



2019

Functional Equivalence and Residual Rights Post-*Carpenter*. Framing a Test Consistent with Precedent and Original Meaning


Laura K. Donohue

Georgetown University Law Center, lkdonohue@law.georgetown.edu

This paper can be downloaded free of charge from:
<https://scholarship.law.georgetown.edu/facpub/2376>
<https://ssrn.com/abstract=3830702>

Supreme Court Review, Vol. 2018, Pp. 347-410.

This open-access article is brought to you by the Georgetown Law Library. Posted with permission of the author.
Follow this and additional works at: <https://scholarship.law.georgetown.edu/facpub>

 Part of the [Constitutional Law Commons](#), [Criminal Law Commons](#), [Fourth Amendment Commons](#), and the [Supreme Court of the United States Commons](#)

FUNCTIONAL EQUIVALENCE AND
RESIDUAL RIGHTS POST-CARPENTER:
FRAMING A TEST CONSISTENT WITH
PRECEDENT AND ORIGINAL MEANING

I. INTRODUCTION

The evolution of Fourth Amendment doctrine over the past century bears a striking resemblance to Hamlet's descent into insanity. Step by step, faced by increasingly sophisticated technologies, the Court has crafted rules, exceptions, and exceptions to the exceptions, until we find ourselves in an incoherent world that bears little relationship to the original rights it encompasses.

The Founders introduced the Fourth Amendment to secure liberty.¹ The clause reinforced the right of the people, as sovereign, to determine the conditions under which the government could intrude

Laura K. Donohue is Professor of Law, Georgetown Law.

AUTHOR'S NOTE: Special thanks to Jeremy McCabe at the Georgetown Law Library for his assistance in cite checking, formatting the footnotes, and obtaining materials used in this article. Nadia Asanchev, George Farahat, Katrina Kleck, and Allen Tran further assisted with formatting and cite checking. I am indebted to Randy Barnett, Jennifer Daskal, John Facciola, Jennifer Granick, Bob Litt, Allegra McLeod, Michael Mosman, Abbe Smith, Lawrence Solum, Geoffrey Stone, and David Vladeck for their thoughtful critique.

¹ 1 Annals of Congress 443, 446, 449 (June 8, 1789).

in their lives.² The interests at stake went well beyond the physical world. As Justice Brandeis famously observed in his dissent in *Olmstead v United States*, the Framers “sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations.”³ Any intrusion had to be justified. For that, a general warrant would be insufficient. Even a particularized one had to meet the requirements in the second part of the clause: probable cause demonstrated to an independent magistrate, supported by oath or affirmation, and “particularly describing the places to be searched, and the persons or things to be seized.”⁴ Outside of these conditions, or a known felon in flight, the Fourth Amendment created an absolute bar.⁵ It was not, as the Court suggested in 1948 and repeated seventy years later in *Carpenter v United States*, an effort “to place obstacles in the way of a too permeating police surveillance.”⁶ It was government surveillance of the privacies of life itself that was forbidden, outside of constitutional strictures.⁷

For decades, the Court adopted a property-based approach, tying the doctrine to common-law trespass, which prioritized the question of whether a physical intrusion had occurred “on a constitutionally protected area.”⁸ When confronted with its first wiretapping case, the Court’s failure was not in recognizing that telephone wires lay outside the home, which they clearly do, but in failing to recognize that through wiretapping, the government gained access to the intimate details of the speakers’ lives—details ensconced in their persons, houses, papers, and effects.

² *Camara v Municipal Court of City and County of San Francisco*, 387 US 523, 528 (1967); *Boyd v United States*, 116 US 616, 630 (1886). See also Raymond Shih Ray Ku, *The Founders’ Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 Minn L Rev 1325, 1326 (2002).

³ *Olmstead v United States*, 277 US 438, 476 (1928) (Brandeis, J, dissenting).

⁴ US Const, Amend IV.

⁵ Laura K. Donohue, *The Original Fourth Amendment*, 83 U Chi L Rev 1181 (2016). See also *Carpenter v United States*, 138 S Ct 2206, 2243 (2018) (Thomas, J, dissenting).

⁶ *United States v Di Re*, 332 US 581, 595 (1948); *Carpenter*, 138 S Ct at 2214 (majority); *Camara*, 3887 US at 528, quoted in *Carpenter*, 138 S Ct at 2213.

⁷ See *Segura v United States*, 468 US 796, 810 (1984) (“But the home is sacred in Fourth Amendment terms not primarily because of the occupants’ possessory interests in the premises, but because of their privacy interests in the activities that take place within.”).

⁸ See *United States v Jones*, 565 US 400, 405, 406 n 3 (2012); *Carpenter*, 138 S Ct at 2213. See also *Kyllo v United States*, 533 US 27, 34–35 (2001); *Carpenter*, 138 S Ct at 2236 (Thomas, J, dissenting).

In 1967, *Katz v United States* did nothing to address this deficiency.⁹ Instead, it took the doctrine further from its original purpose, placing it in a make-believe land of relativistic determinations.¹⁰ If there is a silver lining to be taken from the Court's recent decision in *Carpenter*, it is that multiple Justices acknowledged the problems created by *Katz* and its progeny.¹¹ Justice Thomas launched a devastating attack on the earlier decision, stating, "The *Katz* test has no basis in the text or history of the Fourth Amendment."¹² His complaints are well-founded.

Not only is the test from Justice Harlan's concurrence in *Katz* inconsistent with the original meaning of the Fourth Amendment, but as a matter of constitutional pluralism, it has proven deeply problematic. If, as the Court stated in 2006, "the ultimate touchstone of the Fourth Amendment is 'reasonableness,'"¹³ then it falls to judges to make the call of what is "more" or "less" reasonable. This puts them squarely in the realm of policy-making, risking public confidence in the workings of the Court.¹⁴ In the decades that followed *Katz*, the Court repeatedly ignored societal standards, substituting its own judgment for that of elected representatives and narrowing protections afforded to the people.¹⁵ The

⁹ *Katz v United States*, 389 US 347 (1967).

¹⁰ See Randy E. Barnett and Evan D. Bernick, *The Letter and the Spirit: A Unified Theory of Originalism*, 107 Georgetown L J 1 (2018) (arguing that originalist constitutional construction should be informed by the original function or purpose of the relevant provision).

¹¹ See *Carpenter*, 138 S Ct at 2236 (Thomas, J, dissenting); id at 2261–65 (Gorsuch, J, dissenting). See also *Minnesota v Carter*, 525 US 83, 97 (1998) (Scalia, J, concurring).

¹² *Carpenter*, 138 S Ct at 2236 (Thomas, J, dissenting). See also id at 2238–45 (discussing many ways in which *Katz* departed from the original meaning of the Fourth Amendment).

¹³ *Brigham City v Stuart*, 547 US 398, 403 (2006).

¹⁴ See *Carpenter*, 138 S Ct. at 2236 (Thomas, J, dissenting) (arguing that *Katz* "invites courts to make judgments about policy, not law."); id at 2264 (the right to bring a claim does not "depend on whether a judge happens to agree that your subjective expectation to privacy is a 'reasonable' one."); id at 2265 (Gorsuch, J, dissenting) ("When judges abandon legal judgment for political will . . . [we] risk undermining public confidence in the courts themselves."); id ("Deciding what privacy interests *should* be recognized often calls for a pure policy choice . . . which calls for the exercise of raw political will belonging to legislatures, not the legal judgment proper to courts.").

¹⁵ In *California v Ciraola*, the Court held there is no "reasonable expectation of privacy" in an enclosed yard, as even fences "might not shield [marijuana plants] from the eyes of a citizen or a policeman perched on the top of a truck or a two-level bus," despite state laws making it illegal to ride on top of a truck, trespass on others' property, or climb fences without the owner's consent. See *California v Ciraolo*, 476 US 207, 209, 214 (1986); 1981 Cal Stat 3149, 3155, codified at Cal Veh Code § 21712 (adding Subsection (b), stating that "No person shall ride on any vehicle or upon any portion thereof not designed or intended for the use of passengers,"); 1982 Cal Stat 4709, codified at Cal Veh Code § 23116 (passed Sept 22,

result is a doctrine that is much maligned for logical fallacies, inconsistency, and unmanageability.¹⁶

Along the way, the judiciary carved out broad exceptions, foremost amongst which is the third-party doctrine. In *Katz*, Justice White presaged its evolution, arguing that knowingly exposing information to others implies an assumption of risk that the other party may later disgorge it.¹⁷ For him, the Fourth Amendment had nothing to say about unreliable associates. Drawing an analogy to informant doctrine,

1982, making it illegal for a minor to be in the back of a flatbed truck); 1961 Cal Stat 2919, codified at Cal Penal Code § 602.5 (unauthorized entry of property); 1981 Cal Stat 980, 988, codified at Cal Penal Code § 602 (trespass upon fenced, cultivated land). This last provision is reflected in numerous local ordinances. See, for example, Orange County, California, County Code § 3-8-24. In *United States v Dunn*, the Court determined that it was “reasonable” for a Drug Enforcement Agency agent to cross a perimeter fence, an interior fence, and a barbed wire fence, to peer inside a barn that was located on private property a half mile from any road, before crossing another barbed wire fence and a wooden fence to look inside a second structure. See *United States v Dunn*, 480 US 294, 297 (1987). The Court ignored state and federal judicial decisions that considered barns to be within the curtilage. See, for example, *Luman v State*, 629 P2d 1275, 1276 (Okla Crim App 1981); *United States v Berrong*, 712 F2d 1370, 1374 (11th Cir 1983); *Rosencranz v United States*, 356 F2d 310, 313 (1st Cir 1966); *Walker v United States*, 225 F3d 447; *United States v Swann*, 377 F Supp 1305, 1306 (Md 1974); *United States v King*, 305 F Supp 630, 634 (ND Miss 1969), and dozens of further cases cited in *Dunn*, 480 US at 308–9 (Brennan, J, dissenting). It also ignored state law making it illegal to trespass on private property if given notice. See Tex Penal Code Ann § 30.05 (1980). In *California v Greenwood*, the Court decided that it was not “reasonable” to consider garbage within the Fourth Amendment on the grounds that bags left out on the curb are “readily accessible to animals, children, scavengers, snoops, and other members of the public,” despite local ordinances making it illegal for anyone to go through peoples’ garbage. See *California v Greenwood*, 486 US 35 (1988); California, Laguna Beach, Municipal Code § 7.16.060(b).

¹⁶ *Carpenter*, 138 S Ct at 2244 (Thomas, J, dissenting). Scholars are scathing in their criticism. See, for example, Daniel J. Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security* (Yale, 2011); Amitai Etzioni, *A Cyber Age Privacy Doctrine: More Coherent, Less Subjective, and Operational*, 80 Brooklyn L Rev 1263 (2015); Steven M. Bellovin et al, *When Enough Is Enough: Location Tracking, Mosaic Theory, and Machine Learning*, 8 NYU J L & Liberty 556 (2014); David Gray and Danielle Citron, *The Right to Quantitative Privacy*, 98 Minn L Rev 62, 70 (2013); Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 Miss L J 1309 (2012); Andrew William Bagley, *Don’t Be Evil: The Fourth Amendment in the Age of Google, National Security, and Digital Papers and Effects*, 21 Albany L J Sci & Tech 153 (2011); Priscilla J. Smith et al, *When Machines Are Watching: How Warrantless Use of GPS Surveillance Technology Violates the Fourth Amendment Right Against Unreasonable Searches*, 121 Yale L J Online 177, 177 (2011); John J. Brogan, *Facing the Music: The Dubious Constitutionality of Facial Recognition*, 25 Hastings Comm & Ent L J 65, 73 (2002); Ku, 86 Minn L Rev at 1327 (cited in note 2); Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through Kyllo’s Rules Governing Technological Surveillance*, 86 Minn L Rev 1393 (2002); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S Cal L Rev 1083 (2002).

¹⁷ *Katz*, 389 US at 363 n ** (1967) (White, J, concurring) (“When one man speaks to another he takes all the risks ordinarily inherent in so doing, including the risk that the man to whom he speaks will make public what he has heard. The Fourth Amendment does not protect against unreliable . . . associates.”).

the Court subsequently decided that anything you tell anyone else—even if necessary for the day-to-day running of a household or living in the modern world—does not fall within the protections of the Fourth Amendment. *Miller v United States* and *Smith v Maryland* dealt, respectively, with banking and telephone records.¹⁸ But the rule quickly expanded to encapsulate almost any record entrusted to others.

Intellectually diverse scholars have roundly denounced third-party doctrine.¹⁹ Professor Wayne LaFave declared *Miller* “dead wrong,” “a mockery of the Fourth Amendment.”²⁰ Professor Daniel Solove considered it “one of the most serious threats to privacy in the digital age.”²¹ Professor Randy Barnett has called for “[b]oth the third-party doctrine of *Smith* and the ‘reasonable expectation of privacy’ approach of *Katz* . . . to be adapted to modern circumstances.”²² As Justice Gorsuch observed in *Carpenter*, the exception eviscerated Fourth Amendment doctrine, leaving it unprepared for the modern age: “Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers.”²³ It is ludicrous to think that these documents are not private.

Now we have, with *Carpenter*, an exception to the exception, saying that location data are, well, special and that other things might be special too, but we can’t say right now just what falls into that camp.²⁴ This article observes that while the Court had little choice but to grant certiorari and to find location data protected under the Fourth

¹⁸ *Smith v Maryland*, 442 US 735, 745 (1979); *United States v Miller*, 425 US 435, 443 (1976).

¹⁹ See Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich L Rev 561, 563 n 5 (2009) (observing that “[a] list of every article or book that has criticized the doctrine would make . . . the world’s longest law review footnote”).

²⁰ Wayne R. LaFave, 1 *Search and Seizure: A Treatise on the Fourth Amendment* § 2.7(c) at 747 (Thomson West, 4th ed 2004), cited and quoted in Kerr, 107 Mich L Rev at 564 (cited in note 19).

²¹ Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr’s Misguided Call for Judicial Deference*, 74 Fordham L Rev 747, 753 (2005), cited and quoted in Kerr, 107 Mich L Rev at 564 n 10 (cited in note 19). See also *Carpenter*, 138 S Ct at 2264 (Gorsuch, J, dissenting).

²² Randy E. Barnett, *Why the NSA Data Seizures Are Unconstitutional*, 38 Harv J L & Pub Pol 3, 16 (2015).

²³ *Carpenter*, 138 S Ct at 2262 (Gorsuch, J, dissenting) (writing that *Miller* and *Smith* proved “[a] doubtful application of *Katz* that lets the government search almost whatever it wants whenever it wants.”).

²⁴ See id at 2217, 2223 (majority).

Amendment, the reasoning it adopted exacerbated doctrinal weaknesses and created profound challenges for judiciary going forward.

The *Carpenter* Court held that warrantless access to seven or more days of cell site location information (CSLI) constitutes a violation of the reasonable expectation of privacy that individuals have in the whole of their physical movements.²⁵ But the grounds on which the Court drew a line—the “deeply revealing nature of [CSLI], its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection”²⁶—are not unique to location data. They characterize all sorts of digital records—including those at issue in *Miller* and *Smith*, belying the majority’s claim that the decision leaves third-party doctrine intact. Instead of avoiding *Katz*’s pitfalls, the Court emphasized voluntary assumption of risk, doubling down on the subjective nature of judicial interpretation. Even as it declared the warrantless search of CSLI unreasonable, it introduced myriad questions that will push the lower courts into uncharted territory. Without clear direction, the decision is likely to lead to further chaos, fragmentation in the circuits, and reversals in the courts of appeals—far from the predictability and certainty essential to rule of law.

To mitigate the risk and take account of the significant challenges ahead, this article proposes that, going forward, courts eschew voluntary assumption of risk. An outgrowth of open space and informant doctrines, the approach imported analogical fallacies into the Court’s jurisprudence and turned a blind eye to the implications of new technologies. The perfunctory application of voluntariness to third-party records further eviscerated the constitutional protections extended to private and commercial papers at the founding. The lack of clarity in *Carpenter* between what can be understood as “device-use compulsion” and “record-creation compulsion,” and the insertion of the judiciary into that determination, forces judges into a policy-making role. The Court’s emphasis on novel technologies will further confound efforts to adjudicate Fourth Amendment claims in a consistent manner.

To address problems created by *Carpenter*, this article advocates a property-based approach in which the Court extends the rule of functional equivalence, which characterizes home and border searches,

²⁵ Id at 2219–20, 2223.

²⁶ Id at 2223.

to digital papers. The multifactor test employed in *Carpenter*—the volume of information, its revealing nature, its retroactivity, its near perfect recall, the length of time it was collected, and its precision—underscores the extent to which information reveals the “privacies of life.” While such factors may explain why data are considered within the construct of “papers,” they are neither necessary nor sufficient. Just as the Court has been clear that technology conveying information about the interior of a home triggers Fourth Amendment protections regardless of whether it exposes intimate details, so, too, should the search of digital papers be sufficient to find them constitutionally protected—regardless of the level of intimacy revealed.

In ascertaining who owns digital documents and records, the Court can employ a *but for* analysis, asking whether the material would exist but for the right-holder’s actions. In the context of CSLI, the right-holder buys the phone, charges it, turns it on, and decides when and where to carry it. It is up to the right-holder to decide with whom the resulting location information is shared. Indeed, an individual could not even contract to provide the information to others absent the original right. Simultaneously, the owner has a separate claim on the third party to perform a particular service (in exchange for money), which only exists within the contractual relationship.

To determine whether, by providing access to information, the right-holders divest themselves of their ownership interest in the data, as Justice Gorsuch recognized in *Carpenter*, the law of bailment and positive law have the potential to play a crucial role.²⁷ English common law has long recognized that possession is insufficient to extinguish a property owner’s residual rights.²⁸ A bailor and bailee both hold rights in the same property.²⁹ CSLI closely mirrors a

²⁷ *Carpenter*, 138 S Ct at 2268 (Gorsuch, J, dissenting).

²⁸ See Frederick Pollock and Frederic William Maitland, 2 *History of English Law Before the Time of Edward I* 169 (Cambridge, 2d ed 1898).

²⁹ See, for example, Oliver Wendell Holmes Jr., *The Bailee at Common Law*, in *The Common Law* 164 (Little, Brown, 1881); Joseph H. Beale Jr., *The Carrier’s Liability*, 11 Harv L Rev 158 (1887); Thomas Atkins Street, 2 *The Early Law of Bailment*, in 2 *Foundations of Legal Liability* 251 (Edward Thompson, 1906); Percy Bordwell, *Property in Chattels II: Property in the Bailor*, 29 Harv L Rev 501 (1916); Percy Bordwell, *Property in Chattels III: Property in the Bailee*, 29 Harv L Rev 731 (1916); Eric G. M. Fletcher, *The Carrier’s Liability* (Stevens & Sons, 1932); W. S. Holdsworth, 3 *A History of English Law* 336 (Methuen, 3d ed 1923); Theodore F. T. Plucknett, *A Concise History of the Common Law* 451–52 (Little, Brown, 5th ed 1956). See also G. W. Paton, *Bailment in the Common Law* 48 (Stevens & Sons, 1952); C. H. S. Fifoot, *History and Sources of the Common Law: Tort and Contract* 157–66 (Stevens & Sons, 1949); Samuel Stoljar, *The Early History of Bailment*, 1 Am J Legal Hist 5 (1957).

bailment in *locatio rei*, in which a considerable amount of control is provided to the possessor, without altering the right-holder's power—in this case, over his or her location information. Positive law, in turn, may prove probative in regard to the existence of a property right: where federal or state law has *acknowledged a property right* and placed a correlative *duty of noninterference* on others, government intrusions may constitute a search or seizure within the meaning of the Fourth Amendment. The approach advocated has the advantage of clarity, adaptation to the modern world, and the restoration of core Fourth Amendment rights protected at the founding.

II. CARPENTER: A CASE THAT HAD TO HAPPEN

In 2018, the Court had little choice but to confront the issues raised in *Carpenter*. Use of CSLI had become widespread. Enormously powerful, it allowed law enforcement the ability to find suspects, to place them near crimes, to verify (or undermine) alibis, to discover what people had done (and with whom), and to discover behavioral patterns. Simultaneously, it did not fit well within either statutory law or Fourth Amendment doctrine—a situation exacerbated by the Court's decisions in *Riley v California* and *United States v Jones*.³⁰ Faced with a jurisprudence that denied constitutional protections, defied common sense, and sent contradictory messages, lower courts struggled with how to apply *Katz*. Central to the debate was whether telephone users voluntarily divulged location information to others—a question rooted in informant doctrine and bedeviled by the contemporary dependence on mobile devices.

A. STATUTORY FRAMING

As CSLI came of age, it was not immediately apparent whether statutory provisions authorized law enforcement to collect it. The government began by arguing that it fell within the criminal pen register and trap and trace provisions (PRTT).³¹ But virtually every court to confront the question rejected this approach, not least because the Communications Assistance for Law Enforcement Act

³⁰ *Riley v California*, 134 S Ct 2473 (2014), taken in conjunction with *United States v Wurie*, 728 F3d 1 (2013), cert granted 134 S Ct 999 (2014); *United States v Jones*, 565 US 400 (2012).

³¹ 18 USC §§ 3121–27.

(CALEA) expressly forbade the use of pen register statutes to collect location data.³²

In 1994, Congress had passed CALEA to require service providers to be able to provide law enforcement with information for which it had legal authorization.³³ The hearings aired significant worry about the government's potential use of service providers' records to track individuals. During his testimony, Federal Bureau of Investigation (FBI) Director Louis Freeh acknowledged this concern, declared that the government had no intention of collecting location data, and offered to make it clear in the statutory language that the caller's location would be excluded.³⁴ Congress adopted Freeh's clarification almost verbatim.³⁵ But the statute, which stated that information may not be collected "solely pursuant" to PRTT provisions, appeared to leave open the possibility of a separate authorization. The govern-

³² Communications Assistance for Law Enforcement Act (CALEA), Pub L No 103-414 § 103(a)(2)(b), 108 Stat 4279, 4280-81 (1994). See, for example, *In re Applications of the United States for Orders Pursuant to Title 18, United States Code, Section 2703(d)*, 509 F Supp 2d 64 (D Mass 2007); *In re Application of United States for an Order Authorizing Disclosure of Location Based Services*, 2007 WL 2086663 (SD Tex); *In re Application of the United States for an Order Authorizing the Disclosure of Prospective Cell Site Information*, 412 F Supp 2d 947 (ED Wis 2006); *In re Application of the United States for an Order Authorizing Installation and Use of a Pen Register*, 415 F Supp 2d 211 (WDNY 2006); *In re Application of United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone*, 2006 WL 468300 (SDNY); *In re United States*, 2006 WL 1876847 (ND Ind); *In re United States*, 441 F Supp 2d 816 (SD Tex 2006); *In re Authorizing the Use of a Pen Register*, 384 F Supp 2d 562 (EDNY 2005); *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F Supp 2d 747 (SD Tex 2005); *In re Application of the United States for an Order*, 396 F Supp 2d 294 (EDNY 2005).

³³ Within four years, service providers had to be able to provide law enforcement agencies with "access call-identifying information that is reasonably available to the carrier—(A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and (B) in a manner that allows it to be associated with the communication to which it pertains, except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in [18 USC § 3127])." 47 USC § 1002(a)(2). See 47 USC § 1001 note.

³⁴ See *Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375 before the Subcommittee on Technology and the Law of the Senate Judiciary Committee and the Subcommittee on Civil and Constitutional Rights of the House Judiciary Committee*, 103d Cong, 2d Sess 29-34 (1994) (Statement of FBI Director Freeh).

³⁵ 47 USC § 1002(a)(2). See also *Communications Assistance for Law Enforcement Act*, HR Rep No 103-827, Part I, 103d Cong, 2d Sess 17 (1994), reprinted in 1994 USCCAN 3489, 3497 (The bill "[e]xpressly provides that the authority for pen registers and trap and trace devices cannot be used to obtain tracking and location information, other than that which can be determined from the phone number.").

ment quickly turned to an alternative anchor: the Stored Communications Act (SCA).³⁶

The key question under the SCA was whether the collection of CSLI turned a phone into a “tracking device” or whether what was being sought was merely a “record.”³⁷ If the phone was understood as a tracking device, the statute exempted the data from disclosure under 18 USC § 2703.³⁸ Courts thus paid careful attention to how accurately the technology conveyed location.³⁹

For real-time or prospective information, courts considered the phone to be acting as a tracking device and thus outside the SCA, with the result that probable cause and a warrant would be required to obtain the data.⁴⁰ In contrast, numerous courts considered *historic*

³⁶ Stored Communications Act (SCA), 18 USC § 2701 et seq. See, for example, *In re Application of the United States for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace*, 405 F Supp 2d 435, 436 (EDNY 2005). Some courts rejected the argument that the government could apply under different statutory provisions, saying that CALEA sought to foreclose other options. See *In re Application of the United States for an Order Authorizing the Release of Prospective Cell Site Information*, 407 F Supp 2d 134 (DDC 2006).

³⁷ See, for example, *People v Hall*, 823 NYS 2d 334 (NY 2006); *In re Application of United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone*, 460 F Supp 2d 448 (SDNY 2006); *In re Application for an Order Authorizing the Extension and Use of a Pen Register Device*, 2007 WL 397129 (ED Cal); *In re Application of United States for an Order Relating to Target Phone 2*, 733 F Supp 2d 939, 942–43 (ND Ill 2009).

³⁸ The statute defined “electronic communication” as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photooptical system that affects interstate or foreign commerce, but does not include . . . (C) any communication from a tracking device (as defined in section 3117 of this title).” 18 USC § 2510(12) (emphasis added). That section defined “tracking device” as “an electronic or mechanical device which permits the tracking of the movement of a person or object.” 18 USC § 3117. If a mobile phone is a tracking device, then the electronic signals from it do not count as “electronic communications” for SCA purposes—so 18 USC § 2703(d) is inapplicable.

³⁹ See, for example, *In re Application of the United States for an Order*, 396 F Supp 2d at 310; *In re Application of the United States for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace*, 405 F Supp 2d at 438; *In re Application of the United States for an Order*, 411 F Supp 2d 678, 679–80 (WD La 2006); *In re Application of the United States for Orders Authorizing the Installation and Use of Pen Registers and Caller Identification Devices on Telephone Numbers*, 416 F Supp 2d 390, 396 (D Md 2006); *In re United States for an Order*, 433 F Supp 2d 804, 806 (SD Tex 2006); *United States v Bermudez*, 2006 WL 3197181 (SD Ind).

⁴⁰ See, for example, *In re Application of the United States for an Order Authorizing Disclosure of Location Information of a Specified Wireless Telephone*, 849 F Supp 2d 526, 575 (D Md 2011); *In re Application of United States for an Order*, 2009 WL 1530195, *3–4 (EDNY); *In re United States*, 416 F Supp 2d at 397; *Bermudez*, 2006 WL 3197181, *7 (noting that 18 USC § 2703 does not allow real-time tracking); *In re United States*, 441 F Supp 2d at 828; *In re Application of the United States for an Order Authorizing Disclosure of Prospective Cell Site Information*, 2006 WL 2871743, *6 (ED Wis) (18 USC § 2703 is only retrospective); *United States v*

CSLI to be a “record” under 18 USC § 2703.⁴¹ Here, the government only had to meet the requirements in § 2703(d). The government argued that because the information was derived from wire (not electronic) communications, the tracking device exception did not apply.⁴² As for tower dumps (i.e., a record of every phone using a particular tower), courts generally considered them to qualify as a search under the Fourth Amendment.⁴³ The collection of information on innocent citizens and the volume of information mattered: in some requests, providers turned over up to 150,000 telephone numbers in a given area at a particular time.⁴⁴

B. DOCTRINAL PLACEMENT

Like the statutory realm, the Court’s jurisprudence did not provide an easy fit for CSLI, which fell somewhere between public versus private space and third-party doctrine (both of which consistently ignored the impact of technology on Fourth Amendment rights) and more recent decisions that had begun to acknowledge the privacy interests at stake.⁴⁵ The shadow of *Katz*, and the subjective nature of the reasonableness test, loomed large.

1. *First analogical fallacy: the application of assumption of risk and fairness (from public space doctrine) to location tracking.* The Supreme Court has long held that observation outdoors does not constitute

Espudo, 954 F Supp 2d 1029, 1036–37 (SD Cal 2013) (prospective CSLI does not create a “record” under 2703, which is only for data already captured). But see *United States v Powell*, 943 F Supp 2d 759, 777 (ED Mich 2013) (deciding a mobile phone is not a tracking device because it is not owned by the government and 18 USC § 3117 is geared toward installation). Courts have, for prospective CSLI, tended to resolve the question under *Knotts* and the public/private distinction, and not within the third-party context. See, for example, *United States v Forest*, 355 F3d 942, 950–52 (6th Cir 2004). One court has found that even if an individual has a reasonable expectation of privacy in real-time location data, the government does not violate it by arresting her, without a warrant, while she is traveling with the target of the surveillance. See *United States v Peters*, 333 F Supp 3d 366, 376–78 (D Vt 2018).

⁴¹ See, for example, *In re United States for an Order Authorizing the Use of Two Pen Register and Trap and Trace Devices*, 632 F Supp 2d 202, 207 (EDNY 2008); *In re Application of the United States for an Order Authorizing the Disclosure of Cell Site Location Information*, 2009 WL 8231744 (ED Ky).

⁴² *In re Application of United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to Government*, 620 F3d 304, 310 (3d Cir 2010).

⁴³ See, for example, *In re United States ex rel Order Pursuant to 18 U.S.C. Section 2703(d)*, 930 F Supp 2d 698, 702 (SD Tex 2012); *In re Application of United States for an Order Pursuant to 18 USC § 2703(d)*, 964 F Supp 2d 674, 678 (SDNY 2013).

⁴⁴ *In re Application of United States*, 964 F Supp 2d at 678.

⁴⁵ See also *Carpenter*, 138 S Ct at 2215–16, 2218–19 (discussing *Knotts* and *Jones*).

a search.⁴⁶ Following *Katz*, it came to include anything that could be seen from the air or on the ground—from greenhouses missing roof tiles to cars traveling along thoroughfares.⁴⁷ These cases often downplayed the privacy implications of new technologies, even lauding their use for ensuring more accurate information.⁴⁸

The Court's argument as to why individuals had no reasonable expectation of privacy in public ultimately turned on a two-part argument grounded in assumed risk and fairness. First, what an individual knowingly exposed to others was different from what he or she sought to keep private. By deciding to go outside and get into a car, individuals knowingly ran the risk that others would be able to observe them. Second, a basic principle of fairness applied: it would be strange to tell a police officer that she must close her eyes or cover her ears to block what anyone else could see or hear.⁴⁹ Traveling in public therefore fell outside the protections of the Fourth Amendment.

CSLI, at first glance, appeared to come within the public/private distinction: if there was no privacy interest in a global positioning

⁴⁶ See, for example, *Hester v United States*, 265 US 57 (1924) (observation of open fields does not constitute a search); *Air Pollution Variance Board v Western Alfalfa Corp.*, 416 US 861 (1974) (conducting opacity test on smoke coming out of a stack up to a quarter of a mile away does not constitute a search); *Oliver v United States*, 466 US 170, 178 (1984) (“[A]n individual may not legitimately demand privacy for activities conducted out of doors in fields, except in the area immediately surrounding the home.”); *United States v Dunn*, 480 US 294, 304 (1987) (“Under *Oliver* and *Hester*, there is no constitutional difference between police observations conducted while in a public place and while standing in the open fields.”); *California v Greenwood*, 486 US 35, 40 (1988) (citations omitted) (examination of garbage left at the curb does not constitute a search on the grounds that it is “readily accessible to animals, children, scavengers, snoops, and other members of the public”).

⁴⁷ See *California v Ciraolo*, 476 US 207, 211 (1986) (noting that even high fences “might not shield [marijuana plants] from the eyes of a citizen or a policeman perched on the top of a truck or a two-level bus.”); *Dow Chemical Co. v United States*, 476 US 227, 236, 239 (1986) (drawing a distinction between private and public space and holding that while the company had a “reasonable, legitimate, and objective expectation of privacy within the interior of its covered buildings,” it did not have one in regard to areas visible outside the structure); *Florida v Riley*, 488 US 445 (1989) (holding that areas visible from the air were not protected under the Fourth Amendment); *Cardwell v Lewis*, 417 US 583, 590 (1974) (plurality) (“A car has little capacity for escaping public scrutiny. It travels public thoroughfares where its occupants and its contents are in plain view.”); *United States v Karo*, 468 US 705 (1984); *United States v Knotts*, 460 US 276 (1983). Compare *United States v Michael*, 622 F2d 744 (5th Cir 1980) (holding that warrantless installation of a beeper outside of exigent circumstances required prior judicial authorization), rehearing granted, 628 F2d 931 (5th Cir 1980), rev’d, 645 F2d 252 (5th Cir 1981) (holding that installation of a beeper requires only reasonable suspicion).

⁴⁸ See, for example, *Knotts*, 460 US at 282 (“Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.”).

⁴⁹ See also *Katz*, 389 US at 361 (Harlan, J. concurring) (considering actions in public to lay outside Fourth Amendment protections).

system (GPS) chip on a car, why would it be any different in regard to a GPS chip in a telephone? Either way, the information revealed the location of an individual in public space. GPS, moreover, is accurate within centimeters. Why should CSLI, which is *less* accurate, come within the protections of the Fourth Amendment?

The picture, though, was more complicated. For one, cars generally do not follow individuals inside the curtilage of the home. Phones do. For another, the ubiquity of mobile devices resulted in the generation of terabytes of information about millions of people for lengthy periods of time. This raised deeper privacy implications than someone watching a car drive by. It was unclear, though, whether and how this distinction impacted the doctrine. If there were no interests implicated at the front end, what created the back-end right? The only doctrinally relevant question was whether it was a search at the outset.⁵⁰ In addition, unlike GPS systems or RFID chips, for mobile devices, law enforcement did not have to *do* or *attach* anything to the individual or vehicle in order to obtain extensive amounts of information.⁵¹ It was not entirely clear how this cut. Finally, both parts of the Court's logic for the public/private distinction—that upon entering the public sphere an individual assumed the risk that other citizens could observe them, and that there was something fundamentally unfair about disadvantaging law enforcement in comparison to others—rang somewhat hollow when *no* person actually could observe an individual twenty-four hours a day, seven days a week, for months, or even years without end.

2. *Second analogical fallacy: the application of assumption of risk and voluntariness (from informant doctrine) to third-party records.* The second jurisprudential home, third-party doctrine, proved equally problematic. It derived from cases dealing with informers that predated *Katz* and continued in its wake.⁵² Like open space doctrine, the informant cases saw technology not as deepening any expectation of privacy, but merely as enhancing human capabilities and offering a

⁵⁰ See *United States v. Graham*, 846 F. Supp. 2d 384 (D. Md. 2012).

⁵¹ *In re Application of the United States for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace*, 405 F. Supp. 2d 435, 449 (SDNY 2005).

⁵² For informant cases prior to *Katz*, see *On Lee v. United States*, 343 U.S. 747 (1952); *Lopez v. United States*, 373 U.S. 427 (1963); *Hoffa v. United States*, 385 U.S. 293 (1966); *Lewis v. United States*, 385 U.S. 206 (1966). For cases following *Katz*, see *United States v. White*, 401 U.S. 745 (1971); *United States v. Caceras*, 440 U.S. 741 (1979).

more efficient way to get (more) accurate information.⁵³ They also followed a parallel assumption-of-risk argument: voluntarily confiding information in others meant that an individual essentially consented to the possibility that the other person would divulge the information to others.⁵⁴

Katz did nothing to alter the calculation. In 1971, the Court maintained its stance in *United States v White*, in which a prosecutor introduced a recorded conversation between an informer and a suspect at trial.⁵⁵ Justice White, writing for the Court, explained, “[O]ne contemplating illegal activities must realize and risk that his companions may be reporting to the police. . . . [I]f he has no doubts, or allays them, or risks what doubt he has, the risk is his.”⁵⁶

In *Miller*, Justice Powell, writing for the Court, cited back to the informant cases to exempt third-party business records from the protections of the Fourth Amendment:

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.⁵⁷

For the Court, just as criminals assumed the risk in telling others of their plans that someone would pass on that information, so, too, did the decision to provide financial information to a bank deprive it of Fourth Amendment protections. The key was that the data were

⁵³ See, for example, *Lopez v United States*, 373 US 427, 438–39 (1963) (the Constitution does not recognize a right to probe “flaws in the agent’s memory, or to challenge the agent’s credibility without being beset by corroborating evidence that is not susceptible of impeachment.”); *White*, 401 US at 751–52 (plurality) (“If the law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent, neither should it protect him when that same agent has recorded or transmitted the conversations”); *id.* at 753 (arguing that the Court should not “be too ready to erect constitutional barriers to relevant and probative evidence which is also accurate and reliable.”).

⁵⁴ See *On Lee v United States*, 343 US at 751–53 (by confiding information to an undercover agent on whom a microphone had been placed, On Lee consented to the possibility that law enforcement would overhear the conversation); *Lopez*, 373 US at 438–39 (use of a recording device did nothing to alter the assumption of risk); *Hoffa*, 385 US at 303 (“The risk of being overheard by an eavesdropper or betrayed by an informer . . . is the kind of risk we necessarily assume whenever we speak.”).

⁵⁵ *White*, 401 US at 746–47 (plurality).

⁵⁶ *Id.* at 752.

⁵⁷ *United States v Miller*, 425 US 435, 443 (1976). In *Carpenter*, Gorsuch asks what theory underlies the assumption of risk argument in third-party doctrine tying it back, potentially, to tort law. See *Carpenter*, 138 S Ct at 2263 (Gorsuch, J, dissenting).

voluntarily divulged, indicating that the individual consented to the possibility that they would be provided to others.⁵⁸ By applying this logic to third-party business records, the Court employed an analogical fallacy with profound implications.

Most critically, by equating spoken words with “papers and effects,” the Court buried an essential Fourth Amendment protection. At the founding, “papers” had a privileged place in the Constitution, reflecting the contemporary view that such documents were protected from government inspection.⁵⁹ In the 1765 case of *Entick v Carrington*, Lord Camden famously reflected, “Papers are the owner’s goods and chattels: they are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection.”⁶⁰ The Father of Candor seized on the case and loosed a vitriolic attack on the Crown: “What then, can be more excruciating torture, than to have the lowest of mankind . . . enter suddenly into [Entick’s] house, and forcibly carry away his scrutores, with all his papers of every kind, under a pretence of law.”⁶¹ Entry mattered. But of equal importance was doing so *to access Entick’s papers*. Reeling from the trials associated with the Crown’s effort to apprehend Entick and “the authors, printers, and publishers” of *North Britain* No. 45, Parliament passed a resolution condemning the Crown’s actions and expressing strong protections for private and commercial documents.⁶² Edmund Burke wrote, “The lawful secrets of *business and friendship* were rendered inviolable, by the [Parliamentary] resolution for condemning the seizure of papers.”⁶³

⁵⁸ *Miller*, 425 US at 442 (“All of the documents obtained . . . contain only information voluntarily conveyed to the banks.”).

⁵⁹ Donald A. Dripps, “Dearest Property”: *Digital Evidence and the History of Private “Papers” as Special Objects of Search and Seizure*, 103 J Crim L & Criminol 49 (2013); Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 Wake Forest L Rev 307 (1998).

⁶⁰ *Entick v Carrington*, 19 Howell St Tr 1030 (KB 1765).

⁶¹ Father of Candor, *A Letter Concerning Libels, Warrants, the Seizure of Papers, and Sureties for the Peace of Behavior* (7th ed 1770) (first published in 1764 as *An enquiry into the doctrine lately propagated concerning libels, warrents, and the seizure of papers*, with likely authorship John Almon).

⁶² *The General Warrant on Which John Wilkes Was Arrested, 30 April 1763*, in D. B. Horn, ed, *English Historical Documents 1714–1815* 61, 61–62 (Methuen, 1967). See also Donohue, 83 U Chi L Rev at 1196–1207 (cited in note 5).

⁶³ 1 Edmund Burke, *A Short Account of a Late Short Administration* (1766), in *The Works of the Right Honorable Edmund Burke* 265, 265 (1865), quoted in Dripps, 103 J Crim L & Criminol at 72 (cited in note 59) (emphasis added).

Americans were equally appalled at the Crown's reach.⁶⁴ Papers—whether social, personal, or commercial—were sacrosanct.⁶⁵ Accordingly, the new state constitutions, as well as the federal constitution, protected “papers.”⁶⁶ For nearly a century, there was no effort made by Congress to obtain personal or business-related documents. It was not until 1863 that the first statute appeared, authorizing warrants to obtain “any invoices, books, or papers” related to undutied goods.⁶⁷ It was an enormous departure from the status quo—and from *Entick*, which was still good law.⁶⁸ Whether or not it was “reasonable” to obtain commercial papers was of no consequence. The government *could not obtain them at all*. Accordingly, the *Boyd* Court flatly rejected the statute, noting that it was the first time in the history of England or the United States that a legislature had tried to search and seize, or to compel the production, of “a man’s private papers . . . for the purpose of using them in evidence against him in a criminal case.”⁶⁹ Forcing the production of papers “would be subversive of all the comforts of society.”⁷⁰

The *Boyd* Court got it right: alteration did have profound consequences. Starting with *Miller*, the ability of the people to engage in commercial relationships within the protections of the Fourth Amendment sharply eroded. The *Miller* Court failed to acknowledge that what was potentially at stake was all of a person’s business records—effectively eviscerating a critical constitutional right.

The analogical reasoning underlying third-party doctrine also failed to appreciate that there was a world of difference between confiding illegal behavior in (supposed) coconspirators, and engaging in an entirely legal, contractual relationship to conduct business. The information entrusted to a bank was provided for a specific, legal purpose. The customers’ financial records were not publicly available. Indeed, banks were under a *legal obligation* not to allow the information

⁶⁴ Donohue, 83 U Chi L Rev at 1257–60 (cited in note 5).

⁶⁵ H. Brian Holland, *A Cognitive Theory of the Third-Party Doctrine and Digital Papers*, 91 Temple L Rev 55, 60 (2018).

⁶⁶ See Pa Const of 1776, Decl of Rights Art X (superseded 1790); NH Const of 1783, Bill of Rights Art XIX; Vt Const of 1777, Decl of Rights Art XI (superseded 1793); Ma Const of 1780, Part the First: Declaration of Rights Art XIV; US Const, Amend IV.

⁶⁷ See Act of Mar 3, 1863, ch 76, 12 Stat 737, 740.

⁶⁸ See generally Dripps, 103 J Crim L & Criminol at 72 (cited in note 59).

⁶⁹ *Boyd v United States*, 116 US 616, 622 (1886).

⁷⁰ *Id* at 628.

to be made public. Although Congress responded to *Miller* with the Right to Financial Privacy Act, the Court held its course.⁷¹

Another weakness in the analogy centered on consent. In *Miller*, as aforementioned, the Court assumed that, like the criminal confiding in potential accomplices, the person with a bank account knew that the bank might turn the information over to others.⁷² This argument performs a sleight of hand: consenting to give the bank access to financial data for a specific use is not the same as consenting to the company releasing it to the public at large—much less to the government.⁷³ To the contrary, it is a limited disclosure for a specific, contractual purpose.

Finally, the analogical reasoning failed in regard to its emphasis on voluntariness. It assumed that, just like confiding in coconspirators, submitting financial information to the bank was voluntary.⁷⁴ The Court did *not* consider whether *banking* itself was voluntary in the modern world. Nor did it give any credence to the fact that the Bank Secrecy Act *required* the bank to obtain consumer information and maintain certain records.⁷⁵ For the Court, “The depositor [took] the risk, in revealing his affairs to another, that the information [would] be conveyed by that person to the Government.”⁷⁶

To summarize, analogizing between informant doctrine and third-party records buried a critical constitutional protection for commercial “papers”; equated legal, contractual relationships with the secret whisperings of criminals (thereby denying the former protection); assumed that consenting to provide information to a third party for a limited, legal purpose amounted to acquiescing to government

⁷¹ Right to Financial Privacy Act of 1978, Pub L No 95-630, 92 Stat 3641.

⁷² See also *Carpenter*, 138 S Ct at 2263 (Gorsuch, J, dissenting) (“Consenting to give a third party access to private papers that remain my property is not the same thing as consenting to a *search of those papers by the government*.”) (emphasis in original); *id* (citing and quoting Kerr, 107 Mich L Rev at 588 (“So long as a person knows that they are disclosing information to a third party, their choice to do so is voluntary and the consent valid”) (cited in note 19).

⁷³ See also *Smith v Maryland*, 442 US 735, 749 (1979) (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”).

⁷⁴ *Miller*, 425 US at 442 (“[a]ll of the documents obtained, including financial statements and deposit slips, contain only information *voluntarily* conveyed to the banks and exposed to their employees in the ordinary course of business.”) (emphasis added).

⁷⁵ *Id* at 442–43.

⁷⁶ *Id* at 443 (citing *White*, *Hoffa*, and *Lopez*).

search of the material; and presumed that conducting business as part of the ordinary affairs of modern life was voluntary.

As they confronted CSLI, the lower courts wrestled with the voluntariness component, seeing it as the linchpin for ascertaining whether third-party doctrine applied. They questioned the extent to which individuals freely elected either to carry phones or to provide their location to the service provider.⁷⁷ With precious little guidance from *Katz* or its progeny, the decisions ended up all over the map.

Some judges considered the provision of CSLI to be voluntary.⁷⁸ Others came out on the other side.⁷⁹ One of the most notable cases arose in 2008 in the Third Circuit, where *all* of the magistrate judges in the Western District of Pennsylvania, in a highly unusual move, cosigned an opinion rejecting a § 2703(d) order for historical cell site data.⁸⁰ The decision turned on whether customers voluntarily provided location information. The court recognized the ubiquitous use of cell phones and observed that users do not share their location “in any meaningful way.”⁸¹ “[W]hen a cell phone user receives a call,” moreover, “he hasn’t voluntarily exposed anything at all.”⁸² The court considered the phone to be a tracking device, for which a warrant was

⁷⁷ See, for example, *In re Application of the United States for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace*, 405 F Supp 2d at 449; *In re Application of the United States for an Order Authorizing the Disclosure of Cell Site Location Information*, 2009 WL 8231744 (ED Ky).

⁷⁸ See, for example, *United States v Gordon*, 2012 WL 8499876 (DDC) (upholding); *United States v Ruby*, 2013 WL 5448888 (SD Cal) (upholding six weeks of CSLI on grounds they are business records/not protected under *Smith* and *Miller*); *United States v Rigmaiden*, 2013 WL 1932800 (D Ariz) (*Smith* and *Miller* control); *United States v Denard*, 24 F3d 599 (5th Cir 2013).

⁷⁹ See, for example, *In re Application of United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to Government*, 620 F3d 304 (3rd Cir 2010); *In re United States for Historical Cell Site Data*, 747 F Supp 2d 827 (SD Tex 2010).

⁸⁰ *In re United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 534 F Supp 2d 585 (WD Pa 2008). The appellate court commented, “This is unique in the author’s experience of more than three decades on this court and demonstrates the impressive level of support Magistrate Judge Lenihan’s opinion has among her colleagues.” *In re Application for an Order*, 620 F3d at 308.

⁸¹ *In re Application for an Order*, 620 F3d at 317. See also *In re United States*, 534 F Supp 2d at 589 (“Our individual cell phones now come with us everywhere: not only on the streets, but in (a) business, financial, medical and other offices; (b) restaurants, theaters and other venues of leisure activity; (c) churches, synagogues and other places of religious affiliation; and (d) our homes and those of our family members, friends, and personal and professional associates.”).

⁸² *In re Application for an Order*, 620 F3d at 317–18.

required.⁸³ Rule 41, amended by the Supreme Court in 2006, provided for the installation and use of a tracking device, for a renewable period not to exceed forty-five days.⁸⁴ Failure to meet these requirements resulted in exclusion of the evidence.⁸⁵

The government appealed the magistrates' decision to the District Court, which, recognizing the complex issues in the case, affirmed the decision in a short, two-page order, kicking it up to the Court of Appeals for de novo review. The Third Circuit concurred, saying that the magistrate had the discretion to require a warrant.⁸⁶ The government could not force a disclosure with less if a court considered the records to be more sensitive.

3. *Addressing the technology gap: Jones, Riley, and disarray.* The subjective nature of the test from *Katz*, in concert with technological advances and inherent doctrinal hostility to acknowledging any resultant constitutional implications, created a world in which "the right of the people to be secure" against government inspection steadily narrowed. The dissonance between the supposed reasonableness test and reality demanded attention. But as the Supreme Court began acknowledging the deeper privacy interests in mobile telephone-related technologies, the application of *Katz* to location tracking was thrown into further doubt.

One of the most important cases, *United States v Jones*, originated in the 2010 case of *United States v Maynard*. The FBI placed a GPS device on a suspected drug dealer's car while it was on private property and then tracked the position of the car every ten seconds for twenty-eight days, without a warrant. The D.C. Circuit held that the tracking amounted to a search, which was per se unreasonable and thus, absent a warrant, violated the Fourth Amendment.⁸⁷ Writing for the panel, Judge Douglas Ginsburg zeroed in on one of the analogical fallacies in open space doctrine: he concluded that Jones had not knowingly exposed his behavior to the public "because the likelihood anyone

⁸³ *In re United States*, 534 F Supp 2d at 613–14.

⁸⁴ *Id.* at 592.

⁸⁵ *Id.*

⁸⁶ *In re Application for an Order*, 620 F3d at 317.

⁸⁷ *United States v Maynard*, 615 F3d 544, 555–56 (DC Cir 2010), rehearing en banc denied, *United States v Jones*, 625 F3d 766 (DC Cir 2010) (mem), cert denied, *Maynard v United States*, 131 S Ct 671 (2010) (mem).

will observe all those movements is effectively nil.”⁸⁸ While, perhaps, physically possible, a reasonable person would not expect a government agent to tail them twenty-four hours a day for a month.

The Supreme Court granted cert in *Maynard* (renamed *Jones*) and ultimately decided the case based on trespass.⁸⁹ Two concurrences, though, created a “shadow majority” that cast doubt on location tracking and the future of third-party doctrine.

In her concurring opinion, Justice Sotomayor wrote, “GPS monitoring generates a precise, comprehensive record of a person’s public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.”⁹⁰ Sotomayor indicated that she might go so far as to reconsider third-party doctrine altogether, noting that it was “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.”⁹¹

Justice Alito, in a concurring opinion joined by Justices Ginsburg, Breyer, and Kagan, similarly raised arguments that challenged location tracking and third-party doctrine. “[W]hat is really important,” he suggested, is “the *use* of a GPS for the purpose of long-term tracking.”⁹² The majority’s approach led “to incongruous results.”⁹³ Under the open space doctrine, no Fourth Amendment interest would be implicated if law enforcement had followed the car, even longer, from the air and the ground. So why would the installation of a GPS chip yield a different result?⁹⁴ What would the constitutional analysis have been if law enforcement had simply tracked a GPS system already installed in the car?⁹⁵ Alito expressed concern at myriad “new devices that permit the monitoring of a person’s movements,” acknowledging that “cell phones and other wireless devices now permit wireless carriers to track and record the location of users,” which implicated more than 322 million wireless devices.⁹⁶ The point at which

⁸⁸ *Maynard*, 615 F3d at 558, 563.

⁸⁹ *United States v Jones*, 565 US 400 (2012).

⁹⁰ *Id.* at 417 (Sotomayor, J, concurring).

⁹¹ *Id.*

⁹² *Jones*, 565 US at 424 (Alito, J, concurring).

⁹³ *Id.* at 425.

⁹⁴ *Id.*

⁹⁵ *Id.* at 426.

⁹⁶ *Jones*, 565 US at 428.

the tracking became a search “was surely crossed before the 4-week mark.”⁹⁷

Two years after *Jones*, the Supreme Court again wrestled with how to apply *Katz* in a way that took account of the intrusiveness of mobile technologies. *Riley v California* focused on another exception carved out by the Court post-*Katz*: search incident to arrest.⁹⁸ In *Riley*, a law enforcement officer stopped the petitioner for a traffic violation, leading to an arrest on weapons charges.⁹⁹ During the arrest, the officer, discovering a mobile phone in Riley’s pants pocket, scrolled through it and found photographs, videos, and language suggesting involvement in gang activity.¹⁰⁰ Based in part on the data uncovered, the government prosecuted him for a prior shooting with a sentence enhancement for membership in the Bloods.¹⁰¹

The Supreme Court objected, carving out (yet another) exception to an exception: officers may search an individual incident to arrest without a warrant, but if they want to inspect a telephone they must first obtain a warrant.¹⁰² The immense storage capacity of cell phones had “several interrelated consequences for privacy”: they collect more information in one place than present in isolated records; the volume at stake in even one category of information may be enormous; data held on the device can stretch back for years; and the records provide a detailed and comprehensive view into an individual’s private life.¹⁰³

Together, *Jones* and *Riley* indicated judicial disquiet at how the exceptions carved out post-*Katz* had failed to take account of the

⁹⁷ *Id.* at 431.

⁹⁸ *Riley v California*, 134 S Ct 2473 (2014), taken in conjunction with *United States v Wurie*, 728 F3d 1 (2013), cert granted 134 S Ct 999 (2014). See also *Chimel v California*, 395 US 752, 762–63 (1969) (requiring a search incident to arrest be restricted to the area of the arrestee’s immediate control as justified by the need for officer safety and preservation of evidence); *United States v Robinson*, 414 US 218, 235 (1973) (holding, “[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.”); *United States v Chadwick*, 433 US 1, 15 (1977) (limiting the search incident to arrest exception to “personal property . . . immediately associated with the person of the arrestee.”).

⁹⁹ *Riley*, 134 S Ct at 2480.

¹⁰⁰ *Id.*

¹⁰¹ *Id.* at 2481.

¹⁰² *Id.* at 2485.

¹⁰³ *Riley*, 134 S Ct at 2489–91.

impact of new technologies on Fourth Amendment rights. But they did not squarely address the underlying doctrinal concerns.

4. *Growing judicial tension.* In the aftermath of *Jones*, the Fifth, Sixth, Tenth, and Eleventh Circuits held that historic CSLI amounted to information voluntarily conveyed to a third party and thus controlled by *Miller* and *Smith* and not abrogated by *Jones*.¹⁰⁴ Simultaneously, the judiciary expressed significant frustration and concern. In 2017, the Tenth Circuit raised alarm at the implications, writing, “[W]e, too, fear the Orwellian-style surveillance state that could emerge from unfettered government collection of personal data.”¹⁰⁵ But “until the Supreme Court instructs us otherwise, we are bound to follow its

¹⁰⁴ See *United States v Richardson*, 732 Fed Appx 822, 828 (11th Cir 2018) (per curiam) (holding warrantless acquisition of cell-tower data as outside the Fourth Amendment); *United States v Banks*, 884 F3d 998, 1011–13 (10th Cir 2018) (finding a state court order for historical and real-time tracking consistent with statutory requirements and exigent circumstances); *United States v Thompson*, 866 F3d 1149, 1156–59 (10th Cir 2017), cert granted, 138 S Ct 2706 (stating covered by *Smith/Miller*); *United States v Carpenter*, 819 F3d 880, 887–88 (6th Cir 2016) (adding the content/noncontent distinction, saying that *Smith* is mainly about noncontent and concluding, “The business records here fall on the unprotected side of this line. Those records say nothing about the content of any calls.”); *United States v Davis*, 785 F3d 498, 511 (11th Cir 2015) (en banc) (there is “no reason to conclude that cell phone users lack facts about the functions of cell towers or about telephone providers’ recording cell tower usage.”); *United States v Graham*, 824 F3d 421, 424–26 (4th Cir 2016) (en banc) (overturning panel on third-party grounds); *In re Application of the United States for Historical Cell Site Data*, 724 F3d 600, 614, 610, 613–14 (5th Cir 2013) (even though user “does not directly inform his service provider of the location of the nearest cell phone tower,” it is the company that holds the information, demonstrating that the customer “knowingly exposes his activities” to the third party. Additionally, use of a mobile phone is “entirely voluntary.”); *United States v Skinner*, 690 F3d 772, 777 (6th Cir 2012) (defendant has no “reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone.”). Compare *United States v Riley*, 858 F3d 1012, 1018 (6th Cir 2017) (Court of Appeals held that police officers did not conduct search under Fourth Amendment when it tracked real-time GPS coordinates of firearm defendant’s cell phone for seven hours on date of his arrest), and *United States v Forest*, 355 F3d 942, 950–52 (6th Cir 2004) (rejecting *Miller/Smith* but applying *Knotts* to find no reasonable expectation of privacy in CSLI and holding that coconspirator lacked standing to bring a constitutional claim simply because he also was being tracked when they were together). Numerous district court cases followed suit. See, for example, *United States v Jones*, 2018 WL 3212073 (ED Ky); *United States v Serrano*, 2017 WL 3055244 (SDNY); *United States v Rosario*, 2017 WL 2117534 (ND Ill); *United States v Adkinson*, 2017 WL 1318420, *5 (SD Ind); *United States v Lambis*, 197 F Supp 3d 606, 615 (SDNY 2016); *United States v Wheeler*, 169 F Supp 3d 896, 910 (ED Wis 2016); *United States v Lang*, 78 F Supp 3d 830, 836 (ND Ill 2015); *United States v Rogers*, 71 F Supp 3d 745 (ND Ill 2014); *United States v Moreno-Nevarez*, 2013 WL 5631017, *2 (SD Cal); *United States v Money*, 2013 WL 412626 (ED Ky); *United States v Caraballo*, 963 F Supp 2d 341 (D Vt 2013); *United States v Degaule*, 797 F Supp 2d 1332 (ND Ga 2011); *United States v Benford*, 2010 WL 1266507, *2–3 (ND Ind); *United States v Navas*, 640 F Supp 2d 256 (SDNY 2009), rev’d in part on other grounds, *United States v Navas*, 597 F3d 492 (2d Cir 2010); *In re Applications of United States for Orders Pursuant to Title 18, US Code, Section 2703(d)*, 509 F Supp 2d 81 (D Mass 2007).

¹⁰⁵ *United States v Thompson*, 866 F3d 1149, 1159 (10th Cir 2017) (also writing, “Thompson raises valid concerns about the third-party doctrine in the digital age.”). See also *Carpenter*, 819 F3d 893–94 (Stranch concurring in the judgment but rejecting the reasoning) (writing “the sheer quantity of sensitive information procured without a warrant in this case raises

third-party doctrine precedents.”¹⁰⁶ The Fourth Circuit reflected, “The Supreme Court may in the future limit, or even eliminate, the third-party doctrine. . . . But without a change in controlling law,” their hands were tied.¹⁰⁷

Scathing criticism of third-party doctrine followed. In the Fourth Circuit, Judge Wynn stated there was “no reason to think that a cell phone user is aware of his CSLI or that he is conveying it,” and noted that such information was recorded even when users receive calls, taking no action of their own.¹⁰⁸ In the Eleventh Circuit Judge Martin wrote that the “application of the third-party doctrine threatens to allow the government access to a staggering amount of information that surely must be protected under the Fourth Amendment.”¹⁰⁹ Several state supreme courts flatly contradicted the Supreme Court, holding that there *is* a reasonable expectation of privacy in real time or historic CSLI under state constitutional provisions nearly identical to the Fourth Amendment.¹¹⁰

In the Sixth Circuit, *United States v Carpenter* reflected the growing confusion and concern among the lower courts. A man arrested for a series of robberies confessed to the crime and identified fifteen

Fourth Amendment concerns of the type the Supreme Court acknowledged in *United States v Jones*,” and observing that “the addition of cellular (not to mention internet) communication has left courts struggling to determine if (and how) existing [Fourth Amendment] tests apply or whether new tests should be framed,” but finding, nevertheless, that the good faith exception to the exclusionary rule applied).

¹⁰⁶ *Thompson*, 866 F3d at 1154.

¹⁰⁷ *United States v Graham*, 824 F3d at 425–26.

¹⁰⁸ *Id* at 445 (Wynn, J, concurring).

¹⁰⁹ *United States v (Quartavious) Davis*, 785 F3d 498, 535 (11th Cir 2015) (en banc) (Martin dissenting).

¹¹⁰ See *Commonwealth v Holley*, 87 NE3d 77 (Mass 2017); *Jones v United States*, 168 A3d 703 (DC 2017); *State v Copes*, 165 A3d 418 (Md 2017); *Commonwealth v Fulgiam*, 73 NE3d 798 (Mass 2017); *State v Lunsford*, 141 A3d 270 (NJ 2016); *State v Simmons*, 143 A3d 819 (Me 2016); *Tracey v State*, 152 So 3d 504 (Fla 2014); *Commonwealth v Augustine*, 4 NE3d 846 (Mass 2014); *State v Earls*, 70 A3d 630 (NJ 2013). But see *Zanders v State*, 73 NE3d 178 (Ind 2017), vac’d, 138 S Ct 2206 (2018); *Hankston v State*, 517 SW3d 112 (Tex Crim App 2018); *Love v State*, 543 SW3d 835 (Tex Crim App 2018); *State v Jenkins*, 884 NW2d 429 (Neb 2016); *Marchman v State*, 787 SE2d 734 (Ga 2016); *Taylor v State*, 371 P3d 1036 (Nev 2016); *State v Simmons*, 143 A3d 819 (Me 2016); *Ford v State*, 477 SW3d 321 (Tex Crim App 2015); *Ross v State*, 769 SE2d 43 (Ga 2015); *State v Griffin*, 834 NW2d 688 (Minn 2013). Compare *State v Subdiaz-Orsorio*, 849 NW2d 748, 768 (Wis 2014) (declining to address “whether society is prepared to recognize as reasonable an expectation of privacy in cell phone location data,” and determining instead that the tracking at issue in the case fell within the exigent circumstances exception); *Commonwealth v Estabrook*, 38 NE3d 231 (Mass 2015) (determining that six hours of CSLI falls short of constitutional search requirements).

accomplices, providing some of their mobile numbers to the FBI.¹¹¹ Prosecutors used the SCA to apply for court orders to produce geolocation data for several suspects, including Timothy Carpenter.¹¹² The government obtained three orders for sixteen different phones, including “[a]ll subscriber information, toll records and call detail records including listed and unlisted numbers dialed or otherwise transmitted to and from [the] target telephones” as well as “cell site information for the target telephones at call origination and at call termination for incoming and outgoing calls.”¹¹³

The request amounted to 127 days of Carpenter’s records,¹¹⁴ which was at the low end of the spectrum in terms of the length of surveillance and the amount of CSLI information obtained. In *United States v Rogers*, for example, a case in the Northern District of Illinois, the government secured three orders for historic CSLI, with a total of 430 days of continuous surveillance of two phones.¹¹⁵ In *United States v Jones*, which arose in the Eastern District of Kentucky, the numbers were even starker: two warrants issued in relation to thirteen different numbers sought historical CSLI for 739 days.¹¹⁶

In the face of the significant inroads into privacy, a doctrinal morass, and open judicial frustration, the Supreme Court had little choice but to grant certiorari. But even as it reached the right answer, it did so in a way that failed either to inter third-party doctrine or to begin to rationalize Fourth Amendment law.

III. THE PROBLEM WITH CARPENTER

Carpenter can best be understood as a 5+1 decision, in which the Court recognized that the whole of one’s movements over a seven-

¹¹¹ *Carpenter*, 138 S Ct at 2218.

¹¹² *Id.*

¹¹³ *Carpenter*, 819 F3d at 884.

¹¹⁴ *Id.* at 886.

¹¹⁵ *United States v Rogers*, 71 F Supp 3d 745 (ND Ill) (first order under § 2703(d) for Rogers’s historic records covering June 1, 2012 to March 29, 2013 (302 days); second order for CSLI from Curtis’s phone covering June 1, 2012 to April 10, 2013 (333 days); third order for both phones covering March 29, 2013 to August 13, 2013 (128 more days), bringing the total for both phones to 430 days in a row).

¹¹⁶ *United States v Jones*, 2018 WL 3212073, *8 (ED Ky). The Nov 16, 2015 warrant authorized search and seizure in relation to thirteen different telephone numbers, including, inter alia, historical collection of CSLI and cell tower identification records for call transmissions, all available text/SMS records (including contents), GPS location records, and roaming records covering September 21, 2013 to September 30, 2015 (DTC wireless’s records), while the March 28, 2016 warrant authorized similar search and seizure as obtained from AT&T, which included CSLI, but not the content of communications. *Id.* at *1.

day period are protected by the Fourth Amendment. In an opinion authored by Chief Justice Roberts, the five-Justice majority applied *Katz* to establish that individuals have a reasonable expectation of privacy in location information held by service providers, carving out an exception to third-party doctrine.¹¹⁷ Justice Gorsuch, in his dissent, also would have protected the information under the Fourth Amendment, but he was deeply unsatisfied with the Court's rationale.

Gorsuch got it right. The decision failed to address the doctrinal morass and created significant uncertainty for lower courts going forward. The factors that distinguish location data apply equally well to numerous types of digital records—including those at issue in *Miller* and *Smith*, raising questions about whether *Carpenter* has overturned third-party doctrine in all but name. The factors employed by the Court rely on subjective determinations, pushing the judiciary even more firmly into a policy-making realm. In its dogged adherence to voluntariness, itself the result of an analogical fallacy, the Court vacillated between device-use compulsion and record-creation compulsion, further obfuscating the doctrine. It provided no guidance whatsoever as to what qualifies as a (reasonable) search of records that now fall within the exception to the exception.

A. CSLI: AN EXCEPTION TO AN EXCEPTION

For the majority in *Carpenter*, the nature of location data loomed large. “[D]etailed, encyclopedic, and effortlessly compiled,”¹¹⁸ the Court wrote, the fact that CSLI was “held by a third-party” was insufficient to deny Fourth Amendment protection.¹¹⁹ In short, “accessing seven days of CSLI constitutes a Fourth Amendment search.”¹²⁰

Jones played a central role in the Court's reasoning in two ways. First, Roberts adopted the shadow majority in the prior case as though it had been the grounds on which it had been decided, writing, “A majority of this Court has already recognized that individuals have

¹¹⁷ *Carpenter*, 138 S Ct 2206, 2217 (2018) (“[A]n individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI.”).

¹¹⁸ *Id.* at 2209.

¹¹⁹ *Id.* at 2211.

¹²⁰ *Id.* at 2217 n. 3. In *Commonwealth v. Estabrook*, 38 NE3d 231, 237 (Mass 2015), a state court held that where the state has complied with statutory requirements for required disclosure of customer communications or records, it may obtain up to six hours of person's CSLI without search warrant.

a reasonable expectation of privacy in the whole of their physical movements.”¹²¹ As Justice Kennedy pointed out in his dissent, in so doing, the Court treated the concurrences as though they were the holding.¹²²

Second, *Carpenter* picked up on language in *Jones*, recognizing the degree to which location data shed light on individuals’ private lives and the role that resource constraints have historically played (indirectly) on what society was prepared to recognize as reasonable.¹²³ Just because records were held by a third party did not negate the character of the information: “time-stamped data provides an intimate window into a person’s life, revealing not only his particular movements, but through them his ‘familial, political, professional, religious, and sexual associations.’”¹²⁴ They could be accessed at the touch of a button “at practically no expense,” making CSLI an “even greater privacy concern[] than the GPS monitoring of a vehicle.”¹²⁵ The issue was not just one of public activity:

A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor’s offices, political headquarters, and other potentially revealing locales. [] Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone’s user.¹²⁶

These qualities, Roberts concluded, paired with factors if not unique to CSLI then certainly characteristic of it, were sufficient to overcome third-party doctrine.

B. WHENCE, THIRD-PARTY DOCTRINE?

To fit its decision within the existing doctrine, the Court reinterpreted *Miller* and *Smith* as applying a balancing test within which CSLI

¹²¹ *Carpenter*, 138 S Ct at 2209–10, citing *United States v Jones*, 565 US 400, 430, 415 (2012) (Alito, J, concurring and Sotomayor, J, concurring).

¹²² *Carpenter*, 138 S Ct at 2231 (Kennedy, J, dissenting), citing *Jones*, 565 US at 404.

¹²³ *Carpenter*, 138 S Ct at 2217 (majority) (prior to digitization, it was costly to pursue suspects for any extended period of time; resultantly, “society’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.”).

¹²⁴ *Id.*, citing *Jones*, 565 US at 415 (Sotomayor, J, concurring).

¹²⁵ *Id.*

¹²⁶ *Id.* at 2218.

could be distinguished. For the majority, these cases were not just about whether an individual had shared information, but also about the nature of the documents as weighed against any legitimate expectation of privacy in the information conveyed.

For the former, the nature of the documents, the Court concluded that the material at issue in CSLI was different in kind than data considered in the prior cases. *Miller* centered on “negotiable instruments to be used in commercial transactions,” while the telephone records in *Smith* provided little by way of “identifying information.”¹²⁷ In contrast, CSLI fell into its own, distinct category, identified by a number of factors: (a) the number of people implicated,¹²⁸ (b) the volume of information,¹²⁹ (c) the revealing nature of the information,¹³⁰ (d) the lack of resource constraints in obtaining it,¹³¹ (e) the retroactive nature of the data,¹³² (f) the near perfect recall,¹³³

¹²⁷ Id at 2219.

¹²⁸ Id at 2215 (“The Government’s [reliance on third-party doctrine] fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter’s location but also everyone else’s, not for a short period but for years and years.”); id at 2218 (“[B]ecause location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone.”).

¹²⁹ Id at 2211–12 (observing the increasing amount of data collected, its use for business purposes ranging from testing the network to applying roaming charges, the increasingly dense cell site coverage, and the increasing number of ways in which the phone was used (e.g., texting and routine data connections) that required location information).

¹³⁰ Id at 2216 (CSLI “is detailed, encyclopedic, and effortlessly compiled.”); id at 2218 (CSLI “gives police access to a category of information otherwise unknowable.”); id at 2220 (CSLI “implicates privacy concerns far beyond those considered in *Smith* and *Miller*.”).

¹³¹ Id at 2217 (“[P]rior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so ‘for any extended period of time was difficult and costly and therefore rarely undertaken.’”); id at 2217–18 (“[Now] cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier’s deep repository of historical location information at practically no expense.”). See also *Jones*, 565 US at 417–18 (Sotomayor, J, concurring); id at 429 (Alito, J, concurring).

¹³² *Carpenter*, 138 S Ct at 2218 (majority) (“[T]he Government can now travel back in time to retrace a person’s whereabouts, subject only to the retention policies of the wireless carriers, which currently maintain records for up to five years.”).

¹³³ Id at 2219 (“Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible. There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today. The Government thus is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information.”).

(g) the potential length of time for which information can be obtained,¹³⁴ and (h) the increasing precision.¹³⁵

For the latter, the expectation of privacy, the Court concluded that the user did not voluntarily convey the information in the same way that a user provided the numbers dialed to the phone company or financial records to a bank. The Court reasoned that mobile phones have become a pervasive part of daily life and an integral part of living in the modern world. Throughout the day, phones automatically log onto cell towers, which means that users do not have to *do* anything to have their location recorded.¹³⁶ In fact, users do not have an option *not* to create a record.¹³⁷ Because conveying the information is not left to the user's discretion, there has been no assumption of risk.¹³⁸

The Court's reinterpretation of *Miller* and *Smith* was met with incredulity by Justices Kennedy, Alito, and Gorsuch in their dissents. For Kennedy, relinquishing the information "to a third party was the entire basis for concluding that the defendants in those cases lacked a reasonable expectation of privacy."¹³⁹ The earlier cases were best read as limiting the damage done by *Katz*, placing "necessary limits on the ability of individuals to assert fourth Amendment interests in property to which they lack a 'requisite connection.'"¹⁴⁰ For Kennedy and

¹³⁴ Id at 2218 (noting that no probable cause is required at the outset for what turns out to be the potential to trail someone every moment of every day for five years).

¹³⁵ Id at 2218–19 ("[T]he rule the Court adopts 'must take account of more sophisticated systems that are already in use or in development.' While the records in this case reflect the state of technology at the start of the decade, the accuracy of CSLI is rapidly approaching GPS-level precision.").

¹³⁶ *Carpenter*, 138 S Ct at 2220 ("Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data.").

¹³⁷ Id ("Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data.").

¹³⁸ Id ("[I]n no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements."), quoting *Smith v Maryland*, 442 US 735, 745 (1979).

¹³⁹ Id at 2232 (Kennedy, J, dissenting). See also id at 2228 (reading *Miller* and *Smith* as considering the "absence of property law analogues" not as part of a balancing test, but as "dispositive of privacy expectations.").

¹⁴⁰ *Carpenter*, 138 S Ct at 2227, quoted and cited id at 2260 (Alito, J, dissenting). See also id at 2259 (Alito, J, dissenting) (writing with *Katz*, "the sharp boundary between personal and third-party rights was tested.").

Alito, *Miller* and *Smith* did not so much create a new doctrine as rectify the uncertainty created by *Katz*.¹⁴¹

Like Kennedy and Alito, Justice Gorsuch read the foundational third-party cases as categorically establishing that individuals have no reasonable expectation of privacy in records held by third parties, “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.”¹⁴² *Miller* and *Smith* did not “distinguish between *kinds* of information disclosed to third parties [or] require courts to decide whether to ‘extend’ those decisions to particular classes of information, depending on their sensitivity.”¹⁴³ They were simply poorly decided—an example of an irrational doctrine. Gorsuch observed, “People often do reasonably expect that information they entrust to third parties, especially information subject to confidentiality agreements, will be kept private.”¹⁴⁴

Justice Kennedy further charged that the Court misapplied even its own misinterpretation of *Miller* and *Smith*: cell site records were not *more* invasive of privacy than financial and telephone records, they were *less* so.¹⁴⁵

What persons purchase and to whom they talk might disclose how much money they make; the political and religious organizations to which they donate; whether they have visited a psychiatrist, plastic surgeon, abortion clinic, or AIDS treatment center; whether they go to gay bars or straight ones; and who are their closest friends and family members. The troves of intimate information the Government can and does obtain using financial records and telephone records dwarfs what can be gathered from cell-site records.¹⁴⁶

Kennedy was correct that the type of information at stake in financial records can be incredibly invasive. This does not mean, though, that the majority was wrong. It does suggest that in a digital age, CSLI is not so unique. The test applied by the Court could apply equally well to a range of records—including those at issue in the foundational third-party cases. How one views the invasiveness of the information

¹⁴¹ See *id.* at 2228 (Kennedy, J., dissenting); *id.* at 2260 (Alito, J., dissenting).

¹⁴² *United States v. Miller*, 425 US 435, 443 (1976), cited and quoted in *Carpenter*, 138 S Ct at 2262 (Gorsuch, J., dissenting).

¹⁴³ *Carpenter*, 138 S Ct at 2262 (Gorsuch, J., dissenting).

¹⁴⁴ *Id.*

¹⁴⁵ *Id.* at 2232 (Kennedy, J., dissenting).

¹⁴⁶ *Id.*

has a lot to do with perspective, underscoring the subjectivity inherent in the Court's approach and illustrating why it will be so difficult to implement going forward.

1. *Broadly applicable.* The *Carpenter* majority claimed that CSLI is different from other kinds of information held by third parties. In its effort to avoid overturning third-party doctrine, however, the majority failed to acknowledge the applicability of its approach to many types of consumer data. The multifactor test applies just as easily to telephony metadata collection which, ostensibly, is the *same type of information* at issue in *Smith*, raising questions about whether *Carpenter* actually overturned third-party doctrine.

Let's start with the number of people implicated, one of the defining factors of CSLI. The same is true of telephony metadata. There are 265.9 million mobile phone users in the United States.¹⁴⁷ These devices generate detailed information about who is in contact with each user, implicating hundreds of millions of people.

Like location data, the volume of communications at issue is enormous and rapidly increasing. In addition to expanding mobile phone use, approximately 224.3 million mobile phone users have Smartphones that run sophisticated applications, which provide further ways for users to communicate with each other.¹⁴⁸ The top app, Facebook, is on 78 percent of all Smartphones.¹⁴⁹ The company has a tremendous reach: in October 2018, the Pew Research Center reported that approximately two-thirds of all adults in the United States use Facebook.¹⁵⁰ Users can send and receive messages to anyone on the network using Facebook Messenger, the mobile phone's browser, the Facebook SMS Service, or third-party apps.¹⁵¹ The company collects

¹⁴⁷ MaXab, *How Many Cell Phone Subscribers in the US 2018* (Media Tech Reviews, Mar 20, 2018), online at <http://www.mediatechreviews.com/how-many-cell-phone-subscribers-the-us>. This number is expected to increase. *Share of Americans Using a Personal Cell Phone Users in 2018, by Age* (Statista), online at <https://www.statista.com/statistics/231612/number-of-cell-phone-users-usa>.

¹⁴⁸ *Smartphone* (Techopedia), online at <https://www.techopedia.com/definition/2977/smartphone>.

¹⁴⁹ MaXab, *How Many Cell Phone Subscribers* (cited in note 147).

¹⁵⁰ John Gramlich, *8 Facts About Americans and Facebook* (Pew Research Center, Oct 24, 2018), online at <http://www.pewresearch.org/fact-tank/2018/10/24/facts-about-americans-and-facebook> (reporting that 68 percent of American adults use Facebook, with 74 percent visiting the site daily).

¹⁵¹ *Six Ways to Send Facebook Messages Without Messenger* (Dr. Fone), online at <https://drfone.wondershare.com/facebook/send-facebook-messages-without-messenger.html>.

logs of all communications—including data on individuals who do not even have a Facebook account, gleaned from their inclusion in users' contact lists.¹⁵² Facebook is only one company in a rapidly growing social media market in which some 3 billion people worldwide (approximately one-third of the population on earth) are expected to take part by 2021.¹⁵³

The information that can be extracted from the associated telephony metadata can be far more invasive than location data. Even one-off communications can reveal hobbies, interests, relationships, and beliefs. Patterns impart degrees of intimacy. Using network analytics, relationships can be mapped into nodes and networks and analyzed.¹⁵⁴ Communities previously hidden from view can be detected.¹⁵⁵ Power structures and levels of influence can be identified.¹⁵⁶ Social networks, of course, are not static. Future interactions, col-

¹⁵² Gabriel J. X. Dance, Michael LaFoergia, and Nicholas Confessore, *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants* (NY Times, Dec 18, 2018), online at <https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html?action=click&module=Top%20Stories&pgtype=Homepage>; Kurt Wagner, *This Is How Facebook Collects Data on You Even if You Don't Have an Account* (Recode, Apr 20, 2018), online at <https://www.recode.net/2018/4/20/17254312/facebook-shadow-profiles-data-collection-non-users-mark-zuckerberg>.

¹⁵³ *Mobile Social Media—Statistics & Facts* (Statista), online at <https://www.statista.com/topics/2478/mobile-social-networks>.

¹⁵⁴ See Greg Statell, *How the NSA Uses Social Network Analysis to Map Terrorist Networks* (Digital Tonto, June 12, 2013), online at <https://www.digitaltonto.com/2013/how-the-nsa-uses-social-network-analysis-to-map-terrorist-networks>; Amir Gandomi and Murtaza Haider, *Beyond the Hype: Big Data Concepts, Methods, and Analytics*, 35 *Int'l J. Info Management* 137 (2015); Julia Heidemann, Mathias Klier, and Florian Probst, *Online Social Networks: A Survey of a Global Phenomenon*, *Computer Networks* 56 *Computer Networks* 3866 (2012).

¹⁵⁵ Charu C. Aggarwal, *An Introduction to Social Network Data Analytics* (Springer, 2011). See also *Community Detection Algorithms* (Neo4j), online at <https://neo4j.com/docs/graph-algorithms/current/algorithms/community>.

¹⁵⁶ Degree centrality counts how many neighbors a node within a network has. *Degree Centrality* (Network Science), online at <https://www.sci.unich.it/~francesc/teaching/network/degree.html>. Betweenness centrality reveals how information flows through a network—that is, nodes that provide a bridge between different parts of the network. *The Betweenness Centrality Algorithm* (Neo4j), online at <https://neo4j.com/docs/graph-algorithms/current/algorithms/betweenness-centrality>. Closeness centrality indicates the most efficient spread of information through a network, that is, how close they are to the relevant nodes. *The Closeness Centrality Algorithm* (Neo4j), online at <https://neo4j.com/docs/graph-algorithms/current/algorithms/closeness-centrality>. Eigenvector centrality looks at the importance of a node in terms of the importance of nodes with which it is linked. It is a way of ranking importance in a network. *Eigenvector Centrality* (Network Science), online at <https://www.sci.unich.it/~francesc/teaching/network/eigenvector.html>. See also Lei Tang and Huan Liu, *Community Detection and Mining in Social Media*, in Jiawei Han et al, eds, *Synthesis Lectures on Data Mining and Knowledge Discovery* 1–137 (Morgan and Claypool, 2010).

laboration, and influence can be estimated, based on latent data.¹⁵⁷ Using regression equations and machine learning, observers can predict what people are likely to do, *even when the subjects themselves are not aware of their patterns*.¹⁵⁸ The more information that is collected, the more accurate such predictions become.¹⁵⁹

Massive amounts of data are being produced by social media companies such as Facebook, Twitter, and WhatsApp. That information already has been used to predict influenza, stock market trends, and customer attitudes, as well as spiritual beliefs and political views.¹⁶⁰ Over the past five years, there has been an explosion in scholarly articles and book chapters focused on exploiting social network analytics in the criminal context as well.¹⁶¹ The technique can be effective in identifying critical nodes, which law enforcement can then target to disrupt criminal enterprises.¹⁶²

¹⁵⁷ See David Liben-Nowell and Jon Kleinberg, *The Link Prediction Problem for Social Networks*, in Donald Kraft, ed, *Proceedings of the Twelfth International Conference on Information and Knowledge Management* 556 (ACM, 2003).

¹⁵⁸ See Jianqing Fan, Fang Han, and Han Liu, *Challenges of Big Data Analysis*, 1 Natl Sci Rev 293, 293 (2014).

¹⁵⁹ Id at 297–98.

¹⁶⁰ Id at 296–97.

¹⁶¹ See, for example, Giulia Berlosconi, *Social Network Analysis and Crime Prevention*, in Benoit Le Clerc and Ernesto U. Savano, eds, *Crime Prevention in the 21st Century* 129 (Springer, 2017); Morgan Burcher, *Social Network Analysis as a Tool for Criminal Intelligence*, 21 Trends in Organized Crime 278 (2018); David A. Bright, Catherine Greenhill, and Natalya Levenkova, *Dismantling Criminal Networks: Can Node Attributes Play a Role?*, in Carlo Morselli, ed, *Crime and Networks* 148 (Routledge, 2013); Francesco Calderoni, *Identifying Mafia Bosses from Meeting Attendance*, in Anthony J. Masys, ed, *Networks and Network Analysis for Defence and Security* 27 (Springer, 2014); Francesco Calderoni, *Predicting Organized Crime Leaders*, in Gisela Bichler and Aili E. Malm, eds, *Disrupting Criminal Networks: Network Analysis in Crime Prevention* 89 (First Forum, 2015); David Décary-Héту, *Information Exchange Paths in IRC Hacking Chat Rooms*, in Carlo Morselli, ed, *Crime and Networks* 218 (Routledge, 2014); Paul A. C. Duijn and Peter P. H. M. Klerks, *Social Network Analysis Applied to Criminal Networks: Recent Developments in Dutch Law Enforcement*, in Anthony J. Masys, ed, *Networks and Network Analysis for Defence and Security* 121 (Springer, 2014); Jenny C. Piquette, Chris M. Smith, and Andrew V. Papachristos, *Social Network Analysis of Urban Street Gangs*, in Gerben Bruinsma and David Weisburd, eds, *Encyclopedia of Criminology and Criminal Justice* 4981 (Springer, 2014); David A. Bright et al, *Networks Within Networks: Using Multiple Link Types to Examine Network Structure and Identify Key Actors in a Drug Trafficking Operation*, 16 Global Crime 219 (2015).

¹⁶² Burcher, 21 Trends in Organized Crime at 278 (cited in note 161). Instead of focusing on low-level criminals, for instance, law enforcement could use metadata to identify the key members of Mara Salvatrucha (MS-13), a violent criminal gang formed in the 1980s in Los Angeles. They could then call those individuals in for questioning, subject them to more detailed scrutiny, put out false information about them to undermine their position within the organization, or prosecute them in an effort to imprison them and thus interrupt the network.

Like location data, the resource constraints in obtaining telephony metadata and subjecting it to targeted queries or sophisticated algorithms are rapidly diminishing. In the past, it might not have been possible to record most, or even all, of an individual's relationships and communications. Now, not only is it possible, but big data and massive computing power have put technology in hyperdrive. What might have taken days, or even months, of analysis, can now be done at the push of a button.

All of this information, moreover, like location data, is retroactive in that it relates to communications in the past. And while CSLI provides near-perfect recall, telephony metadata reproduce *exactly* what happened, recording at precisely what time, on which date, an individual was in contact with which number or entity. And it is available for weeks, months, or even years at a time. The only limit is that of the cell phone provider or the app itself.

By all the factors laid out by the Court in *Carpenter*, pen register and trap and trace data prove equally, if not even more, invasive than location information. If the intent of the Court is to be believed (i.e., to restore some sort of equilibrium between society and law enforcement), then such records *must* be included in the exception to the exception. A similar argument could be made about banking records, which were at issue in *Miller*.¹⁶³

In *Carpenter*, the Court tried to draw a distinction between location information and telephony metadata based on voluntariness.¹⁶⁴ This

¹⁶³ Banking records implicate nearly every American. The volume of information held by banks is enormous and can be extremely revealing in terms of individuals' private lives. As technology has progressed, fewer and fewer resource constraints exist for obtaining, and analyzing, significant amounts of data. Banking records are just as precise as telephony metadata, and they can be obtained for activity that occurred decades before. As with mobile telephones, it is not an option in the current age not to have a bank account; nor is it voluntary, in any sense of the word, not to confide certain information to banks—particularly information that is required by statute. Banking records look remarkably like location data, in terms of the factors laid out by the Court in *Carpenter*. See also *Carpenter*, 138 S Ct at 2233 (Kennedy, J, dissenting) ("Financial records are of vast scope. Banks and credit card companies keep a comprehensive account of almost every transaction an individual makes on a daily basis. . . . And the decision whether to transact with banks and credit card companies is no more or less voluntary than the decision whether to use a cell phone."); id at 2224 (arguing that the Court has drawn an "unprincipled and unworkable line between cell-site records on the one hand and financial and telephonic records on the other.").

¹⁶⁴ *Carpenter*, 138 S Ct at 2220 (majority). See also *Carpenter*, 138 S Ct at 2227–30 (Kennedy, J, dissenting) (noting that by voluntarily conveying information to the respective companies, the defendants in *Miller* and *Smith* "assumed the risk that the information would be divulged to police," and arguing that *Carpenter* similarly lacked any reasonable expectation of privacy in CSLI).

assertion, however, does not survive scrutiny. For the distinction to hold, one of two things would have to be true: either having a phone must be optional, or providing the numbers to the company must be at the user's discretion. Neither is accurate. As for the former, 99.28 percent of adults aged eighteen to twenty-nine have a mobile phone.¹⁶⁵ As the Court recognized in *Riley*, the devices have become an indispensable part of living in society. In regard to the latter, users cannot mask the numbers that they call. Companies must have this information to connect them to the other party, and vice versa. Providing it to the company is not voluntary in any sense of the word.¹⁶⁶

In sum, the factors considered by the Court as (ostensibly) unique to CSLI apply equally well to telephony metadata—and banking data¹⁶⁷—making the claim that the Court left *Miller* and *Smith* untouched ring somewhat hollow.¹⁶⁸ Applying the *Carpenter* test, it is difficult to see any distinction between many types of third-party documents.¹⁶⁹ With this in mind, Justice Alito's critique, that the Court's "revolutionary" holding fractured the "pillars of Fourth Amendment law," seems about right.¹⁷⁰

2. *Unknowable*. Not only do many different kinds of digital records meet the test laid out in *Carpenter*—including the records at issue in the foundational third-party cases—but it is impossible to say with any certainty how the courts will apply the logic adopted. The Court's approach requires a case-by-case analysis in which unanswerable questions are presented. Because it is based on a bad analogy and highly indeterminate concepts, such as voluntariness and reasonableness, it will prove difficult to implement in any sort of consistent manner.¹⁷¹

¹⁶⁵ *Share of Americans Using a Personal Cell Phone Users in 2018, by Age* (Statista) (cited in note 147).

¹⁶⁶ A third possibility might be that telephone users voluntarily call *certain numbers*. This argument, though, is at odds with the Court's acknowledgment in *Riley* that a phone is concomitant to living in society. It makes no sense to then turn around and say that it is *not* actually necessary to use it to be part of that society.

¹⁶⁷ See note 163.

¹⁶⁸ As Justice Gorsuch laments, *Carpenter* only made matters worse, placing "*Smith* and *Miller* on life support and supplement[ing] them with a new and multilayered inquiry that seems to be only *Katz*-squared." *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting).

¹⁶⁹ The same could be said of educational assessments, employment records, and the like. So, too, does it apply to other forms of metadata, such as IP addresses, websites visited, or text and email contacts.

¹⁷⁰ *Carpenter*, 138 S. Ct. at 2247 (Alito, J., dissenting).

¹⁷¹ See also *id.* at 2261 (recognizing that the reasoning of the majority will require the Court to take every case and subject each type of information to qualifications, further entangling Fourth Amendment jurisprudence).

a) Which records? Like many of the lower courts that confronted CSLI, the *Carpenter* court emphasized voluntary assumption of risk. In doing so, it perpetuated the false analogy between informant doctrine and third-party business records. As explained above, this conflation subordinates the constitutional right to security in “papers”; ignores the difference between admitting illegal activity to a coconspirator and engaging in a legal, contractual relationship; assumes consent for a limited purpose means consent to government surveillance; and sidesteps the extent to which commercial relations are an essential part of ordinary life. It is an awful analogy.

The Court discussed two kinds of potentially compelled (or voluntary) actions: use of a mobile phone, and the generation of location records *while* using the phone.¹⁷² It did not provide guidelines for how to think about these two categories going forward; nor did it address their relative importance or how to gauge greater or lesser degrees of compulsion.

Consider, first, what could be termed device-use compulsion. Noting that carrying a phone is not an option in the contemporary context, the Court neglected to enquire (*a*) whether other mobile devices are “voluntarily” used, or (*b*) whether records connected to the technologies contained on (specifically) mobile telephones fall within the exception.

For (*a*), a colorable case could be made that *many* other kinds of nontelephonic mobile devices are critical in the contemporary environment. The computer on which I am writing this article is essential to my work. It would be almost impossible to undertake modern legal scholarship without one. The same could be said of the use of computers in many different fields. As a matter of private use, computers are used for everything from shopping, entertainment, and scheduling dates with friends, to cooking, buying bus, train, and plane tickets, and planning vacations. They have become a pervasive part of ordinary life. In 2016, the American Community Survey determined that 89 percent of American households have a computer, making it, in the Census Bureau’s estimation, “a common feature of everyday

¹⁷² Although I do not here go into detail, it is worth noting that the way in which the Court referred to compulsion versus voluntary action departs significantly from philosophical treatment of these areas. In *Carpenter*, what the Court appears to mean by these concepts relates to technical requirements of participation in modern society.

life.”¹⁷³ Under *Carpenter*, does this mean that Fourth Amendment protection extends to records associated with computers?

For that matter, are *all* electronic devices, which store digital information, (in)voluntary in a modern era? If not, how do we distinguish between those that are and those that are not? The Court provides no basis on which to calculate which devices are coerced by the circumstances of life. What level of necessity is required? How pervasive must they be? How will voluntariness be determined? By the number of people using the technology? By the percentage of the population? *Carpenter* clarifies none of this.

Perhaps, turning to (b), voluntariness has to do not with the phone itself, but with the specific function the phone performs. If so, then it is not clear if the Court’s reasoning is limited to the traditional place of the phone in contacting others in society—for personal or business purposes—or whether it has something to do with the *types of technologies* typically contained on the telephone. For the former, the primary use is found in the function of the device *as a phone*. So, in order to exist in modern life (i.e., to be part of society), perhaps the underlying theory is that we must carry one in order to be in contact with others. Or perhaps it is just use of the phone when it operates *as a tracking device* that qualifies for protection. But if that is the case, then all photographs that include geolocational metadata, and applications like Yelp, Flixter, or Foursquare, which rely on location information, also are protected. What if the voluntariness is not limited to location data? If use of the mobile telephone is not voluntary (under *Riley* and *Carpenter*), for reasons related to taking part in society, then wouldn’t this encompass other functions the phone performs, such as social media?

And who is to make the voluntariness determination? From *Carpenter*, it appears that the Court has this responsibility. But judges’ experiences will shape the answer. For some, social media may be a complete mystery, not at all part of their daily interactions. For others, Facebook may be an indispensable part of their social life. For those of a younger generation, who see Facebook as something that their grandparents do, their world may revolve around Snapchat, Instagram, and YouTube. For them, participation is not voluntary. It

¹⁷³ Camille Ryan, *Computer and Internet Use in the United States: 2016* (US Census Bureau, Aug 8, 2018), online at <https://www.census.gov/content/dam/Census/library/publications/2018/acs/ACS-39.pdf>.

is required for participating in, and being part of, society.¹⁷⁴ Justices may see it quite differently. The result will further entrench the judiciary in policy determinations.

Perhaps what the Court meant in *Carpenter* was that voluntariness relates not to the device, but to the production of records themselves, a sort of record-creation compulsion: that is, users do not have a meaningful choice whether to convey their location to a service provider.¹⁷⁵ But this is a distinctly odd way to think about what one does when one uses a mobile device. The argument is that by having the device, you are locked into transmitting your location to the internet service provider (ISP) to get service. But by using the device in certain ways—ways equally central to the role of the device in modern society—you also are locked into transmitting all sorts of different kinds of data.

Consider, for instance, Internet Protocol (IP) addresses, which are dynamically assigned to a device when you go online. When you are at home, it is assigned by your ISP. But that number can change as quickly as a power outage, when the server is turned off. As soon as you leave home and use a different network to go online, a new (temporary) IP address is assigned.¹⁷⁶ You can try to mask your IP address by using a Virtual Private Network (VPN) Service, the Onion Router (Tor) (a network that allows users to disguise their identity by using multiple servers and encryption), a proxy server, or free/public WiFi.¹⁷⁷ But most users are not this sophisticated and are left with the default IP address, which reveals their location.

So, under *Carpenter*, does this mean that IP addresses are included? If so, then how about Uniform Resource Locators (URLs)? By using a browser to visit web pages, you may (unwittingly) record the URLs in your browser cache, the operating system cache, the router cache, *and* the ISP cache.¹⁷⁸ Are you providing that information voluntarily or not? If the carrying of the phone is not voluntary, and the access

¹⁷⁴ See discussion in note 172.

¹⁷⁵ *Carpenter*, 138 S Ct at 2220 (majority).

¹⁷⁶ See, for example, *My IP Address Is*: (WhatIsMyIPAddress.com), online at <https://whatismyipaddress.com>.

¹⁷⁷ *How to Hide Your IP Address* (WhatIsMyIPAddress.com), online at <https://whatismyipaddress.com/hide-ip>.

¹⁷⁸ Maneesha Wijesinghe, *What Happens When You Type a URL in the Browser and Press Enter?* (Medium, Apr 25, 2017), online at <https://medium.com/@maneesha.wijesinghe1/what-happens-when-you-type-an-url-in-the-browser-and-press-enter-bb0aa2449c1a>.

it provides to the online world similarly compelled, then it seems as though it ought to be considered within the domain of the Fourth Amendment. As in the case of CSLI, it is simply a by-product of actions you take in the real world—in this case, the decision to go online.

With so many different questions left unanswered by *Carpenter* about how to think about device-use compulsion and record-production compulsion, it will be up to the courts to answer them and to gauge voluntariness—entrenching courts ever more firmly in the policy-making realm and leading to unpredictable results.

b) *When is a search reasonable?* In *Carpenter*, the Court held that seven days of CSLI required a warrant. For Justice Kennedy, this (apparently arbitrary) distinction was “illogical” and would “frustrate principled application of the Fourth Amendment.”¹⁷⁹ Worse, the Court had collapsed its determination that obtaining CSLI constituted a search and the analysis of whether or not it was “reasonable.”¹⁸⁰ For Kennedy, the proper approach would have been to remand the case to address the “important and difficult issues” that marked the second query.¹⁸¹ Underlying his critique was the Court’s failure to address the role of technology not just in determining whether a search had occurred, but whether it was one that society was prepared to recognize as reasonable. That lack of precision regarding the role of technology raised myriad questions that will further frustrate efforts to implement the decision in a reliable manner.

The majority in *Carpenter* went some length to note that “seismic shifts in digital” technologies had created CSLI—a form of information hitherto unknown.¹⁸² When confronted by “new concerns wrought by digital technology,” the Court had to be careful not to reflexively extend precedent.¹⁸³ The majority was critical of the gov-

¹⁷⁹ *Carpenter*, 138 S Ct at 2224 (Kennedy, J, dissenting) (“[T]he Government crosses a constitutional line when it obtains a court’s approval to issue a subpoena for more than six days of cell-site records in order to determine whether a person was within several hundred city blocks of a crime scene.”).

¹⁸⁰ Id at 2235 (“Having concluded . . . that the Government searched Carpenter when it obtained cell-site records from his cell phone service providers, the proper resolution of this case should have been to remand for the Court of Appeals to determine in the first instance whether the search was reasonable.”).

¹⁸¹ Id.

¹⁸² Id at 2219 (majority).

¹⁸³ *Carpenter*, 138 S Ct at 2222.

ernment, and Kennedy, for failing to grasp the implications of the “new technology.”¹⁸⁴ There was a “world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information” now available.¹⁸⁵ The Court also had to be mindful “of more sophisticated [technologies] that were already in use or in development.”¹⁸⁶

The majority’s language suggested that the *novelty* of the technology mattered—that is, the extent to which the technology in question departed from previous circumstances.¹⁸⁷ It was not clear whether the chief complaint was the impact of new technologies or the creation of new types of records.¹⁸⁸ Neither, as a limitation going forward, is persuasive.

While the factors laid out in *Carpenter* underscored the impact of one “new” technology that had resulted in near-universal 24/7 location tracking, in other situations, perhaps the prior limitation is merely one of storage capacity, or battery life—or whether information is shared, an algorithm created, or an old technology applied to a new context. Perhaps it has nothing to do with the novelty of the technology in question.

If it is only “new” technologies, how do we draw the line? This is a hard question. The *Carpenter* court stated, for example, that its decision did not reach traditional cameras.¹⁸⁹ But a camera with still image capabilities and limited memory is a different animal than one with video capabilities and virtually unlimited memory. Still more are these different from cameras with infrared vision, remote rotation, and powerful zoom functions, or that capture not just video, but audio as well. Yet more distant are cameras paired with biometric identification systems, or linked to extensive online databases providing de-

¹⁸⁴ Id at 2219.

¹⁸⁵ Id.

¹⁸⁶ Id at 2218. See also id at 2223 (“As Justice Brandeis explained in his famous dissent, the Court is obligated . . . to ensure that the ‘progress of science’ does not erode Fourth Amendment protections.”) (citations omitted).

¹⁸⁷ See, for example, *Carpenter*, 138 S Ct at 2217 (comparing tailing a suspect “[p]rior to the digital age” to the contemporary use of technology).

¹⁸⁸ On the one hand, the Court focused on the technology itself, as well as the state of the technology. Id at 2219–20. On the other hand, it observed “a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carries today,” referring to CSLI as “an entirely different species of business record.” Id at 2219, 2222.

¹⁸⁹ Id at 2220.

tailed, personally identifiable information. Even further are such cameras mounted on a drone and not tied to one place. Nevertheless, the government considers all of these to be one technology, at times not even deigning to issue a new privacy impact assessment when the nature of the recordings, capacity, or capabilities change.¹⁹⁰

Or perhaps the Court, applying a rule of functional equivalence, would only include technologies that allow for the constructive search of what was traditionally found to be unreasonable when subject to a physical search. The Court has used this approach in related areas. The protections of the home, for instance, extend to anywhere that functions in the same manner, regardless of whether it amounts to an actual “house.”¹⁹¹

Functional equivalence has been particularly important for giving courts latitude to take account of new technologies. Air travel did not exist at the founding, but as individuals began using airports, the Court extended the border exception to the “functional equivalent” of the border: interior airports employed as ports of entry.¹⁹² Where technology has made it possible to conduct a search that otherwise would require entry and thereby exposes the home to inspection, the Court again has applied a rule of functional equivalence.¹⁹³ Accord-

¹⁹⁰ The Department of Justice’s (DOJ) Federal Bureau of Investigation operates the Next Generation Identification–Interstate Photo System (NGI-IPS) and an internal unit called Facial Analysis, Comparison and Evaluation (FACE) Services. Although DOJ developed a Privacy Impact Assessment in 2008 for NGI-IPS, it did not update it as the system integrated new technologies, nor did it publish a PIA on FACE Services. US Government Accountability Office, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy* (May 16, 2016), online at <https://www.gao.gov/products/GAO-16-267>. See also Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 Minn L Rev 407 (2012) (noting the absence of PIAs despite the addition of new technologies).

¹⁹¹ See, for example, *United States v. Dunn*, 480 US 294, 301 n 4 (1987) (defining curtilage as an area “harbor[ing] those intimate activities associated with domestic life and the privacies of the home.”); *United States v. McDonald*, 335 US 451 (1948) (regarding a locked common area of a rooming house to be within the Fourth Amendment).

¹⁹² *Torres v. Puerto Rico*, 442 US 465 (1979) (holding that the search of an individual arriving in the Commonwealth of Puerto Rico from the United States did not satisfy Fourth Amendment requirements because there was no functional equivalent to an international border of the United States); *Almeida-Sanchez v. United States*, 413 US 266, 273 (1973) (“[A] search of the passengers and cargo of an airplane arriving at a St. Louis airport after a nonstop flight from Mexico City would clearly be the functional equivalent of a border search.”).

¹⁹³ See also Barnett and Bernick, 107 Georgetown L J at 3 (cited in note 10) (arguing for a commitment to “the functions, purposes, goals, [and] aims” of constitutional clauses in ascertaining the meaning of the Constitution); Paul Ohm, *The Many Revolutions of Carpenter*, Harv J L & Tech at 34 (forthcoming 2019), online at <https://osf.io/preprints/lawarxiv/bsedj/download> (articulating a rule of technological equivalence as: “The Court in the past has

ingly, in *United States v Knotts*, the Court considered a beeper tracked along a public road to fall outside Fourth Amendment protections; but then, in *United States v Karo*, the Court held that the moment at which a beeper crossed the threshold, a search had occurred.¹⁹⁴ Whether or not law enforcement actually entered the domicile, they could infer that the can of ether being tracked was inside.¹⁹⁵ Similarly, in *Kyllo*, the Court determined that the use of a thermal imaging device to read the heat signatures of exterior walls constituted a search within the meaning of the Fourth Amendment.¹⁹⁶ Justice Scalia, writing for the Court, rejected the government's argument that it was constitutional because the thermal device did not uncover "intimate details." Using it violated a categorical protection: "In the home, our cases show, all details are intimate details, because the entire area is held safe from prying government eyes."¹⁹⁷ Lower courts have adopted the same approach for other technologies that reveal what happens inside the home.¹⁹⁸

In *Carpenter*, the Court favorably cited back to *Kyllo*, acknowledging "[a]s technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes," the Court has tried to ensure the protections guaranteed at the founding.¹⁹⁹ In dicta, the Court went on to accept that the examination of digitized letters would constitute a search. It considered email "a sensible ex-

held that information in a particular, traditional privacy context is protected by the Fourth Amendment. A technology produces information that is a modern-day equivalent to the information produced in the traditional context of step one. The information in the modern context is also protected by the Fourth Amendment.").

¹⁹⁴ *United States v Karo*, 468 US 705, 715 (1984) ("[H]ad a DEA agent thought it useful to enter the Taos residence to verify that the ether was actually in the house and had he done so surreptitiously and without a warrant, there is little doubt that he would have engaged in an unreasonable search within the meaning of the Fourth Amendment. . . . [T]he result is the same where, without a warrant, the Government surreptitiously employs an electronic device to obtain information that it could not have obtained by observation from outside the curtilage of the house."); *Knotts*, 460 US at 281 ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

¹⁹⁵ *Karo*, 468 US at 714–15. See also *Kyllo v United States*, 533 US 27, 36 (2001) (Scalia, J, for the majority) (stating that in *Karo* "the police 'inferred' from the activation of a beeper that a certain can of ether was in the home.").

¹⁹⁶ *Kyllo*, 533 US at 29.

¹⁹⁷ *Id.* at 37–38. See also *Florida v Jardines*, 569 US 1 (2013).

¹⁹⁸ See *Naperville Smart Meter Awareness v Naperville*, 900 F3d 521 (7th Cir 2018).

¹⁹⁹ *Carpenter*, 138 S Ct at 2214.

ception,” an example of “the modern-day equivalents of an individual’s own ‘papers’ or ‘effects.’”²⁰⁰

The challenge in understanding *Carpenter* in light of the rule of functional equivalence is that *Miller* and *Smith* eviscerated the protections afforded to “papers.” Yet it appears that *Carpenter* eliminated third-party doctrine in all but name. So, going forward, if we apply the rule of functional equivalence, how do we understand “papers,” or for that matter, “effects,” in a digital age? Do text messages count? Or instant messages? Or chats in multiplayer online games?

Perhaps the technologies that allow for constructive search of traditional categories provide a minimum. If so, how far out does the new rule go? Again, in dicta, the Court noted that whatever rule the Court adopts must take account of increasingly sophisticated technologies.²⁰¹ But how sophisticated do they need to be? Which (new) technologies constitute a search, but do not fall afoul of the reasonableness determination? How is the decision to be reached? In collapsing its analysis, the Court failed to provide a reliable way for the lower courts to draw a line, even as it cemented them into a policy-making realm.²⁰²

IV. RESIDUAL PROPERTY RIGHTS

While *Carpenter* unquestionably represents a departure from familiar doctrinal landmarks, it leaves us at somewhat of a loss. How should we chart a future course concerning personal, digital information held by companies in a post-*Katz*, post-*Miller* and *Smith*, post-*Carpenter* era?

Consistent with the previous discussion, the voluntary assumption of risk is a nonstarter. Continued use of it will confound efforts to provide consistency across the circuits. In addition to the analogical fallacies at work in the decision, *Carpenter* fails to provide guidance on device-use compulsion and record-creation compulsion, both of

²⁰⁰ Id at 2222, citing and quoting id at 2230 (Kennedy, J, dissenting), citing *United States v Warshak*, 631 F3d 266, 283–88 (6th Cir 2010).

²⁰¹ *Carpenter*, 138 S Ct at 2218–19 (majority).

²⁰² Gorsuch raised myriad further questions that bedevil the holding. See *Carpenter*, 138 S Ct at 2266–67 (Gorsuch, J, dissenting) (concluding, “In the end, our lower court colleagues are left with two amorphous balancing tests, a series of weighty and incommensurable principles to consider in them, and a few illustrative examples that seem little more than the product of judicial intuition.”).

which, in any event, rely on complex policy determinations. This approach further draws courts into value judgments, running the risk that the public will lose confidence in the judiciary.

No better does the “novel technology” approach fare. As argued above, it is beset by hard questions, including how to understand what counts as a “new” technology. As digitization becomes widespread, this approach will become less and less relevant. New forms of information that previously did not even exist will become available, which implicates interests ostensibly protected by the Fourth Amendment.

Given these potentially insuperable difficulties, the judiciary ought seriously to consider returning to constitutional first principles: a property-rights-based approach. As the Supreme Court observed, “One virtue of the Fourth Amendment’s property-rights baseline is that it keeps easy cases easy.”²⁰³ Just as the Court in *Karo* and *Kyllo* adopted a rule of functional equivalence in regard to the home, it can embrace a similar approach to papers. A central question then becomes which digital documents come within constitutional protections. A property-rights approach helps to answer that question. This is the path favored by Gorsuch in *Carpenter*.²⁰⁴ He drew on bailment and positive law, asking what kind of legal interest would be sufficient to generate ownership rights and what sources of law would help to determine the answer.²⁰⁵ In the balance of this article, I identify important reasons why the Court should consider adopting a property-rights approach.

A. GENERATION, OWNERSHIP, AND POSSESSION

As the dissents in *Carpenter* observed, the Fourth Amendment has at its core a right in one’s own property that stems from the inclusion

²⁰³ *Florida v. Jardines*, 569 US 1, 12 (2013).

²⁰⁴ Gorsuch envisioned three possible futures: the Court could doggedly hold to precedent, it could reevaluate the world post-*Katz*, or it could chart a new course. *Carpenter*, 138 S Ct at 2262 (Gorsuch, J, dissenting). The first amounted to “A doubtful application of *Katz* that lets the government search almost whatever it wants whenever it wants.” *Id* at 2264. The second was problematic, as the issue was *Katz* in the first place. *Id*. The third offered the most promising way forward. See *id* at 2267–72.

²⁰⁵ *Id* at 2268. See also William Baude and James Stern, *The Positive Law Model of the Fourth Amendment*, 129 Harv L Rev 1821 (2016) (arguing that a Fourth Amendment search only occurs where a private party could not lawfully perform the action undertaken by the government); Richard Re, *The Positive Law Floor*, 129 Harv L Rev F 313 (2016) (arguing in juxtaposition to Baude and Stern that positive law creates a floor, not a ceiling, on Fourth Amendment protections).

of “*their* persons, houses, papers, and effects.”²⁰⁶ The text does not refer to a right exercised in relation to the property of others.²⁰⁷ It thus requires the Court to ask *whose* property was searched.

This approach is consistent with *Katz*, which, as the Supreme Court has recognized, did not extinguish the role of property rights in the Fourth Amendment.²⁰⁸ Even the “legitimation” of *Katz*’s “expectations” test(s) “must have a source outside the Fourth Amendment, either by reference to concepts of real or personal property or to understandings that are recognized and permitted by society.”²⁰⁹ From this, we can conclude that even under existing precedent, *ownership rights still matter*.

Can individuals have an ownership interest in *digital* documents or records? The answer here is plainly yes. Federal statutes routinely treat “data,” “digital data,” “digital content,” and “digital assets” as property.²¹⁰ The same is true at a state level: since 2013, forty-six states have enacted laws governing access to digital assets ranging from email, social media accounts, and microblogging to electronically stored information.²¹¹ State statutes also create a private right of action to redress the unauthorized collection, retention, disclosure,

²⁰⁶ US Const, Amend IV; *Carpenter*, 138 S Ct at 2260 (Alito, J, dissenting) (The Fourth Amendment protects “*their* persons, houses, papers, and effects”—not those of others) (emphasis in original); id at 2235 (Thomas, J, dissenting) (“The Fourth Amendment guarantees individuals the right to be secure from unreasonable searches of ‘*their* persons, houses, papers, and effects.’”) (emphasis in original); id at 2227 (Kennedy, J, dissenting) (“the Fourth Amendment’s protections must remain tethered to the text of that Amendment, which, again, protects only a person’s own ‘persons, houses, papers, and effects.’”).

²⁰⁷ *Carpenter*, 138 S Ct at 2227 (Kennedy, J, dissenting).

²⁰⁸ *Rakas v Illinois*, 439 US 128, 143–44 n 12 (1978) (“Expectations of privacy protected by the Fourth Amendment . . . need not be based on a common-law interest in real or personal property, or on the invasion of such an interest. These ideas were rejected [in]. . . *Katz*. [.] But by focusing on legitimate expectations of privacy in Fourth Amendment jurisprudence, the Court has not altogether abandoned use of property concepts in determining the presence or absence of the privacy interests protected by that Amendment.”). See also *Carpenter*, 138 S Ct at 2227 (Kennedy, J, dissenting) (writing, “‘property concepts’ are . . . fundamental ‘in determining the presence or absence of the privacy interests protected by’” the Fourth Amendment and that even in *Katz*, the property-based concept remained).

²⁰⁹ *Rakas*, 439 US at 144 n 12.

²¹⁰ See, for example, *Other Digital Content* (Copyright.gov), online at <https://www.copyright.gov/registration/other-digital-content>; Health Insurance Portability and Accountability Act of 1996 (HIPPA), Pub L No 104-191, 110 Stat 1936.

²¹¹ *Access to Digital Assets of Decedents* (National Conference of State Legislatures, Dec 3, 2018), online at <http://www.ncsl.org/research/telecommunications-and-information-technology/access-to-digital-assets-of-decedents.aspx>.

and destruction of biometric data.²¹² As a matter of Supreme Court jurisprudence, the rule of functional equivalence applies: at a minimum, the types of matters that historically would have been protected, if digitized, fall within the Fourth Amendment. Scholars, too, appear to be nearly universal in their agreement.²¹³ To the extent, then, that third-party doctrine eviscerated a foundational right to security of one's digital personal or commercial papers, it undermined rights secured at the founding.

Papers encompass the intimacies of life that arise, at least in part, from an individual's actions and decisions: writing a letter, keeping a diary, dictating a memo, engaging in business transactions, and going about one's daily business. The fact that they are held on parchment or online matters naught. Such documents would not exist *but for* the actions of the owner. The (traditional) position of the letter-writer, diary-keeper, or individual engaged in commercial activity matters. Digital records mirror what happens in the world—what people think, say, do, and believe. They arise from the right-holder's actions.

The question, "who owns this information?" relates not just to the concept of ownership itself, but also to the relationship between the holder of the right and others. This leads to a critical insight: *If it is up to an individual to determine with whom information generated by them is shared, then that person holds the original right.* An individual could not contract to provide the information without power over the data.²¹⁴ Under such circumstances, the right at issue can be understood, at least in part, according to the actions of the right-holder.

²¹² See, for example, the Biometric Information Privacy Act, 740 ILCS 14/1 et seq, which was recently upheld in *Rosenbach v Six Flags Entertainment Corp.*, 2019 WL 323902 (Ill).

²¹³ See Pamela Samuelson, *Privacy as Intellectual Property?*, 52 Stan L Rev 1125, 1130 (arguing that people think about personal data as property); Megan Blass, *The New Data Marketplace: Protecting Personal Data, Electronic Communications, and Individual Privacy in the Age of Mass Surveillance through a Return to a Property-Based Approach to the Fourth Amendment*, 42 Hastings Const L Q 577, 592 (2015) ("Personal data and electronic communications . . . are an extension of the individual and the home. . . [They] are closely tied to the privacies of life or intimate activities that are traditionally associated with the home . . . and deserve continued protection under the Fourth Amendment."); Wendy K. Mariner, *Reconsidering Constitutional Protection for Health Information Privacy*, 18 U Pa J Const L 975, 978 (2016) (arguing that the dependence on sharing personal health information electronically should be reflected in Fourth Amendment doctrine); Edina Harbinja, *Legal Nature of Emails: A Comparative Perspective*, 14 Duke L & Tech Rev 227 (2016) (arguing that email accounts "can be analogized to the paper on which letters are written.").

²¹⁴ See Wesley Newcomb Hohfeld, *Fundamental Legal Conceptions as Applied in Judicial Reasoning* 10 (Yale, 1923) (Walter Wheeler Cook, ed) (articulating the juridical incidents (i.e., privileges, claims, powers, and immunities) embedded in the concept of a right).

Consider freedom of movement. It is the right-holder's exercise of this freedom that generates location data, which would not exist *but for* the individual's actions: purchasing a mobile device, charging it, turning it on, carrying it, and going to particular places at particular times. If the individual did not have an original right to the information, he or she could not contract to share it with an ISP. It would not be hers to provide. However, it clearly *is* hers to provide.

Simultaneously, the right-holder has a claim on the company with whom she contracts to provide communications in a timely, efficient, and consistent manner. That is the whole point of having a mobile device: to be able to use the telephone whenever and wherever one chooses. This claim-right *does not exist independent of the individual's contractual relationship with the company*. The salient question is whether, *by providing it* to the service provider, the right-holder somehow *loses* her ownership interest in the information.²¹⁵ Here, the law of bailment and positive law may play an important role.

1. *Bailment and contractual obligations*. "[T]he fact that a third-party has access to or possession of your papers and effects," Justice Gorsuch wrote in *Carpenter*, "does not necessarily eliminate your interest in them."²¹⁶ Gorsuch's insight is important. History and precedent strongly support distinguishing between ownership and possession in regard to property rights. English law has long favored the former—a preference embedded in the concept of bailment.²¹⁷

By the end of the Middle Ages, common law recognized a bailor's property interest in goods held by others.²¹⁸ In such instances, an

²¹⁵ In cases where an individual writes a letter (or email) and sends it to another person, then the recipient would have the right to reveal the information. The government can only gain access to the document via consent (of either the sender or the recipient) or a particularized warrant. The carrier, however, as the discussion that follows explains, is in a different position: namely, bailment upon consideration.

²¹⁶ *Carpenter*, 138 S Ct at 2268 (Gorsuch, J, dissenting). It creates a bailment—that is, "delivery of personal property by one person (the bailor), to another (the bailee), who holds the property for a certain purpose." *Id.*, quoting and citing *Black's Law Dictionary* 169 (West, 10th ed 2014). See also Richard A. Lord, 19 *Williston on Contracts* § 53:1 (West, 4th ed Nov 2018 update) ("A bailment may be defined as the rightful possession of goods by one who is not the owner."); James Schouler, *A Treatise on the Law of Bailments Including Pledge, Innkeepers and Carriers* 2 n 2 (Little, Brown, 1905) (defining bailment as "A delivery of some chattel by one party to another, to be held according to the special purpose of the delivery, and to be returned or delivered over when that special purpose is accomplished."). If the bailee, who has a legal duty to keep the property safe, fails to do so or violates the bailor's instructions, he is liable for conversion. *Id.* at 2269. He cites state cases: *Goad v Harris*, 207 Ala 357, 92 So 546 (1922); *Knight v Seney*, 124 NE 813, 815–16 (Ill 1919); *Baxter v Woodward*, 158 NW 137, 139 (Mich 1916).

²¹⁷ Pollock and Maitland, 2 *History of English Law* at *152 (cited in note 28).

²¹⁸ *Id.* at *177.

owner “deliver[ed] possession of his chattel to another,”²¹⁹ altering custody without transferring ownership.²²⁰ The bailee (temporarily) held the property for some purpose (e.g., use, enjoyment, or safe-keeping).²²¹

Where the law shifted over time was in regard to liability, recovery, and types of bailment. Thus Ranulf de Glanvill, Chief Justiciar under Henry II, wrote in the twelfth century in the first recognized treatise on English law that the commodatary (the bailee in a *commodatus*, see discussion below) was held to strict liability.²²² In the thirteenth century, Bracton’s *De Legibus et Consuetudinibus Angliae* took a less aggressive stance, holding the depositary liable only in the case of *dolus*—that is, deceit or bad faith.²²³ Due diligence, in some cases, would be sufficient. In 1601, however, Edward Coke, the first lord chief justice of England, essentially returned to Glanvill’s approach when he examined a writ of *detinue* against a bailee from whom the goods in question had been stolen by force.²²⁴ Coke, finding no distinction between the duty to keep chattel and to keep chattel safely, held the bailee to a standard of strict liability for the items in his possession.²²⁵

For the next century, Coke’s approach in *Southcote’s case* held. But in 1703, Lord Chief Justice of England John Holt, drawing in part from Roman law, repudiated Coke’s standard and laid down a series of principles that formed the basis for the modern law of bailment.²²⁶ In 1781, the English jurist William Jones built upon Holt’s principles,

²¹⁹ Id at *168. Bailment vests when content of chattels are made visible to bailee. *Bowdon v Pelleter*, 17 YB 8 Edw II (41 Seldon Society) 136 (1315).

²²⁰ Pollock and Maitland, 2 *History of English Law* at *168 (cited in note 28).

²²¹ See id at *169; Schouler, *A Treatise on the Law of Bailments* § 1 at 1 (cited in note 216).

²²² Ranulf de Glanvill, *Tractatus de legibus et Consuetudinibus Regni Anglie* book 10, ch 13 (*Treatise on the Laws and Customs of the Kingdom of England*) (1554).

²²³ Henrici de Bracton, 2 *De Legibus et Consuetudinibus Angliae* (*On the Laws and Customs of England*) fol 99 b at 111 (Hein, 1990) (Travers Twiss, ed).

²²⁴ *Southcote’s Case*, 76 Eng Rep 1061 (KB 1601).

²²⁵ Id at 1062.

²²⁶ *Coggs v Bernard*, 92 Eng Rep 107, 110 (1703) (“[T]o shew that the tenor of the law was always otherwise, I shall give a history of the authorities in the books in this matter, and by them shew, that there never was any such resolution given before *Southcote’s case*.”). See also William F. Elliott, *A Treatise on the Law of Bailments and Carriers* 3 (Bobbs-Merrill, 1914); Thomas Beven, 2 *Negligence in Law* 746–48 (Stevens and Haynes, 3d ed 1908) (critiquing Oliver Wendell Holmes’s sui generis understanding of English common law). But see Holmes, *The Common Law* at 179–85 (cited in note 29) (generally supporting Coke).

finding in the temporary nature of bailment a certain (albeit limited) duty to the bailor.²²⁷ Like Holt, Jones considered different forms of bailment based on the relationship between bailor and bailee.²²⁸ Supreme Court Justice Joseph Story augmented Jones, cementing the foundation for the contemporary era.²²⁹

Throughout this time, bailment was thought of as a type of contractual relationship, even where no formal contract had been signed.²³⁰ Simultaneously, it was not merely a right *ex contractu*; the common law conveyed it.²³¹ The bailee had possession, while the bailor retained residual ownership rights.²³²

A number of implications followed. A bailor could sue in detinue to recover chattel wrongfully detained.²³³ Although the bailee was merely a custodian, he maintained remedies against anyone who tried to disturb his possession.²³⁴ The bailee thus had something more than

²²⁷ William Jones, *Essay on the Law of Bailments* 5 (Nichols, 1781).

²²⁸ See *id.*

²²⁹ Joseph Story, *Commentaries on the Law of Bailments* v–vii (Hilliard and Brown, 1832).

²³⁰ *Id.* at 2 (“[A] bailment is a delivery of a thing in trust or some special object or purpose, and upon a contract, expressed or implied, to conform to the object or purpose of the trust.”); Henry John Stephen, 2 *New Commentaries on the Laws of England (Partly Founded on Blackstone)* at 129 (John S. Voorhies, 1st Am ed 1843) (“Bailment . . . is delivery of goods for some particular purpose, or on mere deposit, upon a contract express or implied, that, after the purpose has been performed, they shall be re-delivered to the bailor, or otherwise dealt with according to his directions.”); Edwin Charles Goddard, *Outlines of the Law of Bailments and Carriers* § 1 at 1 (Callaghan, 1904) (“A bailment is a contract relation resulting from the delivery of personal chattels by the owner, called the bailor, to a second person, called the bailee, for a specific purpose, upon the accomplishment of which the chattels are to be dealt with according to the owner’s direction.”); Elliot, *A Treatise on the Law* at 1 (cited in note 226) (“A bailment may be defined as a contract by which the possession of personal property is temporarily transferred from the owner to another for the accomplishment of some special purpose.”).

²³¹ See William K. Laidlaw, *Principles of Bailment*, 16 Cornell L Q 286, 287 (1931) (“Although it is frequently said that bailment is founded upon contract, the actual decisions show that it is not so founded.”). See also Alice Erh-Soon Tay, *The Essence of a Bailment: Contract, Agreement or Possession?*, 5 Sydney L Rev 239, 239 (1966).

²³² English law had long recognized these dual rights. See Bracton, 2 *On the Laws and Customs of England* fol 103 b at 144–45 (Bracton wrote, “An action [*vi bonorum raptorum*], on account of movables carried off by force or robbed, is allowed to the owner of a thing or to him from whose custody they have been carried off and who has entered into contract of payment in relation to their owner, so that he has an interest to bring the action.”) (cited in note 223), cited and quoted in Bordwell, 29 Harv L Rev at 510 (cited in note 29). Pollock and Maitland, 2 *The History of English Law* at *172 (cited in note 28) (“[T]he action of detinue is a vindication based upon a proprietary right.”).

²³³ *Id.* at *173. See also Samuel Stoljar, *The Early History of Bailment*, 1 Am J Legal Hist 5 (1957).

²³⁴ Pollock and Maitland, 2 *The History of English Law* at *170 (cited in note 28).

mere possession: he had an interest in the property, and a responsibility for its safety.²³⁵ The bailee *and* the bailor could go after a third party to protect their interests.²³⁶ Bailment further distinguished ownership not just from possession, but from the *right to possess*.²³⁷ As the English jurist Frederick Pollock and Justice Robert Samuel Wright of the Queen's Bench Division explained in the late nineteenth century,

Right to possession (sometimes called constructive "possession,") . . . is one of the constituent elements of the complete right of property; though it may be in a different person from the general owner, and though a person's right of property may continue during a temporary suspension of his right to possession, as in the case of a bailment for a term. Being a part of the right or property it is said not to be lost, even by a general abandonment of the thing.²³⁸

Applied to CSLI, if we assume, *arguendo*, that digital records ought to be treated in the same manner as goods or chattel, under a theory of bailment, the fact that a company holds customer data does not necessarily mean that the individual has alienated his property interest in the record.²³⁹ Nor does an independent right of action by the company against others who attempt to obtain the information necessarily erase the underlying ownership interest. Even should Verizon, for example, *agree* to let other companies use CSLI to market

²³⁵ *Id.* at *169. See also Bracton, 2 *On the Laws and Customs of England* fol 151 (cited in note 223), quoted and cited in both Pollock and Maitland, 2 *The History of English Law* at *169 (cited in note 28), and Holmes, *The Common Law* at 168 (cited in note 29); Frederick Pollock and Robert Samuel Wright, *An Essay on Possession in the Common Law*, Part 3 at 145 (Clarendon, 1888).

²³⁶ As the English Year Books related, "In these actions two rights may be concerned—the right of possession, as is the case where a thing is robbed or stolen from the possession of one who had no right of property in it (for instance, where the thing has been lent, bailed, or let); and the right of property, as is the case where a thing is stolen or robbed from the possession of one to whom the property in it belongs." William Joseph Wittaker, ed, 7 *Seldon Society Publications: The Mirror of Justices* 57 (Bernard Quaritch, 1895).

²³⁷ Pollock and Wright, *An Essay on Possession in the Common Law* at 145 (cited in note 235); Pollock and Maitland, 2 *The History of English Law* at *151 (cited in note 28).

²³⁸ Pollock and Wright, *An Essay on Possession in the Common Law* at 145 (cited in note 235).

²³⁹ This is how the Federal Trade Commission treats data held by service providers. In their case against Facebook, even though the company possessed the information, when customers chose to leave the platform, they retained the right to delete their data. See Complaint, *In the Matter of Facebook, Inc.*, Docket No C-, File No 092 3184, online at <https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf>; Agreement Containing Consent Order, *In the Matter of Facebook, Inc.*, File No 092 3184, online at <https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf>.

goods to the customer, as a categorical matter, the law of bailment might still recognize the customer's underlying property rights. As long as the rights of ownership have not been sold in a market overt, the owner retains residual rights. As Pollock and Maitland explained, "the owner cannot be deprived of his ownership by any transaction between other persons, even though he has parted with possession, and for a time with the right to possess."²⁴⁰

To ascertain whether the individual who carries a mobile device retains an ownership interest in the record of his or her movements, the relationship between the original rights-owner (i.e., the person with the original right to contract with others to provide access to the information) and the entity possessing the property requires further scrutiny.

2. *Digital records as a "bailment upon consideration."* Modern law recognizes different kinds of relationships between bailor and bailee. Although historically they carried differing levels of liability (for the bailee), they did not alter the ownership interest. The court asked what duty was owed *by the one who possesses the goods*. Among the kinds of bailment recognized by eighteenth- and nineteenth-century treatise writers, the ones most relevant to CSLI are included in bailment upon consideration—specifically, contracts related to hiring.²⁴¹ They sub-

²⁴⁰ Pollock and Maitland, 2 *The History of English Law* at *153 (cited in note 28).

²⁴¹ By the eighteenth century, at least five kinds of bailment had come to be recognized in common law. Jones, *Essay on the Law of Bailments* at 35 (cited in note 227); James Kent, 2 *Commentaries on American Law* 558 (O. Halsted, 2d ed 1832). In *Coggs v Bernard*, though, Holt distinguished "six sorts of bailments," which included depositum, commodatum; locatio et conductio; vadium (pawn or pledge); delivery of goods or chattels to be transported for a reward; and delivery of goods or chattels gratis. *Coggs v Bernard*, 92 Eng Rep 107, 109 (1703). *Depositum* dealt with situations in which a deposit was made without reward for recovery. Kent, 2 *Commentaries on American Law* at 560 (cited in note 241). In *Coggs v Bernard*, Lord Holt established that only ordinary care and diligence is expected. *Coggs*, 92 Eng Rep at 110. *Mandatum* amounted to a gratuitous commission, wherein "the mandatary undertakes to do some act about the thing bailed." Kent, 2 *Commentaries on American Law* at 558 (cited in note 241). If the bailee were to transport movable goods, he was only responsible for gross negligence or a breach of good faith. "But if he undertakes to perform some work relating to it, he is then bound to use a degree of diligence and attention suitable to the undertaking and adequate to the performance of it." *Id* at 569–70. *Commodatum* was a loan for use without payment, wherein the item was to be restored *in specie* (e.g., a horse, carriage, or book). The bailee had a higher duty of care to return the same goods. *Id* at 446–49. *Vadium* was a pawn or pledge, such as when something "is bailed to a creditor as a security for a debt." *Id* at 437. The bailee was required "to take ordinary care, and is answerable for ordinary neglect, and no more." *Id* at 449. *Locatio*, which entails "hiring for a reward," is of three types: *locatio rei* (where the bailee, in return for money, has temporary use of the item); *locatio operis faciendi*, in which work and labor is done, or care and attention bestowed by the bailee on the materials bailed, in return for compensation; and *locatio operis mercium vebendarum* (in which goods are bailed

divide into bailments involving: (a) use of a thing (*locatio rei*), (b) work on a thing (*locatio operis faciendi*), (c) the keeping of a thing (*locatio custodiae*), and (d) the transportation of an item (*locatio operis mercium vehendarum*).²⁴² How does CSLI look in this context? The strongest argument places location data in the first category, while two others provide further insight.

Just as telecommunication service providers only have access to customers' location while they are paying for the service, the bailee in *locatio rei* "gains a qualified property in the thing hired, and the [owner] an absolute property in the price."²⁴³ Professor James Kent observed, "This is a contract in daily use in the common business of life."²⁴⁴

As the Court in *Riley* and *Carpenter* was at pains to point out, mobile phones have become a part of daily life. The owner of the phone generates the data and signs a contract to provide it to others. Customers pay for the service, giving companies *temporary* access to their location, in return for which the customer is able to make use of the mobile devices. Companies, in turn, are responsible for ensuring that others do *not* gain access to the information. Failure to safeguard the data creates a liability, not unlike the one established in *locatio rei*.

At no point does the company gain power over the individual's freedom of movement, generation of data, or authority to contract. Once the agreement ends, the company no longer has access to the (former) customer's location. Nor could the company dictate with whom future movements could be shared. In no sense has the ISP gained the authority to alter the customer's privileges or claims. No

to public carrier or private person or transport, in return for either a stipulated or implied reward). Kent, 2 *Commentaries on American Law* at 558, 585–86 (cited in note 241). Modern treatises classify bailments slightly differently. See Lord, 19 *Williston on Contracts* § 53:3 (cited in note 216). The most recent American treatise on bailment, published in 1914, placed all bailments in two categories: gratuitous bailments (i.e., for the benefit of one party) and bailments upon consideration. Elliott, *A Treatise on the Law* at 4–5 (cited in note 226). Of the former, those for the benefit of the bailor divide into deposits and mandates. Those for the benefit of the bailee alone are considered *commodates*. Elliott, *A Treatise on the Law* at 4 (cited in note 226). Bailments upon consideration for mutual benefit divide into two categories: *vadium* (pledges) and contracts of hiring.

²⁴² Elliott, *A Treatise on the Law* at 4–5 (cited in note 226). *Locatio custodiae* applies less directly to CSLI, as it signifies the keeping of a specific item that is then returned to the customer intact.

²⁴³ Kent, 2 *Commentaries on American Law* at 586 (cited in note 241).

²⁴⁴ *Id.*

more so could the ISP itself collect future location data, without express permission. The fact that a consumer has granted access for a limited purpose (providing services) does nothing to divest the individual of her underlying privilege. To the contrary, the company's ability to obtain and use such records rests entirely on the original claim-right exercised by the customer as against the company. It is a bailment for consideration structured in a manner consistent with *locatio rei*.

CSLI also shares characteristics with a second kind of bailment: *locatio operis faciendi*, in which work is done, or care and attention bestowed, by the bailee on the materials bailed, in return for compensation. At least part of the service provided by telecommunications companies relates to the use that is made of the records. Verizon temporarily obtains the information, which it uses to provide better services to its customers. Part of the advantage to the customer is that in the future, calls will be provided more efficiently, with fewer gaps in coverage. While not as complete an account as *locatio rei*, this approach takes account of potentially broader controls over how the information is used by the ISP.

Under a third kind of bailment for consideration, *locatio operis mercium vehendarum*, goods are bailed to a public carrier, a private person, or a transportation service, in return for either a stipulated or implied reward. To the extent that modern telecommunications companies carry communications, there is room for further consideration. Postmasters, for example, historically fell within this category, within which they had a higher duty of care—precisely because of their relationship to the intimate details of individuals' lives. This was the logic adopted by the Court in *Ex parte Jackson*, where it held that private papers were still protected “wherever they may be.”²⁴⁵ It mattered naught that the government itself held the documents (qua the postal service). When sealed from public inspection, letters fell within constitutional protections.²⁴⁶

The divergent theories of liability that depend upon the position of the bailor, as well as degrees of negligence, came to be replaced in the

²⁴⁵ Id, quoting *Ex Parte Jackson*, 96 US 727, 733 (1877).

²⁴⁶ Applying this approach to the contemporary era, Gorsuch wrote, “Just because you entrust your data—in some cases, your modern-day papers and effects—to a third party may not mean you lose any Fourth Amendment interest in its contents.” *Carpenter*, 138 S Ct at 2269.

American context by a uniform negligence standard.²⁴⁷ Keeping in mind concerns about data breaches, the duty placed on ISPs again is remarkably consistent with the traditional responsibilities of a bailment upon consideration. The categories shed light on the different types of relationships contemplated by the law, in which residual ownership rights have historically been maintained by the courts.

3. *Points of convergence and divergence.* In *Carpenter*, Justices Kennedy and Alito largely agreed with Gorsuch in regard to digital documents qua property and the potential role of bailment in a digital age. For Kennedy, “modern-day equivalents of an individual’s own ‘papers or ‘effects’ . . . are held by a third-party” as a “bailment.”²⁴⁸ He considered such matters covered by the Fourth Amendment, even where they might run afoul of third-party doctrine.²⁴⁹ The point of disagreement was whether CSLI involved *that* sort of bailment.²⁵⁰ For Kennedy, it did not: “The businesses were not bailees or custodians of the records, with a duty to hold the records for the defendants’ use.”²⁵¹ Justice Alito similarly noted that bailment may apply to certain types of records entrusted to others, but not to CSLI.²⁵²

Their arguments are difficult to sustain in light of the structure of bailment and how CSLI works. Their logic centered on the level of control exhibited by the companies. Alito noted that *Carpenter*,

had no right to prevent the company from creating or keeping the information in its records. [He] had no right to demand that the providers destroy the records, no right to prevent the providers from destroying the records, and, indeed, no right to modify the records in any way whatsoever (or to prevent the providers from modifying the records). *Carpenter*, in short, has no meaningful control over [CSLI].²⁵³

But the law of bailment recognizes that the possessor not only exercises control over material so bailed, but also has a series of *rights*

²⁴⁷ Richard H. Helmholz, *Bailment Theories and the Liability of Bailees: The Elusive Uniform Standard of Reasonable Care*, 41 Kan L Rev 97, 97 (1992). See also Sheldon D. Elliott, *Degrees of Negligence*, 6 S Cal L Rev 91 (1933).

²⁴⁸ *Carpenter*, 138 S Ct at 2230 (Kennedy, J, dissenting).

²⁴⁹ Id (writing, “*Miller* and *Smith* may not apply when the Government obtains the modern-day equivalents of an individual’s own ‘papers’ or ‘effects,’ even when those papers or effects are held by a third-party.”).

²⁵⁰ Id.

²⁵¹ Id at 2228 (Kennedy, J, dissenting).

²⁵² *Carpenter*, 138 S Ct at 2259 n 6 (Alito, J, dissenting).

²⁵³ Id at 2257 (Alito, J, dissenting). See also id at 2228–29 (Kennedy, J, dissenting).

related to that control. Indeed, to even be considered a bailee, *Williston on Contracts* notes, “one must have both *physical control* of goods and *intent to exercise that control*.”²⁵⁴ The bailment itself “depends on the degree of control and possession, and there must be such a full transfer, actual or constructive, of the property to the bailee as to exclude the possession of the owner and all other persons and give the bailee the sole custody and control of the goods.”²⁵⁵ In such circumstances, though, it is “only possession of property” that is transferred.²⁵⁶ “[T]he bailor remains the true owner.”²⁵⁷

It is not necessary to fully satisfy the ancient, or even modern, law of bailment to recognize that it provides a solid, well-grounded way of thinking about property in a digital era. Some forms of customer data are only brought into being by a third party and do not rely on others’ actions for their existence. Others are unique *to the customer*, to which the company has access. CSLI is of the second sort, in that it wholly depends upon the customer’s decision to purchase a phone, the customer’s use of his property, the customer’s movements, and the customer’s decision to contract with a company to provide services—to the customer. Even after providing location data, the customer is free to share it with others through various apps. And once the contract ends, the service provider no longer has the right to obtain the information. Instead, the consumer decides where it will reside. CSLI is in a different category from that of traditional police surveillance. It is one intimately grounded in property rights.

B. THE ROLE AND LIMITS OF POSITIVE LAW

In *Carpenter*, Justice Gorsuch emphasized that positive law (federal and state) may play a role in helping to establish Fourth Amendment interests.²⁵⁸ This, too, offers a promising approach for understanding property rights in an advanced technological age.

Where federal statutory law or regulatory measures have *privileged certain actors’ control over information* and *denied access to the information to others*, government intrusions may constitute a search or seizure

²⁵⁴ Lord, 19 *Williston on Contracts* § 53:2 (cited in note 216) (emphasis added).

²⁵⁵ *Id.*

²⁵⁶ *Id.*

²⁵⁷ *Id.*

²⁵⁸ *Carpenter*, 138 S Ct at 2270 (Gorsuch, J, dissenting).

within the meaning of the Fourth Amendment.²⁵⁹ This approach is similar to a formulation offered by Professor William Baude and Professor James Stern, who argue that the salient question for Fourth Amendment purposes is “whether it was unlawful for an ordinary private actor to do what the government’s agents did.”²⁶⁰ But it distinguishes between the *privilege* held by the right-holder and the *duty of noninterference* placed on others. In doing so, it recognizes that it is important first to acknowledge *who* holds the right of consent and, second, whether the law establishes an *expectation of security against interference* (based on the obligation on others *not* to access the information absent the right-holder’s consent).

This distinction is constitutionally meaningful. Where an individual has a privileged position, such that they may grant (or withhold) access to the property in question, the law recognizes ownership: in other words, these are “their” papers or effects. Similarly, where private actors have been *denied* access absent the right-holder’s consent, then the privilege owner’s *security* in relation to “*their*” papers has been established. Should a private actor access the information without the privilege-holder’s consent, it would be a violation of the duty owed by the other party to the privilege-holder.

From this, it is logically consistent to conclude that should the *government* try to access the same information, that security also would be violated. Absent a special carve-out for an obligation owed by the privilege-holder to the government, to the extent that the privilege-holder has the right to security of their papers, it may be said to set an expectation of security against all comers.

In fact, there may be an even *higher* burden that the government must meet to gain access to information in which the privilege owner has been granted security.²⁶¹ The government, after all, has massive resources and a monopoly on coercion backed by violence. It can imprison people, take their money, forfeit their property, and even

²⁵⁹ Professors Baude and Stern offer a straightforward distinction between search and seizure, which strikes me as correct: the former “requires an action generally likely to obtain information,” while the latter “requires an assertion of physical control.” Baude and Stern, 129 Harv L Rev at 1833 (cited in note 205). As they observe, there must be a distinction—otherwise the addition of “seizure” would be surplusage. *Id.* at 1832–33.

²⁶⁰ *Id.* at 1826.

²⁶¹ See also Re, 129 Harv L Rev F at 314 (cited in note 205) (writing, “[G]overnment action is different—and often more deserving of regulation—than similar conduct by private parties.”).

take their lives. Private actors (as a matter of law) cannot. The Fourth Amendment itself places restrictions on the government in an effort to restrict the exercise of power and, in so doing, to protect liberty. Positive law thus may help to demarcate constitutional limits.

How does this look in the context of CSLI? Federal laws routinely create rights in intangible things, thereby restricting private actors.²⁶² The 1996 Telecommunications Act, for example, places a duty on carriers “to protect the confidentiality of proprietary information of, and relating to . . . customers.”²⁶³ The statute goes on to lay out the confidentiality of customer proprietary network data, limiting its use, disclosure, or access to the direct provision of services.²⁶⁴ As Gorsuch noted in *Carpenter*, service providers cannot use, disclose, or give others access to customer proprietary network information without the consent of the customer, except as needed for ordinary business purposes.²⁶⁵ They must provide it, when the customer requests, to anyone designated by the customer.²⁶⁶ Where a company fails to protect customer data, the statute provides for a private cause of action.²⁶⁷ Surveying these measures, he concluded, “Plainly, customers have substantial legal interests in this information, including at least some right to include, exclude, and control its use. Those interests might even rise to the level of a property right.”²⁶⁸

While federal statutory measures may provide the strongest evidence in support of property rights (in regard to placing a duty of noninterference on others—including, *arguendo*, the government), state laws also may be probative. Where states have taken certain steps to establish property rights, acknowledging a privilege held by the rights-holder, the courts should at least consider such measures in their analysis. This approach may help to identify constitutional limits on doctrines ill-suited to the digital age.

²⁶² Health care providers, for instance, are required to protect all “individually identifiable health information” relating to an individual’s past, present, or future physical or mental health or condition, in any media in which it is held. Health Insurance Portability and Accountability Act of 1996, Pub L No 104-191, §§ 262, 110 Stat 1936, 2021, 2023, 2029–30.

²⁶³ 47 USC § 222(a).

²⁶⁴ 47 USC § 222(c)(1).

²⁶⁵ *Carpenter*, 138 S Ct 2272 (Gorsuch, J, dissenting), citing 47 USC § 222(c)(1).

²⁶⁶ *Carpenter*, 138 S Ct 2272, citing 47 USC § 222(c)(2).

²⁶⁷ *Carpenter*, 138 S Ct 2272, citing 47 USC § 207.

²⁶⁸ *Carpenter*, 138 S Ct 2272.

Consider open space doctrine. Many states have responded to the privacy invasions occasioned by Unmanned Aerial Systems (UAS) by extending trespass laws to include the airspace above the land.²⁶⁹ California forbids “constructive trespass” onto private property, which does *not* require physical entry into the airspace above private property for a right of action.²⁷⁰ It is illegal “to capture any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a private, personal, or familial activity.”²⁷¹ Not only is the person who conducts the constructive trespass liable for punitive damages, but also anyone who “directs, solicits, actually induces, or actually causes another person, regardless of whether there is an employer-employee relationship” to commit the offense.²⁷²

These and myriad similar state provisions suggest an outer limit to open space doctrine, extending property rights to the constructive trespass of the airspace above private land and placing a duty of non-interference on others—thus protecting the property owners’ enjoyment of their land. While not conclusive, such measures surely are at least probative in understanding the associated property rights when the same restrictions are violated by the government.

This may be particularly true when state provisions expressly forbid state and local *governments* from interfering with property rights. More than eighteen states, for instance, require that law enforcement obtain a warrant before using UAS as part of their investigatory powers.²⁷³ Where data are collected outside of a warrant, most states include a suppression remedy.²⁷⁴ Some go so far as to allow for a civil cause of action against officials, with significant penalties for the dissemination

²⁶⁹ See, for example, Cal Civ Code § 1708.8(a); La Rev Stat Ann § 14:63; Nev Rev Stat § 493.103(1); Or Rev Stat § 837.380(1); Tenn Code Ann § 39-14-405(d). See also Laura K. Donohue, *A Tale of Two Sovereigns: Federal and State Use and Regulation of Unmanned Aircraft Systems*, in Kimon P. Valavanis and George J. Vachtsevanos, eds, *Handbook of Unmanned Aerial Vehicles* (Springer, 2d ed forthcoming 2020), online at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2943018.

²⁷⁰ Cal Civ Code § 1708.8(b). See also NC Gen Stat § 15A-300.1(b).

²⁷¹ Cal Civ Code § 1708.8(a).

²⁷² Cal Civ Code § 1708.8(e).

²⁷³ See, for example, Alaska Stat Ann § 18.65.901(1); Fla Stat § 934.50(3)(b); Idaho Code § 21-213(2)(a); 725 ILCS 167/15(2); Ind Code § 35-33-5-9(a); 25 Me Rev Stat Ann § 4501(4)(B); Mont Code Ann § 46-5-109(1); Nev Rev Stat § 493.112(2); Or Rev Stat §§ 837.310, 837.320; Va Code § 19.2-60.1(B).

²⁷⁴ See, for example, Nev Rev Stat § 493.112(4); Tenn Code Ann § 39-13-609(e)(2).

of material obtained via warrantless surveillance. In North Carolina, the target of the surveillance is entitled to \$5,000 for *every* photograph or video illegally disseminated by any government agency or employee.²⁷⁵ States also forbid and/or tightly regulate UAS use of biometric identification technologies, infrared imaging, video analytics, and enhanced visual aids.²⁷⁶

More specifically, in regard to CSLI, some states preclude law enforcement from accessing information generated by electronic devices without proper legal process. The 2015 California Electronic Communications Privacy Act (CalECPA) creates a property right in digital assets, that is, digitally stored content and online accounts, such as photographs, text messages, postings, spreadsheets, word documents, email, and myriad other digital formats and their associated metadata.²⁷⁷ Lawmakers introduced the statute to curb ballooning law enforcement requests for commercial third-party records.²⁷⁸

Looking to state law to establish property rights (and thereby gauge constitutional entitlements) is consistent with the Court's jurisprudence. The Fifth and Fourteenth Amendments refer to "property," but the Constitution says nothing about *whether* ownership rights exist, much less their scope.²⁷⁹ Courts make this determination by looking to state and local law.²⁸⁰ Regulatory takings determinations turn on two sources: the state's property law, and the reasonable expectations of owners as "shaped by the State's law of property—i.e., whether and to what degree the State's law has accorded legal rec-

²⁷⁵ NC Gen Stat § 15A-300.1(e).

²⁷⁶ See, for example, 20 Vt Stat Ann § 4622(d)(2); 25 Me Rev Stat Ann § 4501(5)(D).

²⁷⁷ California Electronic Communications Privacy Act, 2015 Cal Stat 5110, codified at Cal Penal Code § 1546 et seq.

²⁷⁸ See *SB 178 Fact Sheet (Leno and Anderson)* (ACLU of Northern California, Sept 2, 2015), online at https://www.aclunc.org/sites/default/files/SB%20178%20CalECPA%20Fact%20Sheet_1.pdf (noting, inter alia, a 70 percent increase for location data from AT&T within the past year and a 52 percent increase in requests to Twitter).

²⁷⁹ See US Const, Amend V ("No person shall . . . be deprived of . . . property, without due process of law; nor shall private property be taken for public use, without just compensation."); US Const, Amend XIV ("[N]or shall any State deprive any person of . . . property, without due process of law."). See also *Phillips v Washington Legal Foundation*, 524 US 156, 164 (1998) (holding that the Fifth Amendment protects but does not create property interests), quoting *Board of Regents of State Colleges v Roth*, 408 US 564, 577 (1972).

²⁸⁰ *United States v Powelson*, 319 US 266, 279 (1943) (Justice Douglas writing for the Court, noting that although "the meaning of 'property' as used in . . . the Fifth Amendment is a federal question, it will normally obtain its content by reference to local law." See also *United States v Causby*, 328 US 256, 266 (1946), quoting and citing *Powelson*).

ognition and protection” to the property owner’s interests.²⁸¹ Even states may not avoid confiscatory regulations takings claims by disavowing property interests historically recognized under their laws.²⁸² The query is not limited to economic value. As an annotation from the *American Law Reports* explains, it incorporates “a group of rights that a so-called owner exercises in his or her domination of [the item], such as the right to possess, use, and dispose of it.”²⁸³

The Court’s Fifth and Fourteenth Amendment jurisprudence underscores the importance of the protections extended to property.²⁸⁴ What is included may expand over time: liberty and property “relate to the whole domain of social and economic fact, and the statesmen who founded this Nation knew too well that only a stagnant society remains unchanged.”²⁸⁵ Liberty means not just “freedom from bodily restraint but also the right of the individual to contract, to engage in any of the common occupations of life, to acquire useful knowledge, to marry, establish a home . . . to worship God according to the dictates of his own conscience, and generally to enjoy those privileges long recognized . . . as essential to the orderly pursuit of happiness by free men.”²⁸⁶

As a matter of Fourth Amendment doctrine, positive law may create a floor, but not a ceiling, for constitutional rights.²⁸⁷ Once the law has established a privilege in the right-holder and placed a duty of noninterference on others, it is for the government to demonstrate that it has the right to violate security of property. But a heavier burden may be on them, in light of their particular position of power over the people.

²⁸¹ *Lucas v South Carolina Coastal Council*, 505 US 1003, 1016 n 7 (1992). See also *id* at 1027.

²⁸² *Phillips*, 524 US at 167, citing *id* at 1029.

²⁸³ Ann K. Wooster, Annotation, *What Constitutes Taking of Property Requiring Compensation Under Takings—Supreme Court Cases*, 10 ALR Fed 2d 231, 257 (2006).

²⁸⁴ See *Board of Regents of State Colleges*, 408 US at 571 (“‘Liberty’ and ‘property’ are broad and majestic terms. They are among the ‘(g)reat (constitutional) concepts . . . purposely left to gather meaning from experience’”), quoting *National Mutual Insurance Co. v Tidewater Transfer Co.*, 337 US 582, 646 (Frankfurter, J, dissenting).

²⁸⁵ *Board of Regents of State Colleges*, 408 US at 571.

²⁸⁶ *Meyer v Nebraska*, 262 US 390, 399 (1923).

²⁸⁷ I agree here with Professor Re, who proposes that the Court learn from how legislatures treat private parties without being limited by them: “[W]hen the law has made a deliberate choice to protect against certain intrusions on privacy and security by private parties, then police should have to adduce some kind of justification for undertaking a similar intrusion.” See Re, 129 Harv L Rev F at 313 (cited in note 205). Accordingly, I disagree with Professors Baude and Stern who see the positive law inquiry as a ceiling, not a floor. See Baude and Stern, 129 Harv L Rev at 1888 (cited in note 205).

Elected representatives, of course, do not hold the final determination of constitutional protections. That falls to the judiciary. As Justice Scalia declared in *Jones*, “we must ‘assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.’”²⁸⁸ In *Carpenter*, Gorsuch agreed, noting that *Ex parte Jackson* reflected this principle. He explained that in *Jackson*,

this Court said that “[n]o law of Congress” could authorize letter carriers “to invade the secrecy of letters.” So the post office couldn’t impose a regulation dictating that those mailing letters surrender all legal interests in them once they’re deposited in a mailbox. If that is right, *Jackson* suggests the existence of a constitutional floor below which Fourth Amendment rights may not descend.²⁸⁹

Congress is constitutionally prohibited from granting warrantless access to houses or papers, absent cause.²⁹⁰

In addition to helping to secure rights guaranteed at the founding, adapting them to modern times, and providing a standard consistent with judicial precedent, appealing to positive law to gauge property rights for Fourth Amendment purposes has at least three policy advantages. First, it offers clarity. Where relevant laws have been adopted, the Court can look to them as part of their calculus. Second, it helps to insulate the courts from policy-making, freeing them to focus on matters of law. The Court’s prior refusal to take account of statutory law in determining what society considers more or less reasonable resulted in contradictory and counterintuitive results that continue to undermine judicial credibility. Just as it was illegal in California in the 1980s to cross fences or to trawl through a neighbor’s trash, it is now illegal to obtain digital assets, or to record what happens on private land, even when the recording takes place outside the property line and in public view. Third, the positive law approach acknowledges the role played by the legislature in responding to new and emerging technologies. This was one of the dissents’ primary concerns in *Carpen-*

²⁸⁸ *United States v Jones*, 565 US 400, 406 (2012), quoting *Kyllo v United States*, 533 US 27, 34 (2001), cited in *Carpenter*, 138 S Ct at 2271 (Gorsuch, J, dissenting). See also *Pennsylvania Coal Co. v Mahon*, 260 US 393, 413 (1922) (“The greatest weight is given to the judgment of the legislature but it always is open to interested parties to contend that the legislature has gone beyond its constitutional powers.”).

²⁸⁹ *Carpenter*, 138 S Ct at 2270, quoting *Ex parte Jackson*, 96 US 727, 733 (1877).

²⁹⁰ See *Carpenter*, 138 S Ct at 2271.

ter.²⁹¹ For Kennedy, “The last thing the Court should do is incorporate an arbitrary and outside limit—in this case six days’ worth of cell-site records—and use it as the foundation for a new constitutional framework.”²⁹² Asking whether positive law establishes a privilege, however, and whether there is a duty of noninterference—and using this as probative as to whether a property right (as held against the government) exists—is a very different kind of exercise, and one entirely compatible with the dissents’ view that it is relevant to, but not dispositive of, the property interests at stake.²⁹³

V. THE WAY FORWARD

In 1910 Sir Winston Churchill inveighed: “Let us . . . go forward together. Advance with courage, and the cause of the people shall prevail.”²⁹⁴ Such is the moment at which we stand, that the Court simply must find a way to ensure, at a minimum, the rights that were guaranteed by the Constitution at the founding. How, then, should we think about digitization and the Fourth Amendment going forward?²⁹⁵

Voluntariness and assumption of risk do not have a central role to play. The application of open space doctrine to location tracking rested on a faulty analogy. Unlike cars, mobile devices follow you into the home. The approach ignored the impact of new technologies on rights—in contrast to the Court’s recognition in *Jones*, *Riley*, and *Carpenter* of the deeper privacy interests at stake. Other citizens, moreover, cannot track you twenty-four hours a day, seven days a week,

²⁹¹ See, for example, *id.* at 2261 (Alito, J., dissenting); *id.* at 2233 (Kennedy, J., dissenting).

²⁹² *Carpenter*, 138 S Ct at 2233 (Kennedy, J., dissenting).

²⁹³ See, for example, *id.* at 2242–43 (Thomas, J., dissenting); *id.* at 2227–28 (Kennedy, J., dissenting).

²⁹⁴ Sir Winston Churchill, *The Lords and the Budget*, in Robert Rhodes James, ed., *Churchill Speaks: Winston S. Churchill in Peace and War Collected Speeches, 1897–1963*, at 185, 189 (Chelsea House, 1980) (speech given at the Manchester Free Trade Hall on Mar 19, 1910).

²⁹⁵ Since *Carpenter*, courts have exempted prior, warrantless collection based on good faith, exigent circumstances, and reliance on binding precedent. See *United States v Joyner*, 899 F3d 1199, 1204–05 (11th Cir 2018); *United States v Chavez*, 894 F3d 593, 608 (4th Cir 2018); *United States v Curtis*, 901 F3d 846, 848 (7th Cir 2018); *United States v Zolbiates*, 901 F3d 137, 143 (2d Cir 2018); *United States v Chambers*, 2018 WL 4523607, *1–2 (2d Cir), rem’d from *Chambers v United States*, 138 S Ct 2705 (2018) (mem). But see *United States v Thompson*, 866 F3d 1149 (10th Cir 2017), vac’d and rehearing granted by *Thompson v United States*, 138 S Ct 2706 (mem) (2018); *United States v Stimler*, 864 F3d 253 (3d Cir 2017), vac’d and rehearing granted by *United States v Goldstein*, 902 F3d 411 (3d Cir) (mem).

for years. If they did, it would be downright creepy. And however much an individual uses technology does not mean that others can see it: from network security and encryption to the use of passwords and consent clauses, users protect their data in myriad ways.

The assumption of risk and voluntariness argument drawn from informant doctrine also falls short. This approach, which formed the core of third-party doctrine, decimated constitutional protections extended to papers. It ignored the difference between engaging in illegal activity and forming legal, contractual relationships. It (erroneously) equated consenting to give a company access to one's personal information with consenting to give the government access. And it assumed that not using a bank or having a telephone were viable options in the modern world. As the Court noted in *Riley* and emphasized again in *Carpenter*, mobile devices are not voluntary. Ordinary citizens cannot go through their day without encountering Amazon, much less phones or computers.²⁹⁶ Any effort by the Courts to parse which devices or apps are more or less voluntary will put the judiciary ever more firmly in the policy-making realm, risking future public confidence.

A more promising approach going forward is for the Court to adopt a property-based approach, which, happily, is compatible with both precedent and the original meaning of the text. Digital documents and records constitute "papers" within the meaning of the Fourth Amendment, such that their warrantless acquisition and analysis is per se unreasonable.²⁹⁷ This approach applies the rule of functional

²⁹⁶ See Kashmir Hill, *I Tried to Block Amazon from My Life: It Was Impossible* (Gizmodo, Jan 22, 2019), online at <https://gizmodo.com/i-tried-to-block-amazon-from-my-life-it-was-impossible-1830565336>.

²⁹⁷ In *Carpenter*, Justices Kennedy and Alito considered compulsory process to support *Miller*, *Smith*, and third-party doctrine. For Kennedy, the reason that the government could use a subpoena to compel individuals to release information within their control was because it differed "from a warrant in its force and intrusive power." *Carpenter*, 138 S Ct at 2228 (Kennedy, J, dissenting). He explained: "While a warrant allows the Government to enter and seize and make the examination itself, a subpoena simply requires the person to whom it is directed to make the disclosure." Kennedy's argument was not strictly accurate. In requesting 128 days of records, the government sought *all* location data on the target, not just one discrete piece of information. Once served with a § 2703(d) order, the companies were forced to comply. Additionally, in the 1946 case of *Oklahoma Press Publishing Co. v Walling*, the Supreme Court established that the Fourth Amendment applies to the compelled production of documents. See *Oklahoma Press Publishing Co. v Walling*, 327 US 186 (1946). Orders must "be sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome." *Donovan v Lone Steer, Inc.*, 464 US 408, 415 (1984), quoting *See v City of Seattle*, 387 US 541, 544 (1967). See also *Carpenter*, 138 S Ct at 2228 (Kennedy, J, dissenting); id at 2255

equivalence, already adopted in regard to “houses,” to another, enumerated category.²⁹⁸ It recognizes that while digitization has altered the world in which we live, it has not impacted guaranteed rights. In *Carpenter*, the Court balked at leaving individuals “at the mercy of advancing technology.”²⁹⁹ As Gorsuch observed, it is not just “the specific rights known at the founding” that come within Fourth Amendment protections, but also “their modern analogues.”³⁰⁰

To the extent that the factors employed by the Court to evaluate CSLI (e.g., its volume, revealing nature, retroactivity, near perfect recall, temporal extent, and precision) are relevant, it is not in making some sort of relativistic determination, but in illustrating the extent to which digital records reveal the same intimacies of life traditionally protected under the Fourth Amendment. This approach is consistent with *Riley* and *Jones*, where the Court recognized the revelatory nature of the information at stake. While probative in terms of whether digital documents or records are included in “papers,” however, the degree of invasiveness is neither necessary nor sufficient. The Court does not rest constructive search on the quality of information: in *Kyllo*, it did not matter whether measuring heat levels revealed the type of “intimacies of life” traditionally protected. It was the government’s access to *anything* in the home—including information that allowed it to draw inferences—that constituted a violation. The Court took the same position in *Karo*.

Instead, in determining who owns digital records, the Court should consider adopting a *but for* approach: where the underlying data arise from the actions of an individual, and that person has the original legal right to determine whether and with whom it is shared, they hold an ownership interest in it. This provides a clear line. For situations involving third parties, the law of bailment upon consideration offers a way to distinguish between ownership and possession and to evaluate whether the owner has divested himself of the right of ownership.

(Alito, J, dissenting). CSLI reveals much more than the information being sought, and the Court has never held that a subpoena can elicit records in which the suspect has a reasonable expectation of privacy. *Id.* at 2221 (majority). See also *id.* at 2271 (Gorsuch, J, dissenting) (establishing as his fifth proposition that a constitutional floor may prevent efforts to circumvent Fourth Amendment requirements through subpoenas).

²⁹⁸ See *United States v. Karo*, 468 US 705, 715 (1984), and *Kyllo v. United States*, 533 US 27, 34 (2001).

²⁹⁹ *Carpenter*, 138 S Ct at 2214.

³⁰⁰ *Id.* at 2271 (Gorsuch, J, dissenting).

To the extent that positive law recognizes and protects the right of ownership, it speaks to a constitutional minimum. Here, courts should look to the establishment of a privilege in the right-holder and the corresponding duty held by private citizens—and, by extension, the government—to noninterference absent consent or appropriate (constitutional) process. This approach draws attention to the requirements of ownership (in “their” papers) and security, restoring rights secured at the founding. It adapts the Fourth Amendment to the modern age. And it is consistent with *Katz*, which recognized property interests and suggested that societal expectations matter—in this case, as acknowledged by legislators. Beyond this, it offers clarity and insulates judges from making policy determinations, allowing them to focus on matters of law, even as it takes account of judicial concerns that the legislature play a role in mediating new technologies. In sum, as the Court develops its jurisprudence post-*Carpenter*, it should consider acknowledging the gravitational force of the original Fourth Amendment in protecting essential rights in a digital age.