA has two important implications. First, there are many problems of Internet privacy that the SCA does not address. The SCA is not a catch-all statute designed to protect the privacy of stored Internet communications; instead it is narrowly tailored to provide a set of Fourth Amendment–like protections for computer networks.").

315 For a far more in-depth analysis, we recommend Professor Kerr's excellent and comprehensive article on the SCA. *See also* Charles H. Kennedy & Peter Swire, *State Wiretaps and Electronic Surveillance After September 11*, 54 HASTINGS L.J. 971 (2002).

316 18 U.S.C. § 2511 et seq.

317 18 U.S.C. § 3121 et seq.

meaning of that communication."[318]

B. Compelling Non-Content Records

The SCA provides two different levels of protection for different types of non-content records. The statute distinguishes between subscriber information and other non-content records. As used here, "subscriber information" includes:

(A) name; (B) address; (C) local and long-distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number).[319]

To compel disclosure of this subscriber information, the government needs only a subpoena.[320]

To compel other non-content records, the government must obtain a court order under the SCA's section 2703(d).[321] Because historical cell-site location information (CSLI) is not explicitly listed as requiring only a subpoena, law enforcement requests for CSLI from wireless providers are done pursuant to a section 2703(d) order.[322]

Section 2703(d) of the SCA provides that the government may require a service provider to disclose any and all non-content records when "the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation."[323]

C. Compelling Content Records

The SCA also has two different tiers of protection for content records. First, we very briefly review the statutory framework. Then we address the constitutionality of the SCA providing law enforcement with a mechanism to compel the contents of communications without a probable cause warrant.

---

[318] 18 U.S.C.A. § 2510(8) (West, Westlaw through P.L. 115-117 approved 1/12/18).

[319] 18 U.S.C.A. § 2703(c)(2).

[320] *See id.* at § 2703(c)–(d) (for government's requirements to obtain disclosure).

[321] *Id.* at § 2703(d).

[322] *See, e.g.*, *United States v. Carpenter*, 819 F.3d 880, 884 (6th Cir. 2016).

[323] 18 U.S.C.A. § 2703(d).

1. Statutory Framework for Compelling Content

The SCA provides two different levels of protection for the content of communications. The precise statutory mechanism by which the law makes these distinctions is quite complex and premised on an outdated understanding of how people use digital devices and services, and we do not purport to provide a detailed explanation of that statutory mechanism here.[324]

First, the higher tier of protection. For unopened emails residing on a service provider's server, the SCA distinguishes between data less than 180 days old and data 180 days old and older.[325] The government needs a probable cause search warrant to compel unopened emails that have been on a service provider's server for 180 days or less.[326]

Why does the SCA treat unopened emails that are older than 180 days differently? Because back "in 1986, Congress viewed communications over six months old to be abandoned and therefore subject to reduced protection."[327]

The lower tier of protection applies to three different types of data: (1) unopened emails older than 180 days; (2) all opened emails; and (3) any and all other content files residing on a service provider's server.[328] Compelling any one or all of these types of data requires less than a probable cause search warrant: If the government provides notice to the owner of the communications, then it can compel this class of data with a subpoena or with a section 2703(d) order.[329]

The word "notice" is, however, misleading, because the government may delay providing notice to the owner of the data for up to 90 days if that notification might have an adverse

---

[324] *See* Kerr, *SCA*, *supra* note 316 (for further discussion of the statute).

[325] 18 U.S.C.A § 2703(a).

[326] *See id.* ("A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage . . . for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction.").

[327] Peter J. Henning, *Digital Privacy to Come Under Supreme Court's Scrutiny*, THE NEW YORK TIMES (July 10, 2017), https://www.nytimes.com/2017/07/10/business/dealbook/digital-privacy-supreme-court.html. *See also* Achal Oza, *Amend the ECPA: Fourth Amendment Protection Erodes as E-Mails Get Dusty*, 88(4) B.U. L. REV. 1043 (2008).

[328] *See K*err, *SCA*, *supra* note 316, at 1233 (discussing the SCA protections afforded different types of data).

[329] 18 U.S.C.A. § 2703(a)–(b).

result.[330] Adverse results include the destruction of evidence.[331] So if the government uses a subpoena to compel this class of data (i.e., opened emails, other content files, and unopened emails older than 180 days) and the government is concerned the owner may try to delete the data when she finds out the government is seeking it, notice to the owner may be delayed for up to three months.[332]

Also, recall that a section 2703(d) order—which is identical for compelling all non-content records—requires the government provide "specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation."[333] But because the standard for obtaining a section 2703(d) order is more exacting than a mere subpoena, in practice, the government may compel the contents of opened emails, other content files, and unopened emails older than 180 days with no more than a subpoena and a three-month delayed notice.[334]

2. The Constitutionality of Compelling Content Under the SCA

There is significant doubt about the constitutionality of several provisions of the SCA, but the U.S. Supreme Court has not (yet at least) squarely addressed the issue. The leading case is *United States v. Warshak*,[335] in which the U.S. Court of Appeals for the Sixth Circuit held that the government's compulsion of the content of the defendant's emails violated the Fourth Amendment.[336] Several circuits have agreed with *Warshak* in dicta that the government may not constitutionally compel the content of email communications without a probable cause warrant.[337]

In 2004, the government began to suspect Steven Warshak of using his company to engage in a variety of wide-ranging fraudulent practices.[338] Warshak had several email accounts with

---

330 18 U.S.C.A. § 2705(a)(1) (West, Westlaw through P.L. 115-117 approved 1/12/18).

331 *Id.* at § 2705(a)(2)(c).

332 *Id.* at § 2705(a).

333 18 U.S.C.A. § 2703(d).

334 *See* Kerr, *SCA*, *supra* note 316, at 1218–20 (discussing the practical uses of § 2703(d)).

335 631 F.3d 266 (6th Cir. 2010).

336 *Id.* at 288.

337 *See, e.g.*, *Visa Marketing v. Burkett*, 812 F.3d 954, 969 (11th Cir. 2016); *In re Grand Jury Subpoena*, 828 F.3d 1083, 1090–91 (9th Cir. 2016).

338 *Warshak*, 631 F.3d at 276–81.

different ISPs, including NuVox Communications.[339] In October 2004, the government used a provision of the SCA to order NuVox to prospectively preserve the contents of any emails to or from Warshak's email account.[340] In January 2005 and again in May 2005, the government served NuVox with subpoenas, compelling NuVox to disclose all of Warshak's emails the ISP had preserved.[341] The government compelled the contents of approximately 27,000 emails.[342] Under the delayed-notice provisions of the SCA, Warshak did not receive notice of either the preservation order or the subpoenas until May 2006.[343]

The court first noted that "Warshak plainly manifested an expectation that his emails would be shielded from outside scrutiny," particularly "[g]iven the often sensitive and sometimes damning substances of his emails."[344] The court then turned to the second prong of *Katz*, whether society is prepared to recognize Warshak's subjective expectation of privacy as objectively reasonable.[345]

The court reviewed how Fourth Amendment jurisprudence had evolved in response to technology during the 20th century to provide protection to phone calls that are roughly equivalent to the protections enjoyed by physical letters, the dominant form of communication at the time of the Founding.[346] The court held that the same principles apply to email:

> If we accept that an email is analogous to a letter or a phone call, it is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment. An ISP is the intermediary that makes email communication possible. Emails must pass through an ISP's servers to reach their intended recipient. Thus, the ISP is the functional equivalent of a post office or a telephone company. As we have discussed above, the police may not storm the post office and intercept a letter,

---

339 *Id.* at 283.
340 *Id.*; 18 U.S.C.A. § 2703(f).
341 *Warshak*, 631 F.3d at 283.
342 *Id.*
343 *Id.*
344 *Id.* at 284.
345 *Id.*
346 *Id.* at 285–86 ("[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish.").

> and they are likewise forbidden from using the phone system to make a clandestine recording of a telephone call—unless they get a warrant, that is. It only stands to reason that, if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception.[347]

The government argued that analogizing Warshak's email service provider to the post office or a phone company was inappropriate because NuVox contractually reserved the right to access Warshak's emails.[348] The court rejected the government's argument for two reasons, but it expressly reserved the question of whether a service provider's terms of service could ever defeat a reasonable expectation of privacy.[349]

First, the court noted that it could not be correct that "the mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy."[350] For support, the court observed that both the postal service and phone companies have the ability to access the contents of communications, but this ability does not defeat a reasonable expectation of privacy.[351] Second, the court reasoned that even a *right* to access the content of communications did not necessarily defeat a reasonable expectation of privacy.[352] For support, the court noted that, at the time *Katz* was decided, telephone companies traditionally had a right to monitor calls "when reasonably necessary to 'protect themselves and their properties against the improper and illegal use of their facilities.'"[353] The court found substantial similarity between the

---

[347] *Warshak*, 631 F.3d at 286 (citing *Jacobsen*, 466 U.S. at 114; *Katz*, 389 U.S. at 353).

[348] *Id.*

[349] *Id.* ("While we acknowledge that a subscriber agreement might, in some cases, be sweeping enough to defeat a reasonable expectation of privacy in the contents of an email account . . . we doubt that will be the case in most situations, and it is certainly not the case here." (citation omitted)).

[350] *Id.*

[351] *Id.* at 287 ("In *Katz*, the Supreme Court found it reasonable to expect privacy during a telephone call despite the ability of an operator to listen in. . . . Similarly, the ability of a rogue mail handler to rip open a letter does not make it unreasonable to assume that sealed mail will remain private on its journey across the country." (citing *Smith*, 442 U.S. at 746–47 (Stewart, J., dissenting) (citation omitted)).

[352] *Id.* at 287.

[353] *Warshak*, 631 F.3d at 287 (quoting *Bubis v. United States*, 384 F.2d 643, 648

telephone company's reserved right to listen to the content of calls and NuVox's reserved right to retain and access emails in its service provider agreement.[354]

The court addressed *Miller* last. The court opaquely alluded to the tension between *Katz* and *Miller*—which we discuss in detail in the analysis section VI, *infra*—when it observed that "the Supreme Court held that a bank depositor does not have a reasonable expectation of privacy in the *contents* of bank records, checks, and deposit slips."[355] The court found *Miller* distinguishable in two ways:

> First, *Miller* involved simple business records, as opposed to the potentially unlimited variety of "confidential communications" at issue here. Second, the bank depositor in *Miller* conveyed information to the bank so that the bank could put the information to use "in the ordinary course of business." By contrast, Warshak received his emails through NuVox. NuVox was an intermediary, not the intended recipient of the emails.[356]

With *Miller* distinguished, the court held that an email subscriber "enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP," thus requiring the government to obtain a probable cause warrant before compelling the contents of emails.[357] And it expressly held that "to the extent the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional."[358]

V. *CARPENTER* AND OTHER LOWER-COURT CSLI DECISIONS

In addition to the Sixth Circuit's decision in *Carpenter*, four other Circuit Courts of Appeal have squarely addressed the Fourth Amendment's applicability to CSLI: the Third Circuit, the Fourth

---

(9th Cir. 1967)).

354 *Id.* at 287.

355 *Id.* (citing *Miller*, 425 U.S. at 442) (emphasis added).

356 *Id.* at 288.

357 *Id.*

358 *Id. See also* Jonathan L. Zittrain, *Searches and Seizures in a Networked World*, 119 HARV. L. REV. 83, 85 (2006) ("There is little reason to think that people have — or ought to have — any less of a first-order reasonable expectation of privacy for e-mail stored on their behalf by Google and Microsoft than they would have if it were stored 'locally' in personal computers after being downloaded and deleted from their e-mail service providers.").

Circuit, the Fifth Circuit, and the Eleventh Circuit. In this section, we first relate the facts of *Carpenter* and describe the two Sixth Circuit panel opinions; second, we briefly describe CSLI decisions from other circuits.

A. Facts and Decision Below in Carpenter v. United States

In April 2011, the police arrested four men suspected of involvement in a string of armed robberies of electronics stores in and around Detroit, Michigan.[359] One of these suspects confessed that a group of co-conspirators was responsible for nine armed robberies in southeastern Michigan and northwestern Ohio between December 2010 and March 2011.[360] As part of his confession, the suspect told law enforcement that the conspiracy included up to 15 additional people whom served as getaway drivers and lookouts during the robberies.[361] The suspect who confessed provided his cell phone number—and the cell phone numbers of several additional members of the conspiracy—to the FBI.[362] FBI agents later reviewed the suspect's call records to identify additional cell phone numbers that the suspect had called around the time of the robberies.[363]

In May and June 2011, FBI agents applied for three orders from magistrate judges in the U.S. District Court for the Eastern District of Michigan under the SCA, seeking "transactional records" of 16 cell phone numbers from a several wireless telecommunication provider services (wireless providers).[364] The government's three applications included requests for the following information:

- The requested records included "all subscriber information, toll records and call detail records including listed and unlisted numbers dialed or otherwise transmitted to and from the target telephones from December 1, 2010 to [May 2, 2011]," a request for 152 days of records;[365]

---

[359] *Carpenter*, 819 F.3d at 884. *See also* Henderson, *The Best Way Forward, supra* note 9 (for more discussion of the facts underlying *Carpenter*).

[360] *Id.*

[361] *Id.*

[362] *Id.*

[363] *Id.*

[364] *Id.*

[365] *Carpenter*, 819 F.3d at 884 (internal quotation marks and alterations omitted); *see Carpenter* Cert. Petition, *supra* note 2, at 4 (listing the relevant dates and total number of days requested).

- The requested records also included "cell site information for the target telephones at call origination and at call termination for incoming and outgoing calls" for the same range of dates;[366]
- And that these records would "'provide evidence that . . . Timothy Carpenter and other known and unknown individuals' had violated the Hobbs Act, 18 U.S.C. § 1951."[367]

The magistrate judges granted the applications pursuant to section 2703(d) of the SCA.[368] Timothy Carpenter's wireless carrier, MetroPCS,[369] complied with the orders and provided the government with the above-described transactional records, telecommunications metadata, and CSLI for 127 days.[370]

On the basis of this and other information, the government charged Carpenter with six crimes related to the robberies.[371] The district court denied Carpenter's motion in limine to suppress the government's CSLI evidence on Fourth Amendment grounds.[372]

At trial, multiple co-conspirators testified that Carpenter organized most of the robberies, that he often provided the firearms for the robberies, and that he acted as a lookout during the robberies.[373] FBI agent Christopher Hess provided expert witness testimony about the government's CSLI evidence; he explained:

> [C]ellphones work by establishing a radio connection with nearby cell towers (or "cell sites"); that phones are constantly searching for the strongest signal from those towers; and that individual towers project different

---

366 *Carpenter*, 819 F.3d at 884.

367 *Id.* 18 U.S.C. § 1951 provides:

> "Whoever in any way or degree obstructs, delays, or affects commerce or the movement of any article or commodity in commerce, by robbery or extortion or attempts or conspires so to do, or commits or threatens physical violence to any person or property in furtherance of a plan or purpose to do anything in violation of this section shall be fined under this title or imprisoned not more than twenty years, or both."

18 U.S.C. § 1951 (2006).

368 *Carpenter*, 819 F.3d at 884; 18 U.S.C.A. § 2703(d).

369 The government also obtained two additional days' worth of Carpenter's transaction records and CSLI from Sprint, with whom MetroPCS has a roaming agreement. *See Carpenter* Cert. Petition, *supra* note 2, at 5–6.

370 *Id.* at 4–5 n.2 ("MetroPCS produced 127 days of records (December 1, 2010 through April 6, 2011).").

371 *Carpenter*, 819 F.3d at 884.

372 *Id.*

373 *Id.*

> signals in each direction or "sector," so that a cellphone located on the north side of a cell tower will use a different signal than a cellphone located on the south side of the same tower. Hess said that cell towers are typically spaced widely in rural areas, where a tower's coverage might reach as far as 20 miles. In an urban area like Detroit, however, each cell site covers "typically anywhere from a half-mile to two miles." He testified that wireless carriers typically log and store certain call-detail records of their customers' calls, including the date, time, and length of each call; the phone numbers engaged on the call; and the cell sites where the call began and ended.[374]

Using the data provided by MetroPCS, Hess created maps that showed Carpenter's phone was within one-half mile and two miles of the site of each robbery at approximately the same time the robberies occurred.[375]

The jury convicted Carpenter of five of the six charges, and he was sentenced to 1,395 months in prison.[376] On appeal to the Sixth Circuit, Carpenter challenged the district court's denial of his motion to suppress the government's CSLI evidence.[377]

A partially-divided panel of the Sixth Circuit affirmed.[378] Judge Raymond Kethledge, writing for the majority, concluded that *Smith* controlled and that Carpenter had no Fourth Amendment right to his CSLI.[379] The majority's Fourth Amendment analysis begins by noting that "the federal courts have long recognized a core distinction: although the content of personal communications is private, the information necessary to get those communications from point A to point B is not."[380] Judge Kethledge explained the differential treatment of conversations in *Katz* and numbers dialed in *Smith* and that a similar distinction applies to email.[381] But, he noted, "courts have not (yet, at least) extended [Fourth Amendment] protections to the internet analogue to envelope markings, namely the metadata used to route internet communications, like sender and recipient addresses on an email,

---

374 *Id.* at 885.
375 *Id.*
376 *Id.*
377 *Carpenter*, 819 F.3d at 885.
378 *Id.* at 893.
379 *Id.* at 887.
380 *Id.* at 886.
381 *Id.* at 887 (citing *Warshak*, 631 F.3d at 288.

or IP addresses."[382]

Characterizing Carpenter's CSLI as business records, Judge Kethledge concluded they "fall on the unprotected side of this line."[383] To support his conclusion that CSLI were no different from the pen register-generated records in *Smith*, he noted that CSLI records "say nothing about the content of any calls," that "wireless providers gathered [them] in the ordinary course of business," and that "carriers keep records of these data to find weak spots in their network and to determine whether roaming charges apply."[384] Judge Kethledge discussed the records at issue in *Smith* in detail, ultimately finding that Carpenter "lack[s] any property interest in cell-site records created and maintained by [his] wireless carriers," and that CSLI is generated "solely 'as a means of establishing communication.'"[385] This led Judge Kethledge to determine that "any cellphone user who has seen her phone's signal strength fluctuate must know that, when she places or receives a call, her phone 'exposes' its location to the nearest cell tower and thus to the company that operates the tower"[386]—a conclusion at odds with CSLI cases in the Third Circuit.

Finally, Judge Kethledge dismissed arguments that either *Jones* or *Riley* had any effect on *Smith*'s applicability. Concerning *Jones*, the majority first distinguished between the placement of a GPS tracker and collection of business records from a third-party service provider.[387] And, the panel held, CSLI is distinct from GPS tracking because CSLI is less precise.[388] Judge Kethledge summarily dismissed the Court's differential treatment of digital data in *Riley*, characterizing the Court's holding as only that "the government may not access a smartphone's internal data—or, one might say, its contents—without a warrant."[389]

Judge Branstetter Stranch concurred in the result but did not join the majority's Fourth Amendment analysis.[390] She began by

---

[382] *Id.* (citing *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010); *United States v. Perrine*, 518 F.3d 1196, 1204–05 (10th Cir. 2008); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2007)).

[383] *Carpenter*, 819 F.3d at 887.

[384] *Id.*

[385] *Id.* at 888 (quoting *Smith*, 442 U.S. at 741).

[386] *Id.* (citing *United States v. Davis*, 785 F.3d 498, 511 (11th Cir. 2015) (en banc); *In re Application for Historical Cell Site Data*, 724 F.3d 600, 614 (5th Cir. 2013)).

[387] *Id.* at 889.

[388] *Id.*

[389] *Carpenter*, 819 F.3d at 889.

[390] *Id.* at 893–94 (Stranch, J., concurring).

discussing the differences between GPS and CSLI and describing a previous Sixth Circuit decision, *United States v. Skinner*,[391] in some detail.[392] In *Skinner*, the federal government obtained a court order authorizing the defendant's wireless carrier to provide the government real-time access to the defendant's phone's GPS data, and a panel of the Sixth Circuit rejected the defendant's Fourth Amendment challenge.[393] The *Skinner* majority "acknowledged 'the concern raised by Justice Alito's concurrence in *Jones'* that long-term location monitoring in government investigations impinges on expectations of privacy, but held that the concern was not implicated in Skinner's case because of the relatively short tracking period [three days]."[394] The *Skinner* majority cited Justice Alito's opinion in *Jones* for the proposition that three days of real-time tracking was sufficiently short to "accord[] with expectations of privacy that our society has recognized as reasonable,"[395] but "framed this conclusion with a key caveat: 'There may be situations where police, using otherwise legal methods, so comprehensively track a person's activities that the very comprehensiveness of the tracking is unreasonable for Fourth Amendment purposes.'"[396]

Judge Stranch then turned to the *Carpenter* majority's primary rationale—that the defendant lacked any Fourth Amendment interest in CSLI records because they are business records that do not contain the content of communications.[397] While noting the majority's analysis "reflects a valid distinction," she nonetheless expressed that it "is here . . . that my concern arises with the existing tests."[398]

Judge Stranch explained that "it seems to me that the business records test is ill suited to address the issues regarding personal

---

391 690 F.3d 772 (6th Cir. 2012).

392 *Carpenter*, 819 F.3d at 894–95 (Stranch, J., concurring).

393 *See Skinner*, 690 F.3d at 774–77 (explaining that the government used data emanating from Skinner's pay-as-you-go cell phone to determine its real-time location and that Skinner's Fourth Amendment violation argument lacked merit because Skinner did not have a reasonable expectation of privacy in the phone data).

394 *Carpenter*, 819 F.3d at 895 (Stranch, J., concurring) (quoting *Skinner*, 690 F.3d at 780).

395 *Skinner*, 690 F.3d at 780 (quoting *Jones*, 565 U.S. at 430 (Altio, J., concurring).

396 *Carpenter*, 819 F.3d at 895 (Stranch, J., concurring) (quoting *Skinner*, 690 F.3d at 780).

397 *Id.*

398 *Id.*

location that are before us."[399] Conceding that CSLI is less precise than GPS, Judge Stranch was nonetheless disturbed by the sheer length of the monitoring here—approximately four months:

> Even taking into account the less precise nature of CSLI as compared to GPS, such extensive monitoring far exceeds the threshold we identified in *Skinner* and the warrantless acquisition of such substantial quantities of CSLI implicates the *Skinner*/*Jones* concerns. I do not think that treating the CSLI obtained as a "business record" and applying that test addresses our circuit's stated concern regarding long-term, comprehensive tracking of an individual's location without a warrant. At issue here is neither relatively innocuous routing information nor precise GPS locator information: it is personal location information that partakes of both. I am also concerned about the applicability of a test that appears to admit to no limitation on the quantity of records or the length of time for which such records may be compelled.[400]

Judge Stranch's opinion concludes that, despite any constitutional defect with the SCA, the good-faith exception to the exclusionary rule should apply to the CSLI records in this case—thus resulting in her concurrence in the judgment.[401]

B. Other Circuit Court Decisions Concerning CSLI

Aside from the Sixth Circuit's two opinions in *Carpenter*, four other Circuit Courts of Appeals have considered the Fourth Amendment status of historical CSLI, which has generated an additional 18 judicial opinions.[402] We do not attempt a

---

399 *Id.*

400 *Id.* at 895–96.

401 *Id.* at 896.

402 *United States v. Stimler*, 864 F.3d 253, 263 (3d Cir. 2017); *id.* at 275 (Restrepo, J., concurring); *United States v. Graham*, 824 F.3d 421, 422 (4th Cir. 2016) (en banc); *id.* at 438 (Wilkinson, J., concurring); *id.* at 441–42 (Wynn, J., dissenting in part and concurring in the judgment); *United States v. Graham*, 796 F.3d 332, 332 (4th Cir. 2015), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016); *id.* at 377 (Thacker, J., concurring); *id.* at 378–79 (Motz, J., dissenting in part and concurring in the judgment); *Davis*, 785 F.3d at 500 (en banc); *id.* at 519 (Pryor, J., concurring); *id.* at 521–22 (Jordan, J., concurring); *id.* at 524 (Rosenbaum, J., concurring); *id.* at 533 (Martin, J., dissenting); *United States v. Davis,* 754 F.3d 1205, 1205 (11th Cir. 2014), *rev'd en banc*, 785 F.3d 498 (11th Cir. 2015) (unanimous panel); *Historical Cell Site Data*, 724 F.3d at 600; *id.* at 615–16 (Dennis, J., dissenting); *In re Application of U.S. for an Order Directing a*

comprehensive accounting of these opinions in this section, so a brief review of the highlights follows.

There are two primary sources of contention between judges who have concluded the Fourth Amendment protects CSLI and those who have concluded just the opposite, and both concern how the third-party doctrine applies to CSLI. First, judges disagree whether cell phone users "voluntarily convey" their location information to their wireless providers.[403] The Court expressly premised its assumption-of-risk conclusion in both *Miller* and *Smith* on the fact the defendants had "voluntarily conveyed" information later disclosed by third parties to the authorities.[404] Courts have divided sharply on whether cell phone users voluntarily convey their CSLI. Some judges argue that CSLI is unlike the *Smith* pen register because CSLI is generated more often than just when a person affirmatively initiates a call.[405] Other judges have focused on what the operative wireless carrier's privacy policy says about information collection and disclosure.[406]

Provider of Electronic Commc'n Service to Disclose Records to the Gov't, 620 F.3d 304, 304 (3d Cir. 2010) (en banc); *id.* at 319–20 (Tashima, J., concurring) [hereinafter *In re Application* (Third Circuit).

[403] *See, e.g.*, *Graham*, 796 F.3d at 353 (concluding CSLI is not voluntarily conveyed), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016) (concluding CSLI is voluntarily conveyed); *Davis*, 785 F.3d at 511 (concluding that, because cell phone users are generally aware that their calls are connected through cell towers, use of a cell phone amounts to voluntary conveyance of "their general location within that cell tower's range"); *Historical Cell Site Data*, 724 F.3d at 614 ("[U]sers know that they convey information about their location to their service providers when they make a call."); *In re Application* (Third Circuit), 620 F.3d at 317–18 ("[W]hen a cell phone user receives a call, he hasn't voluntarily exposed anything at all.").

[404] *See Miller*, 425 U.S. at 442 ("All of the documents . . . contain only information *voluntarily conveyed* to the banks and exposed to their employees in the ordinary course of business." (emphasis added)); *see also Smith*, 442 U.S. 735, 745 ("[P]etitioner *voluntarily conveyed* to [the phone company] information that it had facilities for recording and that it was free to record." (emphasis added)).

[405] *See, e.g.*, *Graham*, 796 F.3d at 354 (4th Cir. 2015) ("The service provider automatically generates CSLI in response to connections made between the cell phone and the provider's network, with and without the user's active participation."), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016); *Stimler*, 864 F.3d at 266 n.40 ("The government's expert explained that CSLI is no longer only generated at the beginning and end of each call, but at every point at which an individual moves closer to a different cell tower . . . .[and] CSLI records are generated far more frequently than they used to be . . . "); *In re Application* (Third Circuit), 620 F.3d at 317 ("A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way.").

[406] *See, e.g.*, *United States v. Graham*, 846 F. Supp. 2d 384, 401 (D. Md. 2012) ("[A]ny assumption of ignorance is belied by Sprint/Nextel, Inc.'s privacy policy, which informs its customers that it collects location data."); *Graham*, 796 F.3d at 345 ("[T]he policy only states that Sprint/Nextel *collects* information about the

The majority of courts, however, have concluded that CSLI is in fact voluntarily conveyed to wireless carriers.[407]

Second, courts have struggled to determine whether CSLI is purely metadata or not.[408] Judges who argue CSLI is more than simple metadata call attention to the invasive nature of comprehensive location tracking[409] and the reality that many types of ostensibly non-content data can be extremely revealing.[410] Judges who argue CSLI is nothing more than routing information rely on analogies to physical letters and pen registers.[411] We discuss these decisions in greater detail in the next section.

VI. A DESCRIPTIVE ANALYSIS OF THE THIRD-PARTY DOCTRINE

In this section, we assemble the pieces of the foregoing in an

---

phone's location—not that it discloses this information to the government or anyone else."), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016).

[407] *See, e.g.*, *Graham,* 824 F.3d at 430 ("A cell phone user voluntarily enters an arrangement with his service provider in which he knows that he must maintain proximity to the provider's cell towers in order for his phone to function."); *Historical Cell Site Data*, 724 F.3d at 611–14 (explaining that the U.S. Supreme Court in a line of cases has held that the government can observe "whatever information . . . voluntarily transmitted to third parties."); *Davis*, 785 F.3d at 509 ("The Supreme Court 'consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties'").

[408] *See, e.g.*, *Davis*, 785 F.3d at 537 (Martin, Cir. J., dissenting) ("The majority suggests that e-mails can be distinguished because cell site location data is 'non-content evidence' [but] offers no coherent definition of the terms 'content' and 'non-content'"); *Graham*, 796 F.3d at 358 ("CSLI is . . . more than simple routing information"), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016); *Graham*, 824 F.3d at 433 ("CSLI, which identifies the equipment used to route calls and texts, undeniably belongs in the non-content category").

[409] *See, e.g.*, *Graham*, 796 F.3d at 359 (referring to the "deep-seated uneasiness and apprehension" regarding the government's capability for electronic surveillance), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016).

[410] *See, e.g.*, *Davis*, 785 F.3d at 537 (Martin, Cir. J., dissenting).

> For instance, would a person's Google search history be content or non-content information? Though a person's search terms may seem like "content," a search term exists in the web address generated by a search engine. And web addresses, like phone numbers, seem like quintessentially non-content information that merely direct a communication.

Id.

[411] *See, e.g.*, *Graham*, 824 F.3d at 433 ("CSLI is non-content information because 'cell-site data—like mailing addresses, phone numbers, and IP addresses—are information that facilitate personal communications, rather than part of the content of those communications themselves.'" (quoting *Carpenter*, 819 F.3d at 887–88)).

attempt to forge a comprehensive understanding of the Court's current third-party standard. This section proceeds in three parts. In the first section, we discuss the first component of the third-party standard: the concept of a voluntary conveyance—where it originates, what it means, and how we believe it applies to CSLI. The second component concerns content, and in the second section, we try to make sense of the Court's third-party cases that protect some, but not all, content disclosed to third parties. In the final section, we discuss other bases the Court may use to resolve *Carpenter* and we raise additional issues about what the current third-party doctrine does not protect.

A. Voluntary Conveyance and CSLI

We interpret the Court's third-party doctrine to require a more substantial analysis than summarily determining whether a particular piece of information looks more like the "personal communication" in *Katz* or more like the "business records" in *Miller* and *Smith*. The first component of the Court's current third-party standard, we believe, requires that all information—traditional understandings of content and metadata alike—must be voluntarily conveyed before losing Fourth Amendment protection.

1. Voluntary Conveyance

The first question for CSLI is whether the suspect "voluntarily conveyed" the information to the third party. Not only did the Court explicitly use that same phrase in both *Miller* and *Smith*,[412] but much of the Court's other discussion makes very little sense if the suspect did not provide the information as a function of her own volition. For example, even in the broadest articulation of the third-party doctrine's rationale in *Miller*, the Court presumes the decision to disclose was voluntary—even if it was not well-informed: There is no Fourth Amendment protection "even if the information is *revealed on the assumption* that it will be used only for a limited purpose."[413] It is plain to us that an unwise

---

[412] *Miller*, 425 U.S. at 442 ("All of the documents . . . contain only information *voluntarily conveyed* to the banks and exposed to their employees in the ordinary course of business.") (emphasis assed); *Smith*, 442 U.S. at 745 ("[P]etitioner *voluntarily conveyed* to [the phone company] information that it had facilities for recording and that it was free to record.") (emphasis added).

[413] *Miller*, 425 U.S. at 443 (emphasis added).

assumption presupposes an affirmative, voluntary choice.

Indeed, the Court's holding in *City of Charleston v. Ferguson* is probably best explained as a function of apprehension about whether the pregnant mother had been coerced into providing her incriminating urine to the third party.[414] Even in dissent in *Ferguson*, Justice Scalia never suggests that anything less than a voluntary conveyance would suffice: "[T]he Fourth Amendment does not protect a wrongdoer's misplaced belief that a person to whom he *voluntarily confides* his wrongdoing will not reveal it."[415]

It has only been quite recently, particularly in the context of CSLI, that judges and scholars have called attention to this oft-overlooked requirement. In their excellent and highly technically-sophisticated article on the third-party doctrine, Steven Bellovin, Matt Blaze, Susan Landau, and Stephanie Pell have recently recognized the importance of a voluntary conveyance:

> [T]he concept of voluntary conveyance is derived directly from *Miller* and *Smith*, specifically in the way these Courts described the nature of the disclosure of the information at issue between the customer and the third party (bank and telephone company, respectively). For a conveyance to be made voluntarily, it must be done with intent or by design, which, of course, presumes knowledge on the part of the consumer of that which is being conveyed. In both *Miller* and *Smith*, the courts' discussions included facts showing consumers knew that they were disclosing the information at issue to the respective third parties.[416]

In 2010, the Third Circuit explicitly held that CSLI is not voluntarily conveyed to a wireless provider:

> A cell phone customer has not "voluntarily" shared his location information with a cellular provider in any meaningful way. As the EFF notes, it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information. Therefore, "[w]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call

---

[414] *Ferguson*, 532 U.S. at 86 (reserving for remand the issue of whether the defendant had been coerced).

[415] *Ferguson*, 532 U.S. at 94 (Scalia, J., dissenting) (emphasis added).

[416] Bellovin, et al., *It's Too Complicated*, *supra* note 245, at 28.

> will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all."[417]

The Third Circuit reaffirmed that holding in July 2017.[418] This latter opinion explicitly noted that technological advancements are making CSLI ever-more precise—and ever-less voluntarily conveyed:

> We do note some aspects of the testimony adduced at trial that suggest that the line between GPS tracking and CSLI records is blurring. . . . The government's expert explained that CSLI is no longer only generated at the beginning and end of each call, but at every point at which an individual moves closer to a different cell tower. . . . Finally, the expert noted that CSLI records are generated far more frequently than they used to be, including when an individual sends text messages or uses certain applications.[419]

The Fourth,[420] Fifth,[421] Sixth (in *Carpenter*),[422] and Eleventh[423] Circuits have held that CSLI is voluntarily conveyed. The opinions with the most substantial analysis of the voluntary conveyance issue are the Fifth and Eleventh Circuit opinions. The Fifth Circuit argued that cell phone numbers and CSLI are indistinguishable because the cell phone user knows both are conveyed to her wireless provider in order to complete the call:

> The contact's telephone number is necessary for the service provider to connect the call; the user is aware of this fact; therefore, he is aware that he is conveying that information to the service provider and voluntarily does so when he makes the call. A similar analysis for cell site information leads to the conclusion that a user voluntarily conveys such information when he places a call, even

---

417 *In re Application (Third Circuit)*, 620 F.3d at 317–18.

418 *See Stimler*, 864 F.3d at 264 ("Thus, the rejection of the third-party doctrine was necessary to the holding of *In re Application*. . . . Accordingly, we continue to adhere to our view, espoused in *In re Application*, that the third-party doctrine does not apply because cell phone users do not voluntarily disclose CSLI to their service providers simply by signing a service contract").

419 *Id.* at 266 n.40. *See also* Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. L. REV 139, 161 (2016) (reporting that an "active cell phone 'registers' with cell towers by emitting a signal roughly every seven seconds").

420 *Graham*, 824 F.3d at 430.

421 *Historical Cell Site Data*, 724 F.3d at 612.

422 *Carpenter*, 819 F.3d at 888.

423 *Davis*, 785 F.3d at 519.

> though he does not directly inform his service provider of the location of the nearest cell phone tower. Because a cell phone user makes a choice to get a phone, to select a particular service provider, and to make a call, and because he knows that the call conveys cell site information, the provider retains this information, and the provider will turn it over to the police if they have a court order, he voluntarily conveys his cell site data each time he makes a call.[424]

The Eleventh Circuit's reasoning is slightly different. Rather than impute knowledge of CSLI to all cell phone users, the majority argued: "Just as in *Smith*, users could not complete their calls without *necessarily* exposing this information to the equipment of third-party service providers."[425] As Professor Bellovin and his coauthors note, however, the Eleventh Circuit's reasoning "appears to conflate the concept of information that is 'necessarily' conveyed with the concept of a knowing, voluntary conveyance."[426]

Judge Beverly Martin, dissenting in the Eleventh Circuit's CSLI opinion, draws exactly this distinction between the necessary and the voluntary:

> The *Smith* Court also emphasized that the numbers a person dials appear on the person's telephone bill and referenced the pre-automation process that required the caller to recite phone numbers out loud to a phone operator in order to make a call. Thus, the Court concluded that "[t]elephone users . . . typically know that they must convey numerical information to the phone company." There is not the same sort of "knowing" disclosure of cell site location data to phone companies because there is no history of cellphone users having to affirmatively disclose their location to an operator in order to make a call.[427]

By far the most substantial discussion of what "voluntary conveyance" actually means comes in Judge James Wynn's dissenting opinion in the Fourth Circuit's CSLI decision. Judge Wynn examines the Supreme Court's third-party opinions—

---

[424] *Historical Cell Site Data*, 724 F.3d at 613–14.

[425] *Davis*, 785 F.3d at 512 n.12 (emphasis added).

[426] Bellovin et al., *It's Too Complicated*, *supra* note 245, at 30.

[427] *Davis*, 785 F.3d at 534–35 (Martin, J., dissenting) (*quoting Smith*, 442 U.S. at 743) (citation omitted).

including the confidential informant decisions[428]—and concludes that a voluntary conveyance has two components.

The first component is knowledge: "[T]he defendant knew he was communicating particular information."[429] In *Miller*, the defendant presumably "knew how much money he was depositing"; in *Smith*, the defendant "knew the numbers he was dialing"; and the defendants in the confidential informant cases "knew about the misconduct they verbally described to another."[430]

The second component is an affirmative act: "[T]he defendant had acted in some way to submit the particular information he knew," and "there was an action—depositing, dialing, speaking—corresponding to each piece of submitted information."[431] Judge Wynn found it critical that in cases where third parties compile information into business records—like financial data in *Miller* and phone numbers in *Smith*—"there was presumptively a discrete action behind each piece of data."[432] We generally agree with Judge Wynn's reading of the Court's precedents and seek to explore the conceptual underpinnings of these two components further.

2. A Middle Ground: Most CSLI Is Involuntarily Conveyed

At one end of the spectrum is the information at issue in *Miller* and *Smith*, in which the defendant both knew the information being conveyed and took some affirmative act to affect the conveyance. At the other end of the spectrum is coercion—which we read *Ferguson* to be primarily concerned with—where a defendant divulges information due to pressure, force, intimidation, or a threat.[433]

To be sure, in a purely binary construction, CSLI would fall closer to the former. Put another way, we don't believe that CSLI is typically coerced from anyone—at least absent the government's use of a stingray device.[434] But we think the concept of voluntary

---

428 *See Lewis*, 385 U.S. at 206; *Hoffa*, 385 U.S. at 293; *White*, 401 U.S. at 745.

429 *Graham*, 824 F.3d at 443 (Wynn, J., dissenting).

430 *Id.*

431 *Id.*

432 *Id.*

433 *See Coerce*, AMERICAN HERITAGE DICTIONARY, https://ahdictionary.com/word/search.html?q=coerce.

434 "Stingray" is a colloquial name for "cell site simulators," devices that mimic cell phone towers to obtain location information from suspects' cell phones. *See generally* ADAM BATES, STINGRAY: A NEW FRONTIER IN POLICE SURVEILLANCE (Cato Institute Policy Analysis No. 809 2017) (for further discussion of police stingray

conveyance is more appropriately constructed as having a middle ground between the voluntary and the coerced. If we take "voluntary" to be something done *with* a person's will[435] and "coerce" to be something done *against* someone's will,[436] then the middle ground is something done *without* someone's will. This third concept is how many dictionaries define "involuntary."[437]

So is CSLI voluntarily or involuntarily conveyed? The overwhelming majority of CSLI seems to us to be involuntarily conveyed. The Third Circuit recently recognized this: "CSLI is no longer only generated at the beginning and end of each call, but at every point at which an individual moves closer to a different cell tower . . . [and] CSLI records are generated far more frequently than they used to be, including when an individual sends text messages or uses certain applications."[438] At most, people voluntarily convey information to their wireless providers when they affirmatively engage their wireless provider's services—by making a call or sending a text message—but the same cannot be true of CSLI logged when someone *receives* calls, texts, an email application engages with a mail server in the background, and when someone paces while talking on the phone.

And it doesn't seem appropriate to impute volition as exclusively a function of using a cell phone, which is what the Fifth Circuit held. The Court has repeatedly held that use of a service does not revoke Fourth Amendment protection for all information the service provider might obtain.[439] Taking the Fifth Circuit's reasoning to its logical extension, even the contents of communications would be unprotected because people agree to convey information to their provider when they use a phone.

The most difficulty we have with Judge Wynn's two-factor formulation is the issue of knowledge. For one thing, it seems odd that Fourth Amendment protection might rise or fall, on a case-

---

surveillance).

435 *See Voluntary*, AMERICAN HERITAGE DICTIONARY, https://ahdictionary.com/word/search.html?q=voluntary.

436 *Coerce*, *supra* note 434.

437 *See, e.g.*, *Involuntary*, OXFORD DICTIONARY, https://en.oxforddictionaries.com/definition/involuntary ("Done without will or conscious control. . . . Done against someone's will; compulsory."); *Involuntary*, AMERICAN HERITAGE DICTIONARY, https://ahdictionary.com/word/search.html?q=involuntary ("1. Acting or done without or against one's will . . . 2. Not subject to control of the volition.").

438 *Stimler*, 864 F.3d at 266 n.40.

439 *See, e.g.*, *Katz*, 389 U.S. at 347 (for a landmark Fourth Amendment decision).

by-case basis, with how familiar any one defendant is with how cell phones work. For another thing, the level of specificity with which you characterize the information at issue will often be dispositive: We think it safe to assume that most or all defendants are aware their cell phone must connect to a cell tower to provide wireless service, and it's no leap to stipulate that defendants are aware wireless providers know where their own towers are located. But on the other hand, it seems unreasonable to believe any defendant has a comprehensive understanding of where every cell tower is located, and thus no defendant truly knows (or has control over) which cell tower she is connected to at any one time. We think this demonstrates that the issue of knowledge about CSLI is a particularly difficult one that courts might best avoid.

In sum, we believe that, at most, a defendant voluntarily conveys CSLI and other routing information when she affirmatively engages a wireless provider's services. But the vast majority of modern CSLI is involuntarily conveyed, and compelling involuntarily conveyed information should be considered an unreasonable Fourth Amendment search.

B. Participants Versus Intermediaries

We now turn away from issues about metadata—namely, whether CSLI is voluntarily conveyed or not—and turn to issues about content—namely, why the Fourth Amendment protects some, but not all, content disclosed to third parties.

As much of the foregoing details, under the third-party doctrine, phone conversations and the body of emails are protected, while the content of communications with a bank is unprotected. What accounts for this difference? There is a fundamental tension inherent in the Court's third-party doctrine, chiefly between *Miller* and *Katz*. In both cases, a suspect disclosed incriminating information to a third party. In *Miller*, the contents of those communications were "negotiable instruments" that were "to be used in commercial transactions."[440] In *Katz*, the contents of those communications came in the form of an incriminating telephone conversation.[441]

Other scholars have noted this tension. Professor Henderson has expressly recognized, "the Supreme Court has never explained when information voluntarily conveyed to a third party 'counts'

---

[440] *Miller*, 425 U.S. at 442.
[441] *Katz*, 389 U.S. at 349.

(i.e., one retains no [reasonable expectation of privacy], as in *Smith* and *Miller*) and when it does not (i.e., one retains a [reasonable expectation of privacy], as in *Katz*)."[442] Professor Matthew J. Tokson has observed that "it remains difficult to predict whether the content/noncontent distinction will remain the central determinant of constitutional protection for email and website communications."[443] Professor Bellovin and his coauthors incisively ask:

> If constitutional protections for communications content in the possession of third party providers do not, in all circumstances, turn upon the content status of the communications data in question, what might that suggest about the analysis of the constitutional status of . . . data that cannot be easily classified as either content or non-content?[444]

And over a decade ago, Professor Peter Swire highlighted that technological change, *Miller*, and the SCA had eroded *Katz*'s holding:

> Once telephone calls are routinely stored, *Katz* and *Berger* may be dead on their own facts. Under current doctrine, individuals have a "reasonable expectation of privacy" in the context of phone calls but not in stored records. The Supreme Court has offered no reason why stored records of telephone calls deserve constitutional protection while stored records of voice mail, e-mail, financial records, personal diaries, and locational information do not. . . . Faced with these facts, courts very possibly would decide that there is no "reasonable expectation of privacy" outside of the home, and overrule *Katz* and *Berger* explicitly.[445]

It is easy to dismiss the results of *Katz* and *Miller* as purely a function of personal communications and business records, but it is considerably more difficult to categorically distinguish between them. And even if it was easy to draw a line between them, it's not clear it would matter—the Court's confidential-informant cases

---

[442] Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 527–28 (2005).

[443] Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50(6) WM. & MARY L. REV. 2105, 2117 (2009).

[444] Bellovin et al., *It's Too Complicated*, *supra* note 245, at 23.

[445] Peter Swire, Katz *Is Dead. Long Live* Katz, 102 MICH. L. REV. 904, 913 (2004).

suggest that unprotected information is not limited to business records.

The Sixth Circuit in *Warshak* grappled with distinguishing between *Katz* and *Miller*, and we use their analysis as a jumping-off point. Recall that the *Warshak* court found *Miller* distinguishable in two ways. First, the content of communications disclosed to a third party in *Miller* were "simple business records," whereas Warshak's emails included a "potentially unlimited variety of confidential communications."[446] Second, the content of communications disclosed to a third party in *Miller* were conveyed "so that the bank could put the information to use in the ordinary course of business."[447] Warshak's emails, however, were disclosed to his service provider only because the provider "was an *intermediary*, not the intended recipient."[448]

The first distinguishing factor—in which the *Warshak* court suggests that "one kind of content is more confidential and sensitive than another"[449]—has difficulty accounting for the Supreme Court's confidential-informant cases. In *On Lee*, *Lewis*, *Hoffa*, and *White*, the Court seems to reject the idea that the Fourth Amendment analysis of the recorded conversations required any evaluation of how sensitive or confidential the discussions were.[450]

The second distinguishing factor, however, does provide for the different outcomes in the informant cases and *Katz*: Warshak's service provider was a mere intermediary, a bailee.[451] We think both the confidential-informant cases and the business-record cases can be distinguished from *Katz* and *Warshak* if we consider whether the disclosing party was a *participant* in a communication

---

446 *Warshak*, 631 F.3d at 288 (citing *Miller*, 425 U.S. at 443) (internal quotation marks omitted).

447 *Id.* (quoting *Miller*, 425 U.S. at 443) (internal quotation marks omitted).

448 *Id.*

449 Bellovin et al., *It's Too Complicated*, *supra* note 245, at 24.

450 *See On Lee*, 343 U.S. at 756 ("Exclusion would have to be based on a policy which placed the penalization of Chin Poy's breach of confidence above ordinary canons of relevancy."); *Lewis*, 385 U.S. at 210 ("Such a rule would, for example, severely hamper the Government in ferreting out those organized criminal activities that are characterized by covert dealings . . . "); *Hoffa*, *385* U.S. at 302 ("Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."); *White*, 401 U.S. at 749 ("*Hoffa* . . . held that however strongly a defendant may trust an apparent colleague, his expectations in this respect are not protected by the Fourth Amendment when it turns out that the colleague is a government agent . . . ").

451 *See* section III.B, *supra* (for further discussion on point).

or whether the disclosing party was an *intermediary* in a communication. Most importantly, participants can consent to disclosure, but intermediaries cannot.

In the confidential-informant cases, the defendant and the informant were participants in a conversation, and the informant provided consent to disclose the contents of that conversation. In *Miller*, the defendant and the bank were participants in a conversation about banking services, and the bank provided consent to disclose the contents of that conversation.

Contrast those cases with the Postal Service. The routing information on the outside of the envelope is a conversation with the mail carrier: "Please deliver this letter to this address." But the mail carrier is an intermediary—and not a participant—in the communication inside the envelope. Thus the mail carrier can consent to disclose what is on the outside of the envelope (when she is a participant) but cannot consent to disclose what is inside the envelope (when she is an intermediary).

This is exactly what we see in *Smith*, *Katz*, *Berger*, and *Warshak*. In *Smith*, the defendant and the operator were participants in a conversation about connecting a telephone call, and the operator provided consent to disclose the contents of that particular conversation.[452] Critically, once the call was connected, the operator ceased to be a participant in the conversation and instead became an intermediary. This latter conversation between the defendant and a co-conspirator—as in *Katz* and *Berger*—remained protected because no participant in the conversation consented to disclosure. So too with *Warshak*: The body of emails was protected because neither the sender nor receiver—the participants in the conversation—consented to disclosure; the ISP was a mere intermediary to that conversation, and thus the ISP lacked the authority to consent to disclosure.[453]

---

[452] To be clear, we know that *Smith* did not actually entail a literal conversation with a live operator. As the Court put it: "The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber. . . . We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate." *Smith*, 442 U.S. at 744–45.

[453] Other courts and commentators have used a similar method of analysis. For example, the Congressional Research Service has observed:

> Another dividing line between protected and unprotected information pertains to the identity of the service provider in the chain of communication. If the provider is seen as a party to the transaction and is a *recipient* of the information, the records are generally considered "business records" of that company and subject to the third-

The traditional construction of the third-party doctrine are dual inquiries into the difference between content (sometimes protected) and metadata (generally unprotected) and the difference between personal communications (generally protected) and business records (generally unprotected). We believe a more accurate and coherent understanding of the third-party is an inquiry into the status of the third-party possessing the incriminating information. We read the Court's cases to mean that it is permissible for a participant to disclose information to the government and that it is impermissible for an intermediary to disclose information to the government.

In sum, we interpret the Court's third-party standard as having two components. First, all information must be voluntarily conveyed to a third party before it loses Fourth Amendment protection. Second, only third-party *participants* have the authority to consent to disclosure; mere *intermediaries* do not.

C. Resolving Carpenter and Issues for Further Discussion

Some are hopeful that the Court will seize the opportunity presented by *Carpenter* to significantly limit the third-party doctrine.[454] While we agree, as a normative matter, that a rejection of the third-party doctrine's applicability in the digital age is desirable,[455] a more wide-ranging rationale is likely to raise a

---

> party doctrine. This rationale is similar to that applied in the undercover informant cases. Although the information provided to an informant constitutes the content of the communication, it is not protected because it was spoken directly to the agent—in other words, the agent was the *recipient* of that information. Alternatively, where the company merely acts as a *conduit* or *intermediary* and "passively convey[s]" that information to an end-user, the material is generally not subject to the third-party doctrine.

RICHARD M. THOMPSON II, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE 13 (Congressional Research Service Report No. 7-5700 2014) (quoting *Forrester*, 512 F.3d at 510).

454 *See, e.g.*, Henderson, *The Best Way Forward*, *supra* note 9, at 27 ("I would personally be comfortable with a warrant requirement vaguely applying to 'longer term' CSLI acquisition, recognizing that 127 days is 'longer term.' Anything more precise—establishing a particular duration threshold—seems premature and inconsistent with the Court's recent more cautious approach.").

455 An intriguing possibility for reconsidering the third-party doctrine in the digital age would explicitly apply the "might actually" test from *Bond* to information shared by third parties. We think it's clear that people's expectations about how data shared with third parties today is very different from expectations at the time of Miller and Smith. Namely, third parties often exclusively use digital data after its been anonymized and aggregated; e.g., with CSLI, the primary benefit of collecting this information for service providers is

number of difficult line-drawing issues, including how many days CSLI the government may request without a warrant,[456] and resolution of when a third-party service provider has authority to disclose its own business records.[457]

Whether the Court uses *Carpenter* as a vehicle for a more fundamental change to the third-party doctrine or not, troubling questions about the kinds of digital data and how much digital data law enforcement may access without a warrant will continue to arise in the lower courts and appear in future certiorari petitions. Irrespective of how and whether the Court definitively alters the third-party doctrine calculus in *Carpenter*, the nature of a common law judicial system makes it inevitable that courts will continue to struggle with how to apply the Fourth Amendment to different types of data. A staggering amount of digital information is unprotected under the current third-party doctrine—regardless of how the doctrine's distinctions are framed.[458] A brief recitation of issues for future discussion and resolution follows below.

First, whether the Fourth Amendment protects Uniform Resource Locators (URLs) is extremely uncertain. URLs are difficult to categorize under existing doctrine because they are sometimes metadata, sometimes content, and, most often, both partially metadata and partially content.[459] The Third Circuit

---

that it provides the ability to analyze the extent of the company's coverage area. This, to us, seems very different from physically handing a deposit slip to a teller and actually telling an operator the number you wish to dial.

[456] *See, e.g.*, Henderson, *The Best Way Forward*, *supra* note 9, at 27–28.

[457] *Compare id.* at 32 ("So, there is a critical difference between my mother holding 'third party information' in my letter—over the disclosure of which she has an underlying autonomy and dignitary interest, a freedom to speak her mind—and a company like our imagined [wireless service provider] holding customer information."), *with* Orin S. Kerr, *Third Party Rights and the Carpenter Cell-Site Case*, THE WASHINGTON POST (June 15, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/06/15/third-party-rights-and-the-carpenter-cell-site-case/ ("Imagine *Carpenter* holds that users have Fourth Amendment rights in cell-site records, and that a warrant is ordinarily required. Can a provider tell the government that as long as the government has a 2703(d) court order, as required by the statute, that it will voluntarily consent to hand over the records under the common authority doctrine?").

[458] By this we mean that it is irrelevant whether this data is analyzed under the participant/intermediary distinction or the traditional content/metadata and communications/records distinctions. All formulations yield troubling results.

[459] *See, e.g.*, Bellovin et al., *It's Too Complicated*, *supra* note 245, at 57; Orin S. Kerr, *Websurfing and the Wiretap Act*, THE WASHINGTON POST (June 4, 2015), https://www.washingtonpost.com/news/volokhconspiracy/wp/2015/06/04/websurfing-and-the-wiretap-act/; Orin S. Kerr, *Websurfing and the Wiretap Act, Part 2: The Third Circuit's Ruling*, THE WASHINGTON POST (Nov. 19, 2015), https://www.washingtonpost.com/news/volokhconspiracy/wp/2015/11/19/websurfing-

recently held, in a case about a violation of the Wiretap Act, that URLs can sometimes constitute content.[460] On the other hand, the Foreign Intelligence Surveillance Court of Review has suggested, in a case about the scope of the Pen Register Statute, that URLs might never qualify as content.[461] These were statutory cases, and what these courts' conclusions mean for a constitutional analysis is extremely difficult to know. If an ISP logs your URLs and we stipulate those URLs reveal at least some content, are those URLs business records unprotected by *Miller* or personal communications protected by *Katz*? As a number of jurists[462] have recognized—including Chief Justice Roberts in *Riley*[463]—URLs can reveal a historically unprecedented amount information about someone.[464]

Second, ambient sound capture and assistive technologies—such as the Amazon Echo, the Google Home, and the Apple

---

and-the-wiretap-act-part-2-the-third-circuits-ruling/.

460 *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125, 137 (3d Cir. 2015) ("In essence, addresses, phone numbers, and URLs may be dialing, routing, addressing, or signaling information, but only when they are performing such a function. If an address, phone number, or URL is instead part of the substantive information conveyed to the recipient, then by definition it is 'content'").

461 *In re: Certified Question of Law*, No. FISCR 16-01, at 12 n.6 (FISA Ct. filed April 14, 2016); *see also* Orin S. Kerr, *Relative vs. Absolute Approaches to the Content/Metadata Line*, LAWFARE (Aug. 25, 2016), https://www.lawfareblog.com/relative-vs-absolute-approaches-contentmetadata-line (quoting the same treatise that the Foreign Intelligence Surveillance Court of Review had quoted).

462 *See, e.g.*, *Davis*, 785 F.3d at 537 (Martin, J., dissenting).

> The majority offers no coherent definition of the terms "content" and "non-content," and I am hard-pressed to come up with one. For instance, would a person's Google search history be content or non-content information? Though a person's search terms may seem like "content," a search term exists in the web address generated by a search engine. And web addresses, like phone numbers, seem like quintessentially non-content information that merely direct a communication.

Id. (footnote omitted).

463 *See Riley*, 134 S. Ct. at 2490 ("An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.").

464 The federal government seems to recognize that URLs are a prime example of a blurred distinction between content and metadata. The Department of Justice advises U.S. Attorneys to refrain from using the Pen Register Statute to collect URLs without first consulting with the Computer Crime and Intellectual Property Section (CCIPS) at DOJ headquarters: "Because of privacy and other concerns relating to the use of pen register orders in this fashion, use of pen registers to collect all or part of a URL is prohibited without prior consultation with CCIPS." U.S. ATTORNEYS' MANUAL 9-7.500 (U.S. Dep't of Justice 2003).

HomePod—present another invasive cache of data retained by a third-party business. These devices can record an untold amount of information about the interior of a home—records that could be construed as third-party business records.[465] And this is no abstract concern: There has already been one widely-publicized case about law enforcement asking Amazon for data recorded by an Echo during the commission of a crime.[466]

Third, people now routinely share massive amounts of biometric data with third-party businesses. It is not difficult to conceive of law enforcement desiring information about a suspect's heart rate at the time the crime occurred, which could easily be captured by devices like the Apple Watch.[467] Would this biometric data be a business record? Like so much sensitive information we now routinely share with third-party businesses—which they retain for "a variety of legitimate business purposes"[468]—there's no clear answer.

Fourth, digital photo-storage services now routinely use machine-learning techniques to automatically scan and categorize users' photos. Users of Apple iCloud photo storage recently learned that the company was automatically grouping photographs of lingerie, bikinis, and bare skin together under a "brassiere" tag.[469] Is the machine-learning algorithm that automatically, silently, and comprehensively scans your photos a third-party witness that defeats an expectation of privacy? Is a company-retained record of your scanned photos subject to compulsion by a subpoena?

In short, Justice Sotomayor's words in *Jones* succinctly capture our concern underlying these issues: *Miller*'s "approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of

---

[465] *See* Bellovin et al., *It's Too Complicated*, *supra* note 245, at 72–3 (discussing the implications of such devices).

[466] *See* Gerald Sauer, *A Murder Case Tests Alexa's Devotion to Your Privacy*, WIRED (Feb. 28, 2017), https://www.wired.com/2017/02/murder-case-tests-alexas-devotion-privacy/; Brian Heater, *After Pushing Back, Amazon Hands Over Echo Data in Arkansas Murder Case*, TECHCRUNCH (Mar. 7, 2017), https://techcrunch.com/2017/03/07/amazon-echo-murder/ (for further discussion).

[467] A man in Connecticut was recently charged with his wife's murder based on data from her FitBit. *See* Harriet Alexander, *Man charged with wife's murder after her FitBit contradicts his timeline of events*, THE TELEGRAPH, Apr. 25, 2017, *available at* https://www.telegraph.co.uk/news/2017/04/25/man-charged-wifes-murder-fitbit-contradicts-timeline-events/.

[468] *Smith*, 442 U.S. at 743.

[469] Dami Lee, *Apple has been categorizing all your 'brassiere' photos for over a year now*, THE VERGE, Oct. 30, 2017, https://www.theverge.com/2017/10/30/16575600/apple-iphone-photos-brassiere-machine-learning.

carrying out mundane tasks."[470] These include, but are by no means not limited to, "disclos[ing] the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers."[471]

CONCLUSION

In *Carpenter v. United States*, the Supreme Court is poised to address how the Fourth Amendment's third-party doctrine applies in the digital age, and the Court's decision may have a profound effect on electronic surveillance law. Clarity is badly needed on the constitutionality of the Stored Communications Act and, more broadly, on the Fourth Amendment status of a historically unprecedented volume of digital data.

---

[470] *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring).
[471] *Id.*