The Fourth Amendment, Third Parties, and the Digital Age

An Honors Thesis Submitted to
the Department of Politics
In partial fulfillment of the Honors Program

Nathan C. Greess
April 18, 2019

I am very grateful to my thesis advisor, Professor Jeffrey Lenowitz, for his support and guidance, and to my thesis readers, Professor Lucy Goodhart and Professor Daniel Breen. I am especially grateful to my family for the love and support they have provided me in writing this thesis and in all things.

TABLE OF CONTENTS

INTRODUCTION

> [I]n the application of a constitution, our contemplation cannot be only of what has been but of what may be. The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home…Can it be that the Constitution affords no protection against such invasions of individual security?
> - Justice Louis D. Brandeis, dissenting in *Olmstead v. United States* (1928)[1]

The rapid advancement and proliferation of technology has catapulted society into a new era. Nearly every American—95 percent—owns a cellular phone. Between 2011 and 2018, the portion of Americans who own a smartphone more than doubled, increasing from 35 percent to 77 percent. Nearly two-thirds own a desktop or laptop computer; more than half own a tablet computer.[2] A growing portion of households now invite Alexa or another personal assistant into their home.[3] Increasingly, our digital lives are becoming defined by the "Internet of Things": devices that connect to the internet and to each other, like a smart thermostat in your home or the smart watch on your wrist.[4] As our reliance on interconnected technology grows, so too does the amount of information and data we share, both knowingly and unwittingly, with third-parties. By using a cellphone, you reveal your location to your cellular service providers; as you browse the

[1] Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).
[2] Pew Research Center, Demographics of Mobile Device Ownership and Adoption in the United States (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/mobile/.
[3] Niraj Chokshi, *Most Americans See Artificial Intelligence as a Threat to Jobs (Just Not Theirs)*, THE NEW YORK TIMES, Jun. 184, 2018, https://www.nytimes.com/2018/03/06/us/artificial-intelligence-jobs.html.
[4] *See* Steven I. Friedland, *Drinking from the Fire Hose: How Massive Self-Surveillance from the Internet of Things Is Changing the Face of Privacy 2017 Evolving Investigative Technologies and the Law Symposium*, 119 W. VA. L. REV. 891 (2016–2017).

internet, you divulge to your internet service provider (ISP) what websites you visit. In the digital age, third-party providers are, as one scholar puts it, "surveillance intermediaries."[5]

While technology has developed rapidly to meet society's needs, the Fourth Amendment has not. For five decades, the Supreme Court has interpreted the Fourth Amendment as affording *no protection* to information one willingly discloses to a third party. In the words of the Court: "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[6] In an era of ubiquitous technology, the third-party doctrine poses a unique threat. Today, what one routinely reveals to third parties differs both qualitatively and quantitatively from what one might have revealed only a few decades ago. By design, much of the technology on which individuals routinely rely *necessitates* the frequent disclosure of a variety of information. While some types of information that individuals disclose to third parties is rather mundane, other types provide a window into the most sensitive aspects of individuals' lives.

In practice, the third-party doctrine allows the government to easily compel a third party to turn over information that an individual disclosed to the third party. The fundamental question is not *can* the government obtain information but rather *how* must the government go about it. Generally speaking, if the government seeks to search or seize something to which the Fourth Amendment affords protection, it must obtain a warrant issued by a judge or magistrate; to do so, the government must to demonstrate "probable cause" to believe that an offense has or is being committed.[7] However, when the third-party doctrine applies, the government need only issue a subpoena to force a third-party to reveal its records of an individual's disclosures. Unlike a

[5] Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 112 (2018).
[6] Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
[7] *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1119 (2002).

warrant, however, a subpoena does not require probable cause or the approval of a judge.[8] As a result, the third-party doctrine permits the government to access without a warrant sensitive information held by third parties, such as internet search history, location records, emails, and data stored in the "cloud."

In 2018, the Supreme Court ruled in *Carpenter v. United States*, bringing the issue of the third-party doctrine to the fore. In *Carpenter*, the Court held that government must obtain a warrant in order to compel cellular service providers to turn over more than six days of a user's historical cell-site location information (CSLI), records that show a phone's approximate location when it connected to the network.[9] The Court's ruling was narrow, leaving the third-party doctrine intact in its application to all other types of third-party records. However, *Carpenter* raised the prospect of reassessing the doctrine in light of technological change.

This paper argues that in the digital era, the third-party doctrine has become untenable and requires reconsideration if the Fourth Amendment's protections are to meaningfully apply to the modern day. This paper proceeds in four parts. In Part I, I examine the development of the Fourth Amendment, demonstrating how the Supreme Court has long relied on property, physical intrusion, and physical space to interpret the scope of the Amendment's protection against "unreasonable searches and seizures." In Part II, I trace the development of the third-party doctrine. The seeds of the doctrine were planted in a set of cases involving disclosures made to undercover government agents and confidential informants—*the "secret agent" cases*. Those cases laid the foundation for a second set of cases involving commercial and transactional records held by third-parties——*the business records cases*—which solidified the doctrine.

[8] *See* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 140 (2007).
[9] Carpenter v. United States, 138 S.Ct. 2206 (2018).

In Part III, I argue that the third-party doctrine rests on an unstable logical and legal foundation and that its flaws are only exacerbated by its application to third-party disclosures in the digital age. I begin by critiquing three common defenses of the third-party doctrine. Next, I argue that the doctrine has three major flaws stemming both from its origin as well as its application to modern technology and forms of third-party disclosure. The doctrine's flaws demonstrate the need to reconsider how the Fourth Amendment applies to third-party disclosures. In Part IV, I consider how the doctrine might be reformed. First, I argue that the statutory protections offer an insufficient solution and I demonstrate the need for a judicial, constitutional solution. Next, I offer an historically-based rationale for construing Fourth Amendment "papers" to include "digital papers," such as documents and data stored in the "cloud." Lastly, I address the Supreme Court's recent decision in *Carpenter v. United States*; I deconstruct the Court's reasoning and identify questions raised by the decision and its potential implications for the third-party doctrine's application in digital age.

PART I: AN OVERVIEW OF THE FOURTH AMENDMENT

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[10]

"Scholars often describe Fourth Amendment law as unruly."[11] At different times throughout the Amendment's history, the Supreme Court has understood the scope of the protection against "unreasonable searches and seizures" very differently. In Part I, I trace the development of the Court's interpretation of the Fourth Amendment through three phases: *property-based liberalism*, *property-based literalism*, and *reasonable expectation of privacy*. I highlight the role that property, physical intrusion, and physical space play in the Court's understanding of the scope of the Amendment's protection and underscore how this interpretation limits protections in a digital era characterized by intangible information.

BOYD V. UNITED STATES: PROPERTY-BASED LIBERALISM

The Supreme Court's 1886 decision in *Boyd v. United States* marked the first instance in which the high court engaged in meaningful interpretation of the Fourth Amendment and guided the development of search and seizure doctrine over the following several decades.[12] The *Boyd*

[10] U.S. Const. amend. IV
[11] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 809 (2004).
[12] *See, e.g.*, Carroll v. United States, 267 US 132, 147 (1925) (describing Boyd as "the leading case on the subject of search and seizure.").

Court's interpretation of the scope of the Fourth Amendment is notable in two respects. First, the Court adopted a liberal construction of the Amendment's search and seizure clause, one which "rested on a conception of individual liberty more expansive than the literal language" of the Fourth Amendment requires.[13] Second, in interpreting Fourth Amendment "reasonableness," the Court "used the law of property to demarcate both the zone of constitutionally protected interests and the limits on investigative authority."[14]

The case stemmed from a civil forfeiture action brought by the United States alleging that E.A. Boyd & Sons (Boyd) had imported thirty-five cases of plate glass without paying the duties required by law. Pursuant with federal law, the government sought and received a subpoena from the District Court requiring Boyd to produce an invoice for a previous shipment of imported glass. Boyd complied, though challenged the compelled production of the invoice and its introduction as evidence at trial, asserting that the statute authorizing the subpoena violated the Fourth Amendment's protection against unreasonable searches and seizures and Fifth Amendment's right against self-incrimination.[15]

The Court ruled in Boyd's favor, holding that "a compulsory production of the private books and papers of the owner of goods sought to be forfeited" violates the Fourth Amendment's protection against unreasonable searches and seizures as well as the Fifth Amendment's right against self-incrimination.[16] *Boyd* construed the meaning of "searches and seizures" liberally so as to encompass actual searches and seizures as well as actions that amount to "the equivalent of a search and seizure."[17] The compelled production of personal papers, though "divested of many

---

[13] Morgan Cloud, *The Fourth Amendment during the Lochner Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 STAN. L. REV. 555, 574 (1996).
[14] Lawrence Rosenthal, *Binary Searches and the Central Meaning of the Fourth Amendment*, 22 WM. & MARY BILL RTS. J. 881, 888 (2014).
[15] Boyd v. United States, 116 U.S. 616, 617–21 (1886).
[16] *Id.* at 634–35.
[17] *Id.*

of the aggravating incidents of actual search and seizure…contains their substance and essence, and effects their substantial purpose."[18] That the government had obtained Boyd's papers by compelling their production rather than by conducting a literal search and seizure was an inconsequential distinction for the Court. The disputed subpoena constituted a search and seizure within the meaning of the Fourth Amendment because its purpose and effect mirrored those produced by an actual search and seizure.[19]

Having found that the compelled production of the invoice amounted to a search and seizure within the meaning of the Fourth Amendment, the Court turned to the principle constitutional question: "[I]s such a proceeding for such a purpose an '*unreasonable* search and seizure' within the meaning of the Fourth Amendment of the Constitution?"[20] The *Boyd* majority had little trouble resolving this question, writing that "it is only necessary to recall the contemporary or then recent history of the controversies on the subject, both in this country and in England."[21] To define the meaning of "unreasonable searches and seizures," Justice Bradley relied primarily on Lord Camden's judgement in the 1765 English case, *Entick v. Carrington*,[22] one of the oft-cited general warrants cases of eighteenth century England.[23] In *Entick*, pursuant with a warrant, government messengers searched Entick's home and seized his private papers in an effort to obtain evidence linking Entick to the publication of seditious papers.[24] Though the warrant named Entick, it was general in all other respects, not specifying the places to be

[18] *Id.* at 635.
[19] *See* Cloud, *supra* note 14, at 574.
[20] *Boyd*, 116 U.S. at 622.
[21] *Id.* at 624–25.
[22] *See* Entick v. Carrington, 19 Howell's State Trials 1029 (1765)
[23] *See, e.g.,* Wilkes v. Wood, 98 Eng. Rep. 489 (1763); Huckle v. Money, 95 Eng. Rep. 768 (1763)
[24] *See* Entick*,* 19 Howell's, at 1031

searched or the items to be seized.[25] Entick sued the government messengers for trespassing and a jury reached a verdict in his favor.[26]

In his decision upholding the jury verdict, Lord Camden framed the protection and security of property as a fundamental right. Invoking Lockean principles, Camden stated that "[t]he great end for which men entered into society was to secure their property. That right is preserved sacred and incommunicable in all instances, where it has not been taken away or abridged by some public law for the good of the whole…By the laws of England, every invasion of private property, be it ever so minute, is a trespass."[27] One who is said to have committed a trespass against another "is bound to show, by way of justification, that some positive law has justified or excused him." If no such justification exists in "text of the statute law" or "by the principles of the common law" then "the silence of the books is an authority" and the plaintiff must prevail, Camden declared.[28] Camden's discussion of the seizure of stolen property demonstrates how the permissibility of a search and seizure turned on the property interests involved. When stolen goods are seized, the rightful owner may recollect his property; however, the seizure of one's private papers (as in *Entick*) involves the government taking property to which it has no cognizable proprietary interest.[29]

Justice Bradley quoted extensively from *Entick*, praising Lord Camden's discussion of the subject as "one of the landmarks of English liberty."[30] Bradley understood *Entick* to reflect the legal consensus at the time the framers drafted the Fourth Amendment, writing that the framers were "undoubtedly familiar with this monument of English freedom" and "its

---

[25] *Id.* at 1034, 1063-65
[26] *Id.* at 1036
[27] *Id.* at 1029, 1066
[28] *Id.* at 1029, 1066
[29] *Entick*, 19 Howell's, at 1029, 1066
[30] Boyd v. United States, 116 U.S. 616, 626 (1886).

propositions were in the minds of those who framed the Fourth Amendment."[31] The framers would have considered Lord Camden's treatment of the issue as "the true and ultimate expression of constitutional law" and "sufficiently explanatory of what was meant by unreasonable searches and seizures," Bradley asserted.[32] The principles at the core of Lord Camden's opinion, particularly the connection between property rights and protection against government intrusion, "affect the very essence of constitutional liberty and security" and "apply to all invasions on the part of the government and its employés [sic] of the sanctity of a man's home and the privacies of life," Bradley wrote.[33]

Two attributes of the *Boyd* decision deserve special consideration. First, *Boyd* embraced an "expansive conception of individual rights grounded in a value-driven theory of constitutional interpretation."[34] The Court declined to adopt a narrow reading of the protections afforded by the Fourth Amendment. Rather than rely on the text alone, the Court looked to the underlying purpose of the search and seizure clause, cautioning that "illegitimate and unconstitutional practices…can only be obviated by adhering to the rule that constitutional provisions for the security of person and property should be liberally construed."[35] For the majority in *Boyd*, the essence of the Fourth Amendment violation was "not the breaking of [Boyd's] doors, and the rummaging of his drawers" but rather "the invasion of his indefeasible right of personal security, personal liberty and private property."[36]

---

[31] *Id.* at 626–27.
[32] *Id.*
[33] *Id.* at 630.
[34] Morgan Cloud, *Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment*, 72 MISS. L.J. 5, 13 (2002).
[35] *Boyd*, 116 U.S. at 635.
[36] *Id.* at 630.

Second, *Boyd* "used property law rules and concepts to define substantive Fourth Amendment rights."[37] The Court's use of property law to define Fourth Amendment "reasonability" had significant practical and doctrinal implications. From a practical perspective, the *Boyd* ruling suggested that the Fourth Amendment provides individuals with a substantial level of protection against government intrusion into private property, particularly private papers, placing a significant constraint on investigative activity. *Boyd* strongly suggested that "items to which the owner has a legitimate right to possess under the law of property are immune from search or seizure even on a warrant or other compelling justification."[38] As the Supreme Court's first substantial Fourth Amendment ruling, *Boyd* and its particular focus on property guided the development of the search and seizure protection through the first half of the twentieth century.[39]

OLMSTEAD AND PROPERTY-BASED LITERALISM

The Court's 1928 decision in *Olmstead v. United States*[40] signaled both the abandonment of *Boyd*'s liberal, rights-driven reading of the Fourth Amendment and a solidification of *Boyd*'s property-based conception of the Fourth Amendment.[41] As part of an investigation into a suspected bootleg liquor ring, government agents tapped Olmstead's home and office phonelines and eavesdropped on conversation for a period of many months.[42] In *Olmstead*, the Court considered "whether the use of evidence of private telephone conversations between the defendants and others, intercepted by means of wire-tapping, amounted to a violation" of the

[37] Cloud, *supra* note 14, at 578.
[38] Rosenthal, *supra* note 15, at 889; This was the holding in Gouled v. United States, 255 U.S. 298 (1921).
[39] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 196 (2004); *see also* Cloud, *supra* note 14, at 578.
[40] Olmstead v. United States, 277 U.S. 438 (1928).
[41] Cloud, *supra* note 14, at 610; *see* Kerr, *supra* note 12, at 102 (referring to Olmstead as the "classic case" of the property-based Fourth Amendment).
[42] *Olmstead*, 277 U.S. at 456–57.

Fourth Amendment.[43] Relying on an originalist chain of reasoning, the Court held that it did not. The majority opinion, written by Justice Taft, reasoned that the government cannot violate the Fourth Amendment without engaging in either a search or a seizure. Citing eighteenth century precedent, Taft concluded that a search can occur *only if* the government commits trespass against one's property. Therefore, the government *must* commit a trespass for the Fourth Amendment to come into play.[44]

However, the government tapped Olmstead's phonelines "without trespass upon any property of the defendants" because the wires "are not part of [Olmstead's] house or office any more than are the highways along which they are stretched."[45] Declining to adopt a liberal construction of the search and seizure clause, the Court instead asserted that "[t]he Amendment itself shows that the search is to be of *material things*—the person, the house, his papers or his effects."[46] Absent an incursion on Olmstead's person or property, the Fourth Amendment did not prohibit the government from eavesdropping on his telephone conversations. "The evidence was secured by the use of the sense of hearing and that only" and involved "no entry of the houses or offices of the defendants."[47] One who simply hears, of course, commits no trespass and intrudes on no property and therefore neither searches nor seizes, the Court reasoned.

Olmstead had two major implications for the development of Fourth Amendment doctrine. First, the *Olmstead* Court understood the Fourth Amendment to protect *only* tangible objects, namely those explicitly identified in the text of the Amendment. Second, such tangible objects were only protected against physical invasion or penetration. While *Olmstead* rejected

---

[43] *Id.* at 455.
[44] *See* William C. Heffernan, *Fourth Amendment Privacy Interests Criminal Law*, 92 J. CRIM. L. & CRIMINOLOGY 1, 16 (2001).
[45] *Olmstead*, 277 U.S. at 457, 465.
[46] *Id.* at 464 (emphasis added).
[47] *Id.*

Boyd's liberal construction of Fourth Amendment protection, it preserved—and strengthened—the connection between property and the Fourth Amendment.[48]

Justice Brandeis forcefully dissented from the Court's ruling in *Olmstead*, rejecting its focus on physical invasion of property and highlighting the dangers of an inflexible Fourth Amendment. Brandeis criticized the Court's view that the Amendment's protections hinged on physical intrusion, asserting that it is "immaterial where the physical connection with the telephone wires leading into the defendants' premises was made."[49] Brandeis' opposition to the majority's ruling extended beyond the particular facts in *Olmstead.* The Fourth Amendment, he argued, "is much broader in scope."[50]

> [The Framers] knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone — the most comprehensive of rights and the right most valued by civilized men. To protect that right, *every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.*[51]

Brandeis ridiculed the majority's rigid understanding of the Fourth Amendment's reach, warning that "[s]ubtler and more far-reaching means of invading privacy have become available to the Government."[52] Looking to the future, he cautioned against a Fourth Amendment which refuses to adapt. The ability to wiretap represented but the beginning of the development of new technology that renders the physical boundaries irrelevant. "Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in

---

[48] Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 316 (1998).
[49] *Olmstead*, 277 U.S. at 479 (Brandeis, J., dissenting).
[50] *Id.* at 478 (Brandeis, J., dissenting).
[51] *Id.* (Brandeis, J., dissenting).
[52] *Id.* at 473 (Brandeis, J., dissenting).

court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home,"[53] he wrote. However, Brandeis' expansive view of privacy did not prevail in *Olmstead*, which instead endorsed a theory of "property-based literalism."[54]

For a significant part of the twentieth century, the Court remained loyal to *Olmstead*'s narrow understanding of the protection against unreasonable searches and seizures, which protected only against physical incursion or trespass into "constitutionally protected areas," one's person, and physical objects.[55] Applying its property-based inquiry, the Court "divided the world into those areas that were constitutionally protected and those that were not."[56] In practice, adhering to a Fourth Amendment defined by a theory of property-based literalism "guaranteed that the Fourth Amendment would be irrelevant as a device for regulating the use of new technologies that allowed the government to invade formerly private places without committing a common law trespass."[57]

KATZ V. UNITED STATES: REASONABLE EXPECTATION OF PRIVACY

Novel legal questions brought about by advances in technology served as the impetus for the Court's landmark ruling in *Katz v. United States*.[58] In the decades following *Olmstead*, the technological landscape of American society had greatly shifted. When the Court ruled in

[53] *Id.* at 474 (Brandeis, J., dissenting).
[54] Clancy, *supra* note 49, at 318.
[55] Thomas K. Clancy, *What Is a Search within the Meaning of the Fourth Amendment*, 70 ALB. L. REV. 1, 18 (2006).
[56] Clancy, *supra* note 49, at 318; *See* Lanza v. New York, 370 U.S. 139, 143 (1962) ("A business office is a protected area, and so may be a store. A hotel room, in the eyes of the Fourth Amendment, may become a person's 'house,' and so, of course, may an apartment. An automobile may not be unreasonably searched. Neither may an occupied taxicab.").
[57] Cloud, *supra* note 14, at 611.
[58] Katz v. United States, 389 U.S. 347 (united states 1967).

Olmstead in 1927, less than forty percent of households owned a telephone. By the 1960s, that figure had more than doubled and more than eighty percent of households had a telephone.[59]

In *Katz*, FBI agents attached an electronic listening device to the outside of a public telephone booth in an attempt to eavesdrop on conversations between Katz and an associate. Katz was charged with "transmitting wagering information by telephone from Los Angeles to Miami and Boston, in violation of a federal statute." At trial, federal prosecutors were permitted to introduce into evidence portions of Katz's conversations that the listening device had overheard and recorded. Katz was convicted and later appealed.[60]

Before the Supreme Court, Katz raised two constitutional questions, both of which framed the issue in Olmstedian terms. The first question asked "whether a public telephone booth is *a constitutionally protected area* so that evidence obtained by attaching an electronic listening recording device to the top of such a booth is obtained in violation of the right to privacy of the user of the booth"; the second asked "whether *physical penetration of a constitutionally protected area* is necessary before a search and seizure can be said to be violative of the Fourth Amendment."[61] Katz clearly phrased both questions with an eye to the Court's post-*Olmstead* ruling, namely *Goldman v. United States*[62] and *Silverman v. United States*.[63] In *Goldman*, the Court held that no Fourth Amendment violation occurred when federal agents placed a listening device on an outer wall of an office because such surveillance involved no physical penetration into a "constitutionally protected area."[64] The circumstances in *Silverman* were somewhat different. There, federal agents inserted a listening device into the

[59] Michael W. Price, *Rethinking Privacy: Fourth Amendment Papers and the Third-Party Doctrine*, 8 J. NAT'L SEC. L. & POL'Y 247, 261 (2016).
[60] *Katz*, 389 U.S. at 348–49.
[61] *Id.* at 349–50 (emphasis added).
[62] Goldman v. United States, 316 U.S. 129 (1942).
[63] Silverman v. United States, 365 U.S 505 (1961).
[64] *Goldman*, 316 U.S. at 131–34.

heating system of a home, allowing them to overhear conversations taking place throughout the home.[65] For the *Silverman* Court, the fact that the case involved physical penetration of the home—the quintessential "constitutionally protected area"— all but resolved the constitutional question. Writing for a unanimous Court, Justice Stewart observed that in contrast to *Goldman*, "the officers overheard the petitioners' conversations only by usurping part of the petitioners' house or office." Eavesdropping involving "a physical intrusion is beyond the pale of even those decisions in which a closely divided Court has held that eavesdropping accomplished by other electronic means did not amount to an invasion of Fourth Amendment rights."[66] The teachings of *Goldman* and *Silverman* clearly impacted how Katz formulated the constitutional questions presented to the Court. The first question urged the Court to determine whether a public phonebooth constituted a "constitutionally protected area" like the office in *Goldman* or the home in *Silverman*; the second question pressed the Court to further define the contours of its physical penetration doctrine.

However, in its ruling in *Katz*, the majority flatly rejected this formulation of the constitutional questions. "We decline to adopt this formulation of the issues," Justice Stewart wrote for the majority. "The correct solution of Fourth Amendment problems is not necessarily promoted by an incantation of the phrase 'constitutionally protected area'…*The Fourth amendment protects people, not places*."[67] Referencing *Olmstead* and *Goldman*, the Court recognized that "it is true that the absence of such penetration was at one time thought to foreclose further Fourth Amendment inquiry, for that Amendment was thought to limit only searches and seizures of tangible property."[68] Relying on the months-old decision in

[65] *Silverman*, 365 U.S at 507.
[66] *Id.* at 509–11.
[67] Katz v. United States, 389 U.S. 347, 350–51 (united states 1967) (emphasis added).
[68] *Id.* at 352–53.

Warden v. Hayden,[69] the Court effectively overruled *Olmstead* and *Goldman*, declaring that "the premise that property interests control the right of the Government to search and seize has been discredited." Those decisions had "been so eroded" that the trespass doctrine no longer controlled the scope of the Fourth Amendment.[70] Ruling for Katz, the Court reasoned:

> One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.[71]

The *Katz* majority's decision was remarkable in several respects. By overruling *Olmstead* and *Goldman* and holding that neither physical penetration nor property interests governed the Fourth Amendment's scope, the Court *appeared* to depart from its longstanding property-based search and seizure doctrine. The majority's aim in doing away with this precedent was clear: "it intended to extend the reach of the Fourth Amendment—and therefore the possibility of constitutional judicial review—to encompass new technologies that permitted government agents to monitor private conversations without any physical trespass."[72] *Katz* was first and foremost a response to the changing technological landscape.

The opinion was also notable for what it did not say. In rejecting *Olmstead*'s trespass test, the *Katz* majority provided no standard to replace it nor a particularly well-stated rationale for its holding in the case.[73] Justice Stewart, writing for the majority, declared that the Fourth Amendment does not translate to "a general constitutional 'right to privacy'" though it does

---

[69] Warden v. Hayden, 387 U.S. 294 (1967).
[70] *Katz*, 389 U.S. at 353; (quoting *Warden*, 387 U.S. at 304)
[71] *Katz*, 389 U.S. at 352.
[72] Cloud, *supra* note 35, at 24–25.
[73] Peter Winn, *Katz and the Origins of the Reasonable Expectation of Privacy Test*, 40 MCGEORGE L. REV. 1, 6 (2009).

protect "individual privacy against certain kinds of governmental intrusion." However, he added, the Amendment's protections also often have "nothing to do with privacy at all."[74] Beyond the assertion that the Fourth Amendment "protects people, not places," the closest the *Katz* majority came to articulating a standard was to state: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[75]

As a result, the majority opinion had little effect on subsequent cases and almost no lasting impact on the Court's search and seizure doctrine.[76] The enduring influence of *Katz* emerged from Justice Harlan's concurrence, which articulated the standard that the Court would soon embrace as the "lodestar"[77] in its interpretation of the Fourth Amendment. Harlan outlined a two-prong rule, referred to as the "reasonable expectation of privacy" standard or the *Katz* test:

> My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable.[78]

Though the *Katz* test is often regarded as a new and revolutionary standard, Harlan presents it as his restatement of "the rule that has emerged from prior decisions." When seeking to understand Justice Harlan's rule, it is important to recognize the continued role of *physical place*, a central but not obvious factor in the *Katz* test. The majority's declaration that "the

---

[74] *Katz*, 389 U.S. at 350.
[75] *Id.* at 351.
[76] Clancy, *supra* note 49, at 328.
[77] Smith v. Maryland, 442 U.S. 735, 739 (1979).
[78] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

Fourth Amendment protects people, not places"[79] might seem to suggest that *Katz* stands for the wholesale repudiation of *Olmstead*'s approach. However, Justice Harlan's concurrence indicates otherwise: the central question is what protections the Fourth Amendment affords people and "generally, as here, the answer to that question requires reference to a 'place.'"[80] For Harlan, the "critical fact" was that when Katz occupied the phonebooth, "shut[] the door behind him, and pa[id] the toll that permits him to place a call," the phonebooth became "a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable."[81] In other words, the Fourth Amendment afforded Katz protection in the phonebooth because, in essence, Katz rented the space for the momentary period of his call.[82] His expectation of privacy stemmed from the control he asserted over the *place*, an expectation which Harlan concluded to be reasonable, though he did not explain why. Viewed in this light, *Katz* and Harlan's reasonable expectation of privacy test do not so much signal an abandonment of the property-based Fourth Amendment as they signal the adoption of a "loose property-based approach."[83]

While *Katz* overruled *Olmstead*, it did not adopt the approach for which Justice Brandeis advocated in his dissent.[84] Brandeis regarded physical location as "immaterial,"[85] believing that the Fourth Amendment afforded broad protections against all forms of government's invasion of one's privacy, by whatever means.[86] Brandeis' Fourth Amendment was one focused squarely on *privacy*, not simply physical incursion on tangible property.[87] In contrast, Justice Harlan's

[79] *Id.* at 351.
[80] *Id.* at 361 (Harlan, J., concurring).
[81] *Id.* (Harlan, J., dissenting) (internal citations omitted).
[82] *See* Kerr, *supra* note 12, at 822.
[83] *Id.* at 820.
[84] *Id.* at 818.
[85] Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting).
[86] *Id.* at 478 (Brandeis, J., dissenting).
[87] Kerr, *supra* note 12, at 817.

reasonable expectation of privacy standard "implicitly incorporates the spatially-based conception of privacy that had prevailed since *Olmstead.*"[88]

***

The reasonable expectation of privacy test continues to serve as the primary lens through which courts interpret the scope of the Fourth Amendment protection. However, the test is at once the central guide and "the central mystery of Fourth Amendment law."[89] First, for better or for worse, courts soon began to interpret the two prongs of the test differently from how Justice Harlan originally intended. In particular, Harlan intended for the subjective prong of the test to focus on whether an individual *exhibited* an expectation of privacy—in other words, whether one acted to shield the information from observation. However, when the Court addressed the subjective inquiry in early post-*Katz* cases, it tended to interpret "subjective" literally and focused the inquiry on whether an individual *actually anticipated* privacy. But because the Court cannot determine what one actually expected without peering into one's mind, whether government action constituted a search came to depend almost entirely on the second component—the objective prong of the test.[90] As one scholar writes, subjective inquiry is a "phantom doctrine" and "as a practical matter, *Katz* test is only one step."[91]

As discussed, the *Katz* test interprets the scope of the Fourth Amendment with an eye to physical space and tangible elements. However, the digital era is not characterized by physical elements but rather by intangible connections and the transfer of information. In *Katz*, the Fourth Amendment afforded protection in large part because of Katz closing the door to the

[88] Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, n. 91 (2006).
[89] Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 504 (2007).
[90] *See* Orin S. Kerr, *"Katz" Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 127 (2015).
[91] *Id.* at 127, 133.

phonebooth, thereby physically excluding others from the space. In the digital context, physical exclusion often proves impossible simply by nature of the medium. Indeed, interconnected technology quite often demands that an individual leave open the proverbial door. Since "many technologies expose new forms of information rather than hide them, the property law principles driving the Fourth Amendment have led to only weak Fourth Amendment protections in new technologies."[92]

PART II: ORIGIN AND DEVELOPMENT OF THE THIRD-PARTY DOCTRINE

In Part I, I introduced the Fourth Amendment, tracing three defining periods in its development, and highlighting how physical space continues to define the way in which courts interpret its scope. In Part II, I turn to the "third-party doctrine," the Court's primary approach to evaluating the Fourth Amendment's protection of information and data that individuals disclose to third-parties.

For more than 40 years, the Supreme Court has held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[93] As a practical matter, the doctrine holds that an individual loses all Fourth Amendment protection in any information one voluntarily discloses, reveals, or provides to a third party; as a result, the government can compel the third-party to produce that information with a subpoena. The doctrine, though a child of the pre-digital era, "plays a significant role in the Court's Fourth Amendment and technology jurisprudence."[94] In the decades since the Court wove the doctrine

[92] Kerr, *supra* note 12, at 831.
[93] Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
[94] Daniel T. Pesciotta, *I'm Not Dead Yet: Katz, Jones, and the Fourth Amendment in the 21st Century Note*, 63 CASE W. RES. L. REV. 187, 202 (2012–2013).

into Fourth Amendment law, the information that individuals disclose to third-parties has substantially changed, both quantitatively and qualitatively. The third-party doctrine has not.

In the following sections, I trace the development of the third-party doctrine, which involves two sets of cases. The first set—*the "secret agent" cases*—involve disclosures made to undercover government agents and confidential informants. The secret agent cases served as the basis for the second set—*the business records cases*—which involve commercial and transactional records held by third-parties.

THE "SECRET AGENT" CASES

The Court first considered the Fourth Amendment implications of third-party disclosure in the context of information revealed to undercover agents and confidential informants.[95] In *On Lee v. United States*[96] in 1952, the Court considered whether the Fourth Amendment is violated when government agents covertly transmit a conversation between an undercover informant and a suspect by equipping the informant with a listening device. In that case, law enforcement suspected Lee of selling opium from his laundry store. During the investigation, the government attached a device to Chin Poy, an undercover informant and friend of Lee, and successfully overhead a conversation between Poy and Lee in which Lee made incriminating statements. Lee was convicted and appealed, arguing that the recording constituted a violation of the Fourth Amendment and should have been excluded at trial.[97]

The Supreme Court disagreed, instead concluding that the investigatory means employed by the government "did not amount to an unlawful search and seizure such as is proscribed by

[95] *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 567 (2009).
[96] On Lee v. United States, 343 U.S. 747 (1952).
[97] *Id.* at 749–52.

the Fourth Amendment."[98] Writing for the majority, Justice Jackson reasoned that Lee "was talking confidentially and indiscreetly with one he trusted, and he was overheard."[99] For the majority, it was irrelevant that the government was able to overhear the conversation by equipping Poy with a wire. Such means had "the same effect on [Lee's] privacy" as if a government agent "had been eavesdropping outside an open window."[100]

The Court reached the same conclusion in *Lopez v. United States*, decided in 1963.[101] In that case, Lopez attempted to bribe an IRS agent who was equipped with a recording device. At trial, Lopez moved to exclude the recording, asserting that it amounted to an unreasonable search. Relying on the holding in *On Lee*, Justice Harlan rejected Lopez's constitutional claims. Harlan reasoned that the Fourth Amendment had clearly not been triggered by a physical trespass since the IRS agent was in Lopez's office with his consent.[102] Moreover, "the device was not planted by means of an unlawful physical invasion of petitioner's premises under circumstances which would violate the Fourth Amendment."[103] The recording device gathered only the statements Lopez made to the IRS agent, "statements which Lopez knew full well could be used against him by [the IRS agent] if he wished."[104] Harlan differentiated *Lopez* from cases involving eavesdropping, noting that "the Government did not use an electronic device to listen in on conversations it could not otherwise have heard." Rather, the government used the recording device in *Lopez* "to obtain the most reliable evidence possible of a conversation in which the Government's own agent was a participant and which that agent was fully entitled to disclose."[105]

---

[98] *Id.* at 751.
[99] *Id.* at 753–54.
[100] *Id.*
[101] Lopez v. United States, 373 U.S. 427 (1963).
[102] *Id.* at 438.
[103] *Id.* at 439.
[104] *Id.* at 438.
[105] *Id.* at 439.

The Court provided similar reasoning in *Hoffa v. United States*,[106] handed down three years after *Lopez*. In *Hoffa*, James Hoffa, President of the International Brotherhood of Teamsters, was convicted of violating a provision of the Taft-Hartley Act.[107] Hoffa had confided in his colleague Edward Partin who, unbeknownst to Hoffa, was acting as a government informant. Partin later provided testimony at trial regarding Hoffa's disclosures.[108] As in *On Lee* and *Lopez*, the Court held that no Fourth Amendment violation had occurred. As in *Lopez*, the investigatory means involved neither physical trespass nor eavesdropping. Writing for the majority, Justice Stewart noted that "Partin was in the suite by invitation, and every conversation which he heard was either directed to him or *knowingly* carried on in his presence."[109] While Hoffa trusted that his disclosures to Partin would remain secret, the Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he *voluntarily* confides his wrongdoing will not reveal it."[110]

While the Court's 1967 ruling in *Katz* shifted the framework for assessing Fourth Amendment claims, it left unchanged the third-party informant doctrine articulated in *On Lee*, *Lopez*, and *Hoffa*.[111] In *United States v. White*,[112] the Court was presented with facts quite similar to those in *Lopez*. Here, White disclosed information about his criminal conduct to an undercover informant who was equipped with a recording device; the resulting recordings were later introduced as evidence at trial.[113] Echoing its reasoning in *Lopez*, the Court wrote: "Inescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to

[106] Hoffa v. United States, 385 U.S. 293 (1966).
[107] *Id.* at 294.
[108] *Id.* at 296–98.
[109] *Id.* at 302 (emphasis added).
[110] *Id.*
[111] Kerr, *supra* note 96, at 568.
[112] United States v. White, 401 U.S. 745 (1971).
[113] *Id.* at 746–47 (plurality opinion).

the police. If he sufficiently doubts their trustworthiness, the association will very probably end or never materialize. But if he has no doubts, or allays them, or risks what doubt he has, the risk is his."[114] The Court's reasoning in *White*—what I term the "assumption of risk" rationale—states explicitly the "risk" component to which the Court seemed to allude in *On Lee*, *Lopez*, and *Hoffa*. However, *White* does not elaborate on why "the risk is his" or explain why it is "inescapable."

THE BUSINESS RECORDS CASES

In *On Lee, Lopez, Hoffa,* and *White*, the Court laid the groundwork for the third-party doctrine. In the business records cases—*United States v. Miller*[115] in 1976 and *Smith v. Maryland*[116] in 1979—the Court solidified the doctrine by explicitly stating that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[117]

Miller stemmed from an Alcohol, Tobacco, and Firearms Bureau investigation into Mitch Miller for crimes relating to the operation of an unregistered distillery. During the course of the investigation, agents sought and obtained grand jury subpoenas compelling two banks at which Miller maintained accounts to produce "all records of accounts" in Miller's name from a roughly four-month period. The banks complied and provided agents with microfilm records of Miller's accounts and copies of "all checks, deposit slips, two financial statements, and three monthly statements." At trial, the government introduced the copies of Miller's financial records as evidence; Miller moved to suppress the records.[118]

---

[114] *Id.* at 752 (plurality opinion).
[115] United States v. Miller, 425 U.S. 435 (1976).
[116] Smith v. Maryland, 442 U.S. 735 (1979).
[117] *Id.* at 743–44.
[118] *Miller*, 425 U.S. at 436–38.

In its ruling, the Court held that the government did not violated the Fourth Amendment when it compelled Miller's banks to turn over his checks and financial records. The Court articulated two reasons for its holding. First, the Court echoed its "assumption of risk" reasoning from *White*: "[T]he 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."[119] An individual who conveys information in the course of a commercial transaction "*takes the risk*, in revealing his affairs to another, that the information will be conveyed by that person to the Government," the Court stated.[120]

Second, the Court found that Miller possessed "no legitimate expectation of privacy" in the *contents* of the original checks and deposit slips, let alone the microfilm copies provided to agents.[121] The Court reasoned that the contents of the documents were "not confidential communications but negotiable instruments to be used in commercial transactions."[122] They "contain[ed] only information *voluntarily* conveyed to the banks and exposed to their employees in the ordinary course of business."[123]

The Court relied on similar reasoning three years later in *Smith v. Maryland*. The authorities suspected Smith of robbing and then making threatening and obscene telephone calls to Patricia McDonough. At the request of police, the telephone company "installed a pen register at its central offices to record the numbers dialed from the telephone at [Smith's] home."[124] The pen register revealed that Smith had placed a call to McDonough and, on the basis of that

[119] *Id.* at 443.
[120] *Id.* (emphasis added).
[121] *Id.* at 442 (internal quotations omitted).
[122] *Id.*
[123] *Id.* (emphasis added).
[124] Smith v. Maryland, 442 U.S. 735, 737 (1979).

information, police obtained a warrant to search Smith's home where they gathered other evidence linking Smith to the robbery and threatening calls. Smith moved to suppress all evidence that stemmed from the installation of the pen register, arguing that it constituted a search and police should have obtained a warrant prior to its installation.[125]

The Court disagreed, finding that the government did not engage in a search when it installed a pen register to record the phone numbers Smith dialed. The Court ostensibly relied on the *Katz* test to assess Smith's claim that the Fourth Amendment protected against the government's conduct. The Court correctly *stated* the test's first prong—asking if Smith, "by his conduct, ha[d] 'exhibited an actual (subjective) expectation of privacy.'"[126] However, the Court did not in fact *answer* the subjective prong, instead stating that "we doubt that people in general entertain any *actual* expectation of privacy in the numbers they dial." All who use a telephone, the Court reasoned, "realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." Moreover, users' phone bills list long distance calls and pen registers are "regularly employed" by the phone company to check for overbilling, among other things.[127] "Although subjective expectations cannot be scientifically gauged," the Court concluded, "it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret."[128]

Turning to the second prong of the *Katz* test, the Court asserted that even if Smith had indeed believed that the numbers he dialed would remain private "this expectation is not one that

[125] *Id.* at 737–38.
[126] *Id.* at 740 (quoting Katz v. United States, 389 U.S. 347, 361 [united states 1967] [Harlan, J., concurring]).
[127] *Id.* at 742.
[128] *Id.* at 743.

society is prepared to recognize as 'reasonable.'"[129] Smith's expectation of privacy would be rendered unreasonable because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[130] As in *Miller*, the Court relied on its "assumption of risk" reasoning: Smith had "*voluntarily* conveyed numerical information to the telephone company and exposed that information to its equipment in the ordinary course of business" and thus "*assumed the risk* that the company would reveal to police the numbers he dialed."[131]

Smith also identified an important caveat to the otherwise categorical third-party doctrine. Dissenting in *Smith*, Justice Stewart, noted:

> The telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment. Yet we have squarely held [in *Katz*] that the user of even a public telephone is entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.[132]

Stewart identifies a significant limitation on the scope of the third-party doctrine: an individual preserves his reasonable expectation of privacy in the *content* of his telephone conversation despite having "voluntarily disclosed" it to the phone company's equipment.[133] The third-party doctrine does not explicitly include this limitation; rather, it necessarily results from *Katz*, which protected the content of telephone conversations against eavesdropping, and *Berger v. New York*, a subsequent case in ruling warrantless wiretapping unconstitutional.[134] This limitation—*the content/non-content distinction*—certainly exempts the content of telephone conversations from the third-party doctrine, however its scope largely remains unclear.[135]

---

[129] *Id.* (internal citation and quotations omitted).
[130] *Id.* at 743–44.
[131] *Id.* at 744 (emphasis added; internal quotations omitted).
[132] *Id.* at 746–47 (Stewart, J., dissenting) (quoting Katz, 389 U.S. at 352) (internal quotations omitted).
[133] *See* Peter C. Ormerod & Lawrence J. Trautman, *A Descriptive Analysis of the Fourth Amendment and the Third-Party Doctrine in the Digital Age*, 28 ALB. L.J. SCI. & TECH. 73, 117 (2018).
[134] *See* Berger v. New York, 388 U.S. 41 (1967).
[135] Part II addresses the content/non-content distinction in detail.

***

The seeds of the third-party doctrine appeared in the secret agent cases in which the Court relied on an "assumption of risk" rationale to find that the Fourth Amendment did not prohibit the government from overhearing and recording conversations between a suspect and a willing informant. Harnessing—and extending—the "assumption of risk" rationale, *Miller* and *Smith* solidified the third-party doctrine into Fourth Amendment law.

PART III: EVALUATING THE THIRD-PARTY DOCTRINE

In Part II, I discussed the origins of the third-party doctrine and traced its development. Having introduced the necessary historical and legal context, in Part III I turn to the task of evaluating the third-party doctrine.

"The third-party doctrine is one of the most widely disparaged constitutional rules still in force."[136] The doctrine has been criticized on numerous fronts. Scholars have criticized the reasoning underlying the doctrine's foundational cases, *Smith* and *Miller*. Critics and even defenders of the doctrine have noted that "even the U.S. Supreme Court has never offered a clear argument in its favor,"[137] Others criticize the Court's reasoning in *Smith* and *Miller* as "a shaky rationale for deciding questions of privacy."[138] Still others have argued that the doctrine rests on a fundamentally flawed understanding of the concept of privacy,[139] one which is "indicative of a

[136] Ormerod & Trautman, *supra* note 134, at 77.
[137] Kerr, *supra* note 96, at 564; *See* Carpenter v. United States, 138 S.Ct. 2206, 2263 (2018) ("What, then, is the explanation for our third party doctrine? The truth is, the Court has never offered a persuasive justification.").
[138] David A. Harris, *Riley v. California and the Beginning of the End for the Third-Party Search Doctrine*, 18 U. PA. J. CONST. L. 895, 912 (2016).
[139] *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, dissenting) (arguing that "privacy is not a discrete commodity, possessed absolutely or not at all.").

complete lack of appreciation for the notion of relativity."[140] Criticism of the third-party doctrine has only intensified as scholars have come to appreciate the doctrine's profound implications when applied to modern communications technology, the internet, and the cloud.[141] Academics are not alone in raising concern about the intersection of the third-party doctrine and modern technology. Jurists, too, have noted that technological change has given rise to difficult questions of Fourth Amendment law, many of which remain unresolved.[142] Justice Sotomayor has urged a reconsideration of the third-party doctrine, characterizing it as "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."[143]

In contrast, there are remarkably few defenders of the third-party doctrine. The strongest defense of the doctrine comes from Professor Orin Kerr,[144] who has been referred to as "the lone defender of the third-party doctrine."[145] While Kerr's scholarship seeks to challenge the consensus view that the doctrine is "a terrible mistake," he expressly does not attempt to justify the doctrine in all its possible applications.[146] Instead, he seeks to provide "a richer and more balanced account of its costs and benefits" and "demonstrate a strong affirmative argument for the doctrine in many cases and at least a plausible argument in others."[147]

---

[140] Gerald G. Ashdown, *Fourth Amendment and the Legitimate Expectation of Privacy, The*, 34 VAND. L. REV. 1289, 1315 (1981).
[141] Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 585 (2010–2011).
[142] *See, e.g.*, Quon v. Arch Wireless Operating Co., Inc., 529 F. 3d 892, 904 (9th Cir. 2008) ("The extent to which the Fourth Amendment provides protection for the contents of electronic communications in the Internet age is an open question.").
[143] United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).
[144] *See, e.g.*, Kerr, *supra* note 96; Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005 (2010); Orin S. Kerr, *Defending the Third-Party Doctrine: A Response to Epstein and Murphy Symposium: Security Breach Notification Six Years Later*, 24 BERKELEY TECH. L.J. 1229 (2009).
[145] Jane Bambauer, *Other People's Papers*, 94 TEX. L. REV. 205, 210 (2015).
[146] Kerr, *Defending the Third-Party Doctrine*, *supra* note 145, at 1229.
[147] Kerr, *supra* note 96, at 566.

Part III proceeds in two sections. I begin by summarizing and briefly critiquing three arguments commonly offered in defense of the third-party doctrine. The first defense, advanced by Kerr, claims that third parties have a "substitution effect" that frustrates effective law enforcement and that third-party doctrine remedies this effect by maintaining the technological neutrality of the Fourth Amendment. The second defense, also advanced by Kerr, asserts that the doctrine fosters vital ex ante clarity in Fourth Amendment rules. The third defense, appearing most often in judicial opinions, argues that the doctrine recognizes necessary limits on one's ability to assert a Fourth Amendment interest in another's property, limits grounded in the text of the Amendment itself.

I then offer a detailed critique of the third-party doctrine. First, I argue that in *Smith* and *Miller* the Court failed to properly apply the *Katz* "reasonable expectation of privacy" test. Second, I demonstrate the various problems that arise from *Smith* and *Miller*'s reliance on the "secret agent" cases and extension of the "assumption of risk" rationale underlying those decisions. Third, I turn to the doctrine's content/non-content distinction and argue that one cannot reliably divide modern third-party disclosures along a content/non-content line, and that even if one could the distinction has lost its ability to provide ex ante clarity.

THREE DEFENSES OF THE THIRD-PARTY DOCTRINE—AND THEIR WEAKNESSES

In this section, I critique three common defenses of the third-party doctrine. First, I argue that critics overstate the supposed "substitution effect" of third parties. Second, I argue that the third-party doctrine's ability to fosters ex ante clarity is neither unique nor a reflection of the wisdom of the doctrine itself. Third, I assert that the textualist defense of the doctrine in fact demonstrates the doctrine's inconsistency with established Fourth Amendment standards.

"Substitution Effect" and Technological Neutrality

Kerr argues that the enlistment of third parties in criminal activity has a substitution effect and contends that the third-party doctrine remedies this effect by maintaining technological neutrality.[148] In a world with little or no third-party-involved technology, Kerr submits, most crimes would include some public component.[149] A criminal might need to venture out into the public to purchase the necessary tools for his crime or to meet his co-conspirators, for example. This public component of traditional criminal activity is "critical to the traditional balance of Fourth Amendment rules," he claims, because it is at least possible for police to observe the public component of a crime. Because police may begin an investigation with nothing more than suspicion that an individual is engaged in criminal activity, the opportunity to view the public components of a crime allows police to gather additional evidence. While this public evidence will rarely solve the crime, it may provide the basis for obtaining a warrant authorizing an invasion of protected areas.[150]

"Third parties pose a major threat to the Fourth Amendment's basic division between unregulated and regulated steps," Kerr contends, because they "act as remote agents that permit wrongdoers to commit crimes entirely in private."[151] A criminal can use third-party services to convert the traditionally public components of a crime into private components—what Kerr terms the "substitution effect."[152] Kerr submits that the third-party doctrine counters this effect by affording approximately the same degree of privacy protection to a criminal who acts alone as

[148] *Id.* at 573.
[149] *Id.* at 574.
[150] *Id.* at 575.
[151] *Id.*
[152] *Id.*

it does to a criminal who uses third parties: "The part of the crime that previously was open to observation—the transaction itself—remains open to observation. The part of the crime that previously was hidden—what the suspect did without third parties in his home—remains hidden."[153]

While the use of third-party technology can certainly shroud from public view aspects of a crime that might otherwise have been publicly observable, it is not clear that the substitution effect is as pervasive as Kerr suggests. To begin with, "a lot of crime does not come with an obvious technological alternative."[154] For example, it is difficult to see how Kerr's substitution effect would apply to crimes of violence—such as rape, murder, assault, and the like—or to disorderly conduct, driving under the influence, and other common offenses that account for the majority of criminal conduct. There are, of course, some crimes that are likely to involve third-party technology—internet fraud is an obvious example. However, skeptics of the substitution effect note that even in those instances, "it is still worth asking how much of what is involved is a true *substitution* effect as opposed to simply a sub-species of crimes in which third-party participation is an indispensable component (or even instrument) of the offense."[155]

Moreover, Kerr seems to overstate the extent to which the third-party substitution effect allows criminal actors to insulate components of their crime from observation or detection and thereby seriously frustrate police investigations. Absent the third-party doctrine, Kerr asserts, "criminals could use third-party agents to *fully* enshroud their criminal enterprises in Fourth Amendment protection."[156] Eliminating the doctrine would create a Catch-22 whereby police

---

[153] *Id.* at 577.
[154] Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239, 1243 (2009).
[155] *Id.*
[156] Kerr, *supra* note 96, at 576.

would need to have probable cause to observe evidence of a crime in the hands of third-parties but would lack the requisite probable cause without first being able to observe evidence of the crime. Kerr warns that "in many cases, this would eliminate the use of third-party evidence in investigations altogether."[157]

There are three reasons to believe that Kerr's argument overexaggerates the extent to which the third-party substitution effect interferes with the ability of police to gather evidence against a suspected criminal. First, even if the Court were to require police to obtain a warrant to compel the production of certain records held by third parties, nothing would prohibit a third party from voluntarily conveying that information to law enforcement. Therefore, "even if there is some constitutional restraint on *government-initiated* access, it is not clear that sharing is a boon for criminals."[158] Wrongdoers who elect to use third-party technology in the commission of their crime would still face the risk that the third-party would decide to share its records with law enforcement of its own free accord.

Second, criminal procedure supplies law enforcement with other means with which to address the challenges posted by crimes that are complex or difficult to investigate—"namely, the grand jury, which is virtually immune from Fourth Amendment strictures."[159] Even if the Court held that police could not obtain certain third-party records merely by issuing a subpoena but must instead obtain a warrant, a grand jury could obtain the documents by issuing a subpoena *duces tecum*.[160]

---

[157] *Id.*
[158] Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine Comment*, 96 IOWA L. REV. BULL. 39, 45 (2010) (emphasis added).
[159] Murphy, *supra* note 155, at 1244.
[160] *See e.g. United States v. Dionisio,* 410 U.S. 1, 9 (1973) ("It is clear that a subpoena to appear before a grand jury is not a 'seizure' in the Fourth Amendment sense, even though that summons may be inconvenient or burdensome"); *United States v. Calandra,* 414 U.S. 338, 354, (1974) ("Grand jury questions…involve no independent governmental invasion of one's person, house, papers, or effects").

Third, Kerr's prediction fails to recognize that criminals' use of third parties can in fact be a benefit to law enforcement in their investigatory and prosecutorial efforts. Involving third parties in criminal conduct "increase[s] the possibility that a trail will be left or witnesses will be created, all of which only helps the state in building its case."[161] Moreover, third party records often have the benefit of being quite comprehensive and retrospective. As a result, a wrongdoer's enlistment of a third party in crime may provide law enforcement with detailed, compelling evidence. In many instances, police would simply be unable to gather similarly comprehensive evidence through observing the public components of a crime. Consider cell site location information (CSLI), for example, which would provide a record of the caller's location whenever his telephone was connected to the network. To obtain similar information through traditional means, police would need to follow the subject for an extended period of time. If, instead, the police wanted to know where the subject was during a particular period *a month ago*, they would likely be out of luck unless they happened to be surveilling the subject during that period. CLSI records, however, would provide police with this information. In this way, the involvement of third parties can prove quite beneficial to law enforcement.

Ex Ante Clarity

Kerr also argues that the third-party doctrine "foster[s] ex ante clarity in Fourth Amendment rules."[162] Under the doctrine, the extent to which the Fourth Amendment protects information depends entirely on the present location of the information; the Fourth Amendment rules governing the information match the Fourth Amendment rules that apply to the location in which the information is stored. Once information has reached its recipient, any Fourth

[161] Murphy, *supra* note 155, at 1244.
[162] Kerr, *supra* note 96, at 581.

Amendment protection that had existed prior to the disclosure is extinguished. This approach promotes clarity, Kerr claims, because the constitutional rules governing the government's collection of information "are determined by information's knowable location rather than its unknowable history."[163]

Kerr contends that ex ante clarity in Fourth Amendment rules is especially vital given the penalty the government faces when it obtains evidence in violation of the Fourth Amendment. When police violate the Fourth Amendment during the course of an investigation, the exclusionary rule is triggered. Under the exclusionary rule, "the evidence obtained as a fruit of the violation ordinarily cannot be used in court."[164] "The severe costs of the exclusionary rule require ex ante clarity in the rules for when a reasonable expectation of privacy exists," Kerr argues.[165] To avoid having evidence suppressed at trial, police must be able to determine when their conduct runs afoul of the Fourth Amendment. Moreover, uncertainty about what the Fourth Amendment protects "can both overdeter police from acting when no protection exists and can lead them to inadvertently trample on Fourth Amendment rights."[166]

Kerr concludes that absent the third-party doctrine, courts would need to articulate an alternative test for determining when the Fourth Amendment does and does not protect information, one which provides police with the same ex ante clarity as the third-party doctrine. While Kerr concedes that the task of creating such a replacement rule "may not be impossible," he asserts that "the difficulty of devising a clear alternative to the third-party doctrine provides a second argument in its favor."[167]

---

[163] *Id.* at 565, 581.
[164] Kerr, *Four Models of Fourth Amendment Protection*, *supra* note 90, at 527; *See generally* Mapp v. Ohio, 367 U.S. 643 (1961); Wong Sun v. United States, 371 U.S. 471 (1963).
[165] Kerr, *supra* note 96, at 581–82.
[166] *Id.* at 582.
[167] *Id.* at 581.

Ex ante clarity in Fourth Amendment rules is quite desirable, indeed. However, the fact that the third-party doctrine tends to foster such clarity cannot alone justify the doctrine itself. First, the third-party doctrine does not have a monopoly on clarity. As a number of scholars have pointed out, the opposite rule would be equally clear.[168] Justice Gorsuch noted this in his dissent in *Carpenter*:

> [Under the third-party doctrine,] [y]ou (and the police) know exactly how much protection you have in information confided to others: none. As rules go, "the king always wins" is admirably clear. But the opposite rule would be clear too: Third party disclosures *never* diminish Fourth Amendment protection (call it "the king always loses"). So clarity alone cannot justify the third party doctrine.[169]

Of course, this is not to suggest that opposite rule would be a wise replacement for the third-party doctrine; rather, it simply serves to demonstrate that a doctrine's ability to foster ex ante clarity indicates only that the doctrine is uncompromising while saying almost nothing about the wisdom of the doctrine itself.

The Textualist Property Argument

Some defenders of the third-party doctrine argue that the doctrine places "necessary limits on the ability of individuals to assert Fourth Amendment interests in property to which they lack a requisite connection."[170] The Fourth Amendment, they note, protects "'the right of the people to be secure in *their* persons, houses, papers, and effects,' not the persons, houses, papers, and effects of others."[171] The third-party doctrine, then, recognizes that one cannot claim

[168] *See* Murphy, *supra* note 155, at 1245; Henderson, *supra* note 159, at 44.
[169] Carpenter v. United States, 138 S.Ct. 2206, 2263–64 (2018) (Gorsuch, J., dissenting).
[170] *Id.* at 2227 (Kennedy, J., dissenting) (internal quotations omitted).
[171] *Id.* at 2247 (Alito, J., dissenting).

a Fourth Amendment interest in another's property simply because one claims to have some relation to it or hand in its creation.

This assertion, however, is *not* an argument that the third-party doctrine aligns with the established interpretation of the Fourth Amendment as protecting things in which one has a "reasonable expectation of privacy." Rather, the contention is that the doctrine is consistent with a textualist understanding of the Amendment and that such an interpretation is the correct one. In other words, it is at its core an attack on *Katz*; it is not a claim that the doctrine is somehow consistent with the post-*Katz* interpretation of the scope of the Fourth Amendment. Even those who advance this argument, such as Justice Thomas, acknowledge that "under the *Katz* test, individuals *can* have a reasonable expectation of privacy in another person's property."[172] For example, in *Minnesota v. Olson*, the Court has held that an overnight guest can have a legitimate expectation of privacy in the host's home[173]; similarly, in *Chapman v. United States*, the Court held that the Fourth Amendment protects an apartment tenant despite the fact that the tenant is only a leaseholder.[174]A unanimous Court recently reaffirmed this principle, remarking that "it is by now well established that a person need not always have a recognized common-law property interest in the place searched to be able to claim a reasonable expectation of privacy in it."[175] The fact that the third-party doctrine can be read as implying that one cannot maintain an expectation of privacy in things in which one lacks a property interest would seem to be a strike against the doctrine because it places the doctrine at odds with *Katz* and its progeny.

[172] *Id.* at 2242 (Thomas, J., dissenting) (emphasis added).
[173] *See* Minnesota v. Olson, 495 U.S. 91 (1990).
[174] *See* Chapman v. United States, 365 U.S. 610 (1961).
[175] Byrd v. United States, 584 U.S. ___, *8 (2018).

THE FLAWED THIRD-PARTY DOCTRINE

In the following section, I elucidate the flawed nature of the doctrine, focusing both on its foundation in *Smith* and *Miller* and on its application to modern technology and forms of third-party disclosure. I do not seek to prove that, as a matter of constitutional law, *Smith* and *Miller* ought to be overruled or that the third-party doctrine ought to be entirely abandoned. However, I do demonstrate that the third-party doctrine demands reconsideration.

Katz, Miller, and Smith

It is difficult to reconcile the third-party doctrine with the *Katz* "reasonable expectation of privacy" test. This tension has not been lost on scholars and legal commentators. Andrew DeFilippis rightly observes that the doctrine's "sweeping denial of Fourth Amendment protection is at odds with the core principles set forth in *Katz.*"[176] The problem originates with the Court's questionable application of the *Katz* test in *Miller* and *Smith*. As earlier discussed, the decision in *Katz* shifted the Court's understanding of the Fourth Amendment search and seizure clause in two related ways. First, *Katz* rejected the reliance on the *Olmstead*-era trespass and property-based doctrine, criticizing the focus on so-called "constitutionally protected areas."[177] Second, the *Katz* ruling introduced the two-prong "reasonable expectation of privacy" test. The subjective prong of the test looked to whether a person "exhibited an actual (subjective) expectation of privacy"; the objective prong looked to whether that expectation is "one that society is prepared to recognize as 'reasonable.'"[178]

---

[176] Andrew J. DeFilippis, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence Note*, 115 YALE L.J. 1086, 1102 (2005–2006).
[177] *See* Katz v. United States, 389 U.S. 347, 351 (united states 1967).
[178] *See id.* at 361.

Yet, in both *Miller* and *Smith*, the Court's approach to the Fourth Amendment question was inconsistent with the teachings of *Katz*. In *Miller*, "the Court clearly misapplied its own precedent."[179] First, the Court relied heavily on *Hoffa v. United States*, a pre-*Katz* ruling, to guide its examination of the Fourth Amendment question presented in *Miller*. Indeed, the Court began its analysis by quoting *Hoffa* for the proposition that "'no interest legitimately protected by the Fourth Amendment' is implicated by governmental investigative activities *unless* there is an intrusion into a zone of privacy, into 'the security a man relies upon when he places himself or his property within a constitutionally protected area.'"[180] Second, the Court's holding that the subpoena of bank records did not implicate a protected Fourth Amendment interest resulted in part from the determination that the documents at issue were not Miller's "private papers" given that he could "assert neither ownership nor possession" of them.[181] Of course, the singular focus on whether an "area" is "constitutionally protected" is at odds with *Katz*, in which the Court rejected the suggestion "that this concept can serve as a talismanic solution to every Fourth Amendment problem."[182] Moreover, the Court's focus on property interests or ownership is inconsistent with *Katz* and other precedent in which the Court rejected the view that property rights govern Fourth Amendment protections.[183]

Likewise, the Court's application of the *Katz* "reasonable expectation of privacy" test was dubious in both cases. In *Smith*, for example, the Court engaged in a warped application of the subjective prong of the *Katz* test. Telephone users, the majority reasoned, "typically know

---

[179] Brenner & Clarke, *supra* note 89, at 241.
[180] United States v. Miller, 425 U.S. 435, 440 (1976); (quoting Hoffa v. United States, 385 U.S. 293, 301–2 [1966]) (emphasis added).
[181] *Miller*, 425 U.S. at 440.
[182] *Katz*, 389 U.S. n. 9.
[183] *See, e.g.*, *id.* at 353 ("[T]he premise that property interests control the right of the Government to search and seize has been discredited."); United States v. Matlock, 415 US 164, 172 n.7 (1973) ("The authority which justifies the third-party consent does not rest upon the law of property, with its attendant historical and legal refinements…").

that they must convey numerical information to the phone company" and that the phone company can and, for some purposes, does record the numbers dialed. Because telephone users are likely aware that they disclose this information when placing a call, the Court concluded that "it is too much to believe that telephone subscribers…harbor any general expectation that the numbers they dial will remain secret."[184] This approach, though, is not the standard envisioned in *Katz*, which calls for the Court to determine whether a telephone user *exhibited* a subjective expectation of privacy in the numbers she dials. Rather, the Court opted to "depart from that subjective standard by applying an objective test based on what judges think reasonably knowledgeable citizens know."[185]

Katz seemed to be even less of a factor in the Court's reasoning in *Miller*. Indeed, the Court referenced *Katz* only once and did so to quote its assertion that the Fourth Amendment does not protect that which one knowingly exposes to the public.[186] As in *Smith*, the Court misapplied the subjective prong of the *Katz* test. The majority noted that the financial documents at issue contained "only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business" and that the checks "are not confidential communications." On this basis, the Court concluded that there existed no "legitimate 'expectation of privacy' in their contents."[187] Here, as in *Smith*, the Court did not inquire into whether a bank depositor *exhibited* a subjective expectation of privacy; rather, the majority determined that the depositor had voluntarily disclosed the information and therefore any expectation of privacy he harbored was not "legitimate."

[184] Smith v. Maryland, 442 U.S. 735, 743 (1979).
[185] Brenner & Clarke, *supra* note 89, at 248.
[186] *See Miller*, 425 U.S. at 442.
[187] *Id.* (emphasis added).

The Court's focus on what the caller in *Smith* and the depositor in *Miller* likely *knew* is not particularly relevant to the approach articulated in *Katz*. However, this focus can be explained in light of the Court's choice to stray from the *Katz* framework in favor of applying the "assumption of risk" rationale.

Reliance on the "Assumption of Risk" Rationale and Secret Agent Cases

The second substantial flaw with the third-party doctrine stems from the *Miller* and *Smith* Court's reliance on the logic of the "secret agent cases," particularly the "assumption of risk" rationale. The Court's reliance on the "assumption of risk" rationale is a "striking feature" of both *Smith* and *Miller*.[188] First, in extending the "assumption of risk" rationale to *Miller* and *Smith*, the Court failed to recognize that the risk at issue in the secret agent cases was quite distinct from the risk that Miller and Smith supposedly assumed. Consider the facts presented in *Hoffa* and *White*. In that case, James Hoffa made incriminating statements to a friend, Edward Partin who, unbeknownst to Hoffa, was functioning as a government informant. Partin later recounted those statements to law enforcement and testified to them at trial. In *White*, James White made statements to a government informant who relayed those conversations to law enforcement via a wire. In both cases, the risk that Hoffa and White assumed was the risk that the individual with whom they voluntarily shared information was currently or would later decide to share that information with the government. In other words, the risk assumed in these instances is that one might misjudge a confidant's promise of secrecy or harbor a "misplaced belief" that a confidant will not decide to disclose to the government what he has been told. As the *White* Court explained, the risk was one of *misplaced trust*: "If he sufficiently doubts their

[188] Harris, *supra* note 139, at 908.

trustworthiness, the association will very probably end or never materialize. But if he has no doubts, or allays them, or risks what doubt he has, the risk is his."[189]

Now, consider the risk involved in *Miller*. Recall that in *Miller*, the government gained access to Miller's bank records by issuing a subpoena *compelling* the bank to produce the requested records.[190] While the *Miller* Court cited *White* to support the conclusion that a bank depositor "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government,"[191] the risk in *Miller* is quite different from the risk in *White*. Whereas the informants in the secret agent cases voluntarily chose to reveal their conversations to government agents, the bank in *Miller* was *forced* to turn over records.[192]

The risk the Court speaks of in *Miller* and *Smith*, therefore, has little to do with a misjudgment of a third party's trustworthiness or promise of confidentiality. If either case can be said to have involved an assumption of risk, it was certainly not the same risk at issue in the secret agent cases. Instead, if we are to believe that Miller and Smith in fact assumed a risk, it was the risk that the third party to whom they revealed information would be *required* by the government to disclose that information against their will. One who reveals information to another cannot mitigate this risk, even assuming one knew with complete certainty that the person with whom he interacts would not willingly disclose the information to others, including the government.

There is a second, independent problem with the application of the "assumption of risk" rationale to third party disclosures, particularly those in which information is disclosed not to a

---

[189] United States v. White, 401 U.S. 745, 752 (1971).
[190] *Miller*, 425 U.S. at 437.
[191] *Id.* at 443.
[192] Had the bank failed to comply with the subpoena, the court would have likely held the bank in contempt. *See* Fed. R. Civ. P. 45(e)

human but rather to some automated third-party technology. In *Hoffa* and *White*, the Court reasoned that one "assumes the risk" that a third party will inform the government by *knowingly* and *voluntarily* sharing information with that third party. However, knowledge and voluntariness function quite differently in contexts different from the interpersonal disclosure scenario; as the basis of the "assumption of risk" rational, the two factors become especially problematic when information is disclosed to some form of automated third-party technology.

The flaw originates with the *Smith* Court's decision to equate the telephone switching equipment to a human operator. In holding that Smith lacked a reasonable expectation of privacy in the telephone numbers he dialed, the Court noted that Smith had "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its *equipment* in the ordinary course of business."[193] The Court reasoned that "the switching equipment that processed those numbers is merely *the modern counterpart of the operator* who, in an earlier day, personally completed calls for the subscriber."[194] By treating an interaction with an automated system as analogous to a human interaction, the Court framed the issue in *Smith* as factually similar to the circumstances in *On Lee, Lopez, Hoffa,* and *White*. One might argue that one who's call is connected via switching equipment accepts a similar level of risk as one who's call is connected via operator; in that scenario the automated system fulfills the same role (and only the same role) as its human analog, an operator, with which most are familiar. However, many forms of modern technology do not have a clear human analog, in part because they do not function as an exact replacement for a service once provided by humans. The approach adopted in *Smith* becomes increasingly problematic as technology becomes more complex. Scholars have recognized the serious implications of treating an interaction with automated technology as if it

[193] Smith v. Maryland, 442 U.S. 735, 744 (1979).
[194] *Id.*

were an interaction with human. Monu Bedi notes that under this approach, "an individual will likely lose Fourth Amendment protection to any information she exposes to a third party's machine in the normal course of business, regardless of whether a human actually observes the information."[195]

The first difference is with *knowledge*. Equating the risk one assumes by communicating with another human to the risk one assumes by interacting with automated technology overlooks the fact that one's knowledge of the information one reveals—and thus one's knowledge of the precise risk assumed—are meaningfully different. The Court's "assumption of risk" rationale is at its strongest when applied to instances in which one individual knowingly and voluntarily discloses information to another, circumstances such as those presented in the "secret agent cases." In these situations, the individual communicating the information is, of course, aware of exactly what she has said. In communicating information to another person, she "knows that the recipient is not only able, but likely, to evaluate the implications of the information transmitted."[196] Finally, she knows that the person with whom she communicated may decide to share the information with others.[197]

When one interacts with a form of automated technology, the characteristics are quite different. First, the individual will likely have relatively less knowledge of and control over the information she discloses. This is especially true of interactions with more complex technologies, which may involve the disclosure of a variety of information that the average user would not intuitively recognize as necessary to the service the technology provides. In the interpersonal disclosure scenario, the individual is aware of precisely what information she has conveyed and

[195] Monu Bedi, *The Fourth Amendment Disclosure Doctrines Symposium: Big Data, National Security, and the Fourth Amendment*, 26 WM. & MARY BILL RTS. J. 461, 466 (2017–2018).
[196] Brenner & Clarke, *supra* note 89, at 251.
[197] *Id.*

has complete control over which things she discloses and which things she does not. This is not necessarily the case in her interactions with many forms of automated technology. Recognition of this difference has led scholars to warn that "as technology advances, the gap will grow larger between the information that a third party can acquire and the information that individuals are actually cognizant of sharing."[198]

In addition to the difference in knowledge, there is a difference in *voluntariness*: the voluntariness of the disclosure is likely greater in the interpersonal scenario than it is in an interaction with automated technology. Few, if any, would dispute that one who verbally shares information with another does so voluntarily. In that scenario, voluntariness manifests in the speaker's ability to share certain things while withholding others or to share nothing at all. However, voluntariness looks very different when one uses other means of communication, particularly those involving automated technology.[199] Consider the case of cell-site location information (CSLI), for example. When one initiates a call on a cellular phone, the caller discloses her approximate location to the cellular provider. This disclosure, we might conclude, is largely voluntary since the disclosure was the result of her voluntary choice to place a call. But her cell phone also *receives* calls—and texts, and emails, and countless other communications—which also result in her location being disclosed, even when she elects not to answer the call.[200]

---

[198] Rebecca Lipman, *The Third Party Exception: Reshaping an Imperfect Doctrine for the Digital Age Student Note*, 8 HARV. L. & POL'Y REV. 471, 481 (2014).

[199] Though the example I offer here is one involving automated technology, it should be noted that the observation I make regarding the voluntariness of disclosure is applicable to more traditional, pre-tech means of communication. For example, the same points apply to the use of a "mail cover" whereby the government tracks the address information of outgoing and *incoming* mail. In the case of "mail covers," the recipient's name and address information might be disclosed even though the recipient did nothing voluntary to result in the disclosure and can only avoid such a disclosure by having no address at all. *See United States v. Choate*, 576 F. 2d 165 (9th Cir. 1978), cert. denied, 439 U.S. 953 (1978) (holding that the use of a "mail cover" does not violate the Fourth Amendment); JoAnn Guzik, *Assumption of Risk Doctrine: Erosion of Fourth Amendment Protection through Fictitious Consent to Search and Seizure, The Fourth Amendment Symposium*, 22 SANTA CLARA L. REV. 1051, 1078–82 (1982).

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

If the owner of the phone can be said to have voluntarily disclosed her location, she did so simply by owning the cell phone; if she is to avoid "assuming the risk" that the government might force her cellular provider to reveal that information, she has little choice but to disconnect the cell phone from the network or give up the device entirely. Indeed, in the digital era, cell phones, computers, the internet, and similar third-party connected technology is central to both personal and commercial life. Unless one entirely disconnects, modern life *forces* one to "assume the risk" that third-party information will become known to the government.

The Content/Non-Content Distinction

The distinction between the content of communications, which is presumptively protected under Fourth Amendment, and non-content information, which the third-party doctrine strips of protection, is "the most important limitation on the third-party doctrine."[201] However, one cannot reliably divide modern third-party disclosures along a content/non-content line. Even if one could make the distinction, it would no longer serve to distinguish information in which one likely has an expectation of privacy from information in which one likely has no such expectation. Moreover, diminishing usefulness of the content/non-content distinction undercuts the doctrine's ability to provide ex ante clarity.

As previously discussed, third-party doctrine's distinction between content and non-content information finds its roots in *Smith* and *Katz*.[202] Recall that in *Katz*, the Court held that the government's warrantless use of a listening device to record the content of a telephone conversation constituted an unreasonable search under the Fourth Amendment. The Court did

---

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.").

[201] Ormerod & Trautman, *supra* note 134, at 116.

[202] *See* Smith v. Maryland, 442 U.S. 735, 739–41 (1979).

not encounter the question of whether similar constitutional protections extended to the non-content information related to the telephone call, such as the numbers dialed or duration of the call, which may be possessed by a third party, such as the telephone company.[203] This question came in *Smith*, in which the Court held that the Fourth Amendment does not prohibit the government's warrantless installation of a pen register to record the telephone numbers one dials.[204] The *Smith* Court noted that the pen register in *Smith* "differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications."[205] Taken together, *Katz* and *Smith* establish a distinction between the Fourth Amendment's protection of the content of communications and the non-content information associated with such communications: content is presumptively protected whereas non-content information is not. The distinction attempts to "[capture] a qualitative difference in the intimacy of different types of communications information,"[206] allowing for the differential treatment of content and non-content information in the context of telephone communications to be extended to other forms of communications.

Even in the pre-digital era, the content/non-content distinction was controversial. Justice Stewart's dissent in *Smith* points to two issues with the bright-line distinction. The first flaw, Stewart argues, is with the legal justification for the distinction between content and non-content information. The third-party doctrine alone does not provide a convincing rationale for establishing such a distinction. The *Smith* majority reasoned that the Fourth Amendment did not protect the telephone numbers Smith dialed because "[w]hen he used his phone, petitioner

---

[203] Steven M. Bellovin et al., *It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law*, 30 HARV. J. L. & TECH. 1, 3 (2016).
[204] *Smith*, 442 U.S. at 745–46.
[205] *Id.* at 741.
[206] Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2112 (2008).

voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business."[207] But, as Justice Stewart rightly noted, even though "[t]he telephone conversation itself must be electronically transmitted by telephone company equipment," the Court had unequivocally held that the content of telephone conversation received Fourth Amendment protection.[208]

Justice Stewart's dissent also identifies a second issue with the content/non-content distinction, one which has gained renewed relevance in the internet age. The distinction between content and non-content information posits that certain information is wholly content whereas other information is wholly non-content. However, that distinction is largely artificial and may fail to appreciate the revealing nature of so-called non-content information. Justice Stewart noted this with respect to the telephone numbers in *Smith*: "The numbers dialed from a private telephone—although certainly more prosaic than the conversation itself—are not without 'content'" given that they "easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life."[209]

However, in the internet era, "the once stable legal distinction between content and non-content has steadily eroded to the point of collapse, decimating in its wake any meaningful application of the third-party doctrine."[210] Modern communications and internet technology creates two major challenges for the content/non-content distinction. First, the structure of modern communications technology does not lend well to a distinction based on the content or non-content status of information. Second, even if such a distinction could be made, the

[207] *Smith*, 442 U.S. at 744.
[208] *Id.* at 746–47 (Stewart, J., dissenting).
[209] *Smith*, 442 U.S. 735 (Stewart, J., dissenting).
[210] Bellovin et al., *supra* note 204, at 2–3.

distinction would no longer serve to distinguish information in which one likely has an expectation of privacy from information in which one likely has no such expectation.

The content/non-content distinction emerged from cases involving postal letters and telephones; despite its inherent imperfections, the distinction functioned reasonably well in the context of those fairly simple technologies. For example, the physical structure of a postal letter allowed for a clear division of content and non-content: the content was sealed inside the envelope whereas the non-content routing information was visible to all on the outside of the envelope. However, the complex structure of modern internet communications does not allow for such a clear differentiation between content and non-content information.

One problem is that many forms of internet communication lack a direct pre-digital analog. To understand this challenge, it is helpful to consider some examples. First, consider the content/non-content distinction as applied to email. In some respects, e-mail mirrors the structure of postal mail, thus allowing for the content/non-content distinction applied to physical letters to be extended to email communications. Courts that have considered the Fourth Amendment's protection of email communications have pointed to these similarities to justify extending protections to the body of e-mails while declining to extend such protections to the to/from addresses or IP addresses associated with an email communication. The Ninth Circuit Court of Appeals adopted this approach in *United States v. Forrester*[211], holding that the to/from and IP address information associated with an email is unprotected non-content information:

> E-mail, like physical mail, has an outside address 'visible' to the third-party carriers that transmit it to its intended location, and also a package of content that the sender presumes will be read only by the intended recipient. The privacy interests in these two forms of

[211] United States v. Forrester, 512 F. 3d 500 (Court of Appeals, 9th Circuit 2007).

> communication are identical. The contents may deserve Fourth Amendment protection, but the address and size of the package do not.[212]

In *United States v. Warshak*, the Sixth Circuit Court of Appeals employed similar reasoning in reaching the conclusion that the body of an email qualifies as protected content.[213] The court referred to email as "the technological scion of tangible mail," and reasoned that "[g]iven the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."[214][215]

While some aspects of email undoubtedly have pre-digital analogs, other aspects simply do not. Consider the subject line of an email. Unlike the text of the email itself, the subject line of an email is a feature that is not comparable to any feature of a postal letter or a telephone communication. The subject line "contains communicative writing and does not contain any routing information, but it is transmitted in the header portion of email packets."[216] In other words, on the one hand, the subject line of an email resembles the body of the email in so far as it is itself the content of a correspondence or at least communicates information relating to the content of the email; at the same time, the subject line is located in the header of the email, the portion of the email that we would otherwise analogize to the outside of envelope.

The weakness of the content/non-content distinction is even more apparent with respect to Uniform Resource Locators (URLs). Even before grappling with the content/non-content distinction, one must consider whether the interaction between an internet user and an automated server constitutes a communication. While the courts have yet to definitely resolve this question

---

[212] *Id.* at 511.
[213] United States v. Warshak, 631 F. 3d 266 (6th Cir. 2010).
[214] *Warshak*, 285-286 (2010)
[215] *United States v. Warshak*, 631 F. 3d at 285–86.
[216] Tokson, *supra* note 207, at 2130.

with respect to internet browsing, scholars suggest that the courts are likely to view the interaction between a human and an automated web host as a type of communication.[217] If, then, we assume that the interactions inherent in web browsing would be communications subject to the content/non-content framework, we are faced with a more difficult question: are URLs the content of the communication or simply non-content routing information? Arguably, a URL might qualify as non-content routing information, content information, or both. In some respects, a URL has the characteristics of outside-the-envelope information: "it specifies the address of the web page that you are requesting."[218] At the same time, a URL might qualify as content: "requesting a web page essentially means sending a message to a remote server saying 'please send me back the page found at this URL.'"[219] Courts are, of course, capable of reaching and justifying decisions as to whether email subject lines, URLs, and other such elements are content or non-content components. However, the fact that such elements exhibit characteristics associated with both the content and non-content components of analog forms of communications undoubtedly diminishes the ease and confidence with which these classifications will be made.

Even if one were able to divide the information disclosed through use of modern communications technology along the content/non-content distinction, a second and possibly more troublesome problem remains: the distinction would no longer serve to reliably differentiate information in which one likely maintains an expectation of privacy from

[217] *See id.* at 2132–33.
[218] Chris Conley, *Non-Content Is Not Non-Sensitive: Moving beyond the Content/Non-Content Distinction*, 54 SANTA CLARA L. REV. 821, 830 (2014).
[219] *Id.*

information in which one likely lacks such an expectation.[220][221] Here, it is instructive to consider two examples: website IP addresses and URLs.

Relatively few courts have considered whether the IP addresses of the websites one visits constitute protected content. However, when faced with this novel question, courts have tended to consider IP address information to be non-content routing information, often likening it to the telephone numbers in *Smith*.[222] The Ninth Circuit adopted this approach in *Forrester*, holding that the "IP addresses [of websites visited] constitute addressing information and reveal no more about the underlying contents of communication than do phone numbers."[223] While knowledge of website IP addresses may allow the government to make "educated guesses" about what an individual viewed on a particular website, the court reasoned that "this is no different from speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed."[224]

Even fewer courts have considered how to categorize URLs and what protections, if any, the Fourth Amendment affords to such information. Those that have contemplated the issue (usually in dicta) have seemed to signal that URLs may, at least in some instances, constitute content. In a footnote in *Forrester*, for example, the Ninth Circuit suggested that surveillance methods that allow the government to determine the URLs of the pages one visits on a website might be "more constitutionally problematic" than techniques that reveal only the IP address

---

[220] See Richards, 1484
[221] *See* Neil Richards, *The Third Party Doctrine and the Future of the Cloud Washington University Law Professor Spotlight*, 94 WASH. U. L. REV. 1441, 1484 (2016–2017).
[222] *See, e.g.*, United States v. Forrester, 512 F. 3d 500 (Court of Appeals, 9th Circuit 2007); US v. Ulbricht, 858 F. 3d 71 (Court of Appeals, 2nd Circuit 2016) ("The recording of IP address information and similar routing data, which reveal the existence of connections between communications devices without disclosing the content of the communications, are precisely analogous to the capture of telephone numbers at issue in Smith.").
[223] *United States v. Forrester*, 512 F. 3d at 510.
[224] *Id.*

associated with the website.[225] The court suggested that a URL might be distinct from an IP address because "a URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person's Internet activity."[226] At least one court has suggested that there may be good reason to consider a URL to be content when the URL includes search terms or user-inputted data, such as the URL resulting from a Google query. As that court noted, "if the user then enters a search phrase, that search phrase would appear in the URL after the first forward slash. This would reveal content…"[227]

Assume, then, that the courts treated website IP address information as non-content and URLs as content. Would the content/non-content distinction reliably distinguish between information in which one likely maintains an expectation of privacy from information in which one likely lacks such an expectation? There is ample reason to believe that it would not. The content/non-content distinction functions relatively well when applied to telephone numbers because a telephone number can only reveal a limited range of information, namely the recipient of the call. It makes sense to treat telephone numbers as *categorically* non-content because there is not significant variation in the information telephone numbers reveal. In other words, it is not the case that in one instance, a telephone number will reveal the content of the communication while in another case, it would reveal only non-content information. The same cannot be said with respect to website IP addresses or URLs.

As the Ninth Circuit noted in *Forrester*, "a website typically has only one IP address even though it may contain hundreds or thousands of pages."[228] Therefore, knowing that an individual contacted the IP address of the New York Times, for example, would not reveal which articles

[225] *Id.* n. 6.
[226] *United States v. Forrester*, 512 F. 3d n. 6.
[227] In re Application of US for Use of Pen Register, 396 F. Supp. 2d 45, 49 (Dist. Court 2005).
[228] *United States v. Forrester*, 512 F. 3d n. 5.

the individual read. However, in other instances, knowledge of the IP address of a website an individual visited could reveal the precise content viewed. "[I]n cases in which a single website uses a single IP address, and when that website is either small enough or subject-specific enough, mere knowledge of the IP address contacted by the user could inevitably reveal the contents of the underlying communication."[229] In such a scenario, a website IP address "would reveal as much or nearly as much about the content of the underlying web surfing communication as would URLs."[230] The complexity and variability of website IP addresses and URLs underscores the fact that reliance on an analytical approach which seeks to define an element as either *categorically* content or non-content risks under-protecting some types information that are ostensibly non-content yet inevitably reveal information that would otherwise be protected as content.

Lastly, the diminishing usefulness of the content/non-content distinction also undermines the third-party doctrine's ability to provide ex ante clarity, a feature that Orin Kerr and others cite in defense of the doctrine. When the distinction between protected content and unprotected non-content is evident, the risk that law enforcement will inadvertently intrude into protected areas of one's life is reduced. Clarity is lost, however, when the distinction is blurred by novel forms of communication that challenge the categorical divide. Investigators contemplating a request for URL records, for example, may be unsure whether such a request would require a warrant or subpoena. Might it depend on whether the records end up including any URLs that contain search phrases? If that were indeed the case, investigators would have no way of knowing in advance of obtaining the records whether such URLs were among them. Whatever ex ante clarity the third-party doctrine might have once offered would be meaningfully reduced.

[229] Tokson, *supra* note 207, at 2148.
[230] *Id.*

Courts, too, would face a challenge, one inherent in the content/non-content distinction but made more significant by the growth of new and complex forms of communication. Recall that in *Katz*, the Court held that Fourth Amendment protections extended to the content of a telephone call. Then, in *Smith*, the Court held that one lacks Fourth Amendment protection in the phone numbers dialed because he knowingly and voluntarily conveys that information to the phone company; the content of the call remained protected. As Justice Stewart observed in his dissent in *Smith*, that the content of phone conversations is conveyed to the phone company, as well.[231] Except for referencing the holding in *Katz*, the Court did not provide a clear explanation of why knowing and voluntary disclosure vitiated any Fourth Amendment protection of telephone numbers but left the protection of the content of conversations intact.

This deficiency is unproblematic so long as the components of a new forms of communication resemble the those of a telephone call. In those cases, distinguishing content from non-content proves relatively simple. But when the structure is different, *Smith*'s content/non-content distinction provides little guidance because it fails to provide courts with the factors that define "content." As lower courts consider the third-party doctrine's application to novel forms of communication, they risk under-protecting certain information that presents differently than the content of a telephone call yet contains aspects worthy of protection.

***

The third-party doctrine rests on an unstable foundation. The doctrine's principal cases, *Smith* and *Miller*, result from a misapplication of the *Katz* test and an unjustifiable extension of the "assumption of risk" rationale. That rationale, while problematic in *Smith* and *Miller*, proves even more untenable when applied to modern forms of third-party disclosure, particularly

[231] Smith v. Maryland, 442 U.S. 735, 746–47 (1979) (Steward, dissenting).

automated technology. Moreover, the principal limitation on the doctrine—the content/non-content distinction—proves unworkable given the complex nature of modern communications technology. These flaws and failings demonstrate the critical need to reconsider and revise the third-party doctrine. In Part IV, I consider how the Court can reform its approach to third-party disclosure.

PART IV: TOWARDS A WORKABLE FOURTH AMENDMENT SOLUTION TO THE THIRD-PARTY PROBLEM

In the digital age, the third-party doctrine proves to be especially problematic. Though crafting a comprehensive framework that refines or replaces the third-party doctrine presents a challenging task given the complexity and variability of information held by third-parties, a number of scholars have proposed varying solutions. Susan Brenner and Leo Clarke propose a system of "relation-based shared privacy" which bases Fourth Amendment protection on factors relating to the relationship between the "consumer" and the "collector" (i.e. third party).[232] Stephen Henderson looks to the jurisprudence of states that deviate from the federal third-party doctrine; he identifies nine relevant factors and four irrelevant considerations for determining whether Fourth Amendment protections apply in particular third-party records.[233] Daniel Solove, on the other hand, proposes a solution that draws on the statutory term, "system of records"—which includes records retrieved using an individual's name or some identifying number, symbol, or similarly identifying assignment. Solove urges the statutory creation of a warrant-

[232] *See* Brenner & Clarke, *supra* note 89, at 266–79.
[233] *See* Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975 (2007).

subpoena hybrid that includes a probable cause requirement; the government would need to obtain this warrant/subpoena to acquire anything contained in a "system of records."[234]

Here, I do not seek to provide a comprehensive regime to replace the third-party doctrine. Rather, in Part IV, I provide insight into viable approaches to reforming the doctrine as well as evaluate recent developments in the Court's jurisprudence and assess their implications. First, I address the role legislature enactments play in the regulation of government acquisition of third-party records; I refute the argument that courts ought to defer to the legislative branch on the issue of privacy in third-party information. After demonstrating the need for a judicial solution, I focus on the Fourth Amendment's application to information and documents stored in the "cloud." As an alternative to extending protections by relying on analogical reasoning, I provide a historically-based rationale for construing Fourth Amendment "papers" to include "digital papers." Finally, I address the Court's recent decision in *Carpenter v. United States*. I deconstruct the Court's reasoning and assess the decision's broader implications.

THE INSUFFICIENCY OF STATUTORY PROTECTIONS

Before considering how the third-party doctrine be modified, I address the role that statutes play in regulating government access to third-party records. In recent decades, "the rules regulating government investigations have increasingly been those of federal statutes, not Fourth Amendment law."[235] This dynamic is especially apparent with respect to law enforcement's interaction with and use of new technology. Rather than provide a conclusive Fourth Amendment response to privacy questions raised by novel technology, judicial decisions have

[234] *See* SOLOVE, *supra* note 40, ch. 11.
[235] Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 753 (2005).

served as the impetus for federal and state legislative action on these matters.[236] As a result, though the third-party doctrine eliminates Fourth Amendment protection against an array of government information-gathering activities, several federal statutes provide some level of protection.[237]

Scholars and jurists have cautioned against prematurely looking to the courts to resolve the legal questions raised by new or changing technology. The Supreme Court has warned that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[238] Orin Kerr suggests that courts should "place a thumb on the scale in favor of judicial caution when technology is in flux" and should consider allowing the legislative branch to determine what rules ought to govern law enforcement activities involving novel technologies.[239] Kerr and others cite several reasons why court are often ill-equipped to address the privacy implications of emerging technology. They argue that the judicial branch lacks the capacity to easily comprehend the privacy implications of the technologies at issue and often create inflexible legal standards that become unworkable when applied to different technology.[240] Legislative rule-making, they contend, "offers significantly better prospects for the generation of balanced, nuanced, and effective investigative rules involving new technologies."[241]

If Congress and state legislatures have acted to address the privacy implications of new technology, why is it necessary for courts to reconsider the third-party doctrine and devise a new approach to determining the Fourth Amendment's application to information held by third-party

---

[236] Kerr, *supra* note 12, at 857.
[237] *See e.g.* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C §§ 2510-22, 2701-12, 3121-27 (2006))
[238] City of Ontario, Cal. v. Quon, 560 U.S. 746, 2629 (2010).
[239] Kerr, *supra* note 12, at 805.
[240] *Id.* at 857–59.
[241] *Id.* at 859.

providers? For at least two reasons, I argue that deference to legislative regulation represents an unwise and unsustainable solution. First, as a normative matter, Congress' efforts to respond to the privacy implications of new technology tend to be insufficient. Using the Stored Communications Act as an example, I demonstrate that statutory schemes quickly become outdated as technology advances, producing problematic outcomes. Second, as a practical matter, courts have *already* begun to extend Fourth Amendment protection to third-party information, even where statutes already regulate government access to such information. Lower courts have demonstrated their willingness to engage in this area but have done so with almost no guidance from the Supreme Court. Without reassessing the doctrine and providing a coherent standard, we risk a reality in which a patchwork of lower court decisions governs government acquisition of third-party records, with Fourth Amendment protection varying by jurisdiction.

When courts have declined to extend Fourth Amendment protections to areas of emerging technology, legislative bodies—particularly Congress—have attempted to fill the void and have done so with mixed results. Six years after the Court's ruling in *Olmstead* opened the door to warrantless wiretapping, Congress enacted Section 605 of the Federal Communications Act.[242] However, "dislike of § 605 was nearly universal" and the law was widely viewed as "a disaster."[243] The language of the statute proved problematic, in large part because it did not provide a clear enforcement mechanism.[244] Indeed, it took a ruling by the Supreme Court to resolve the ambiguity of Section 605 and clarify that a violation of the Act would result in the improperly obtained evidence being excluded in federal court.[245] Congress fixed the flaws in

[242] 6 U.S.C. § 605 (1934) (current version at 47 U.S.C. § 605 (2000))
[243] Solove, *supra* note 237, at 770.
[244] Section 605 reads as follows: "[N]o person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person." 47 U.S.C. § 605; see Solove #6, 770
[245] *See* Nardone v. United States, 302 U.S. 379 (1937).

Section 605 in Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[246] but only after the Court overruled *Olmstead* in *Katz*, thereby extending a constitutional warrant requirement to wiretapping.[247] Similarly, Congress responded to the Court's ruling in *Miller* by enacting the Right to Financial Privacy Act ("RFPA") two years later.[248] In 1986, Congress responded to the Court's 1979 decisions in *Smith* by enacting the Pen Register Act, requiring law enforcement to obtain a court order to use a pen register or trap and trace device.[249]

In 1986, Congress passed the Electronic Communications Privacy Act ("ECPA") of 1986.[250] The EPCA has three principle components.[251] Title I—the Wiretap Act—creates protections for wire, oral, and electronic communications during transit.[252] Title II—the Stored Communications Act (SCA)—protects communications held in electronic storage.[253] Title III—the Pen Register Act—governs the use of pen registers and trap and trace devices, as previously discussed.[254] Here, I focus on the Stored Communications Act, which exemplifies how legislative regulation becomes quickly outdated and provides insufficient protection of third-party records.

The SCA created a rather complex statutory regime governing government access to a range of electrically-stored information and data. The Act distinguishes between two types of providers: providers of electronic communication service ("ECS") and providers of remote

---

[246] *See* Pub. L. No. 90-351, 82 Stat. 211 (1968) (codified as amended at 18 U.S.C. §§ 2510-2520 (2000)).
[247] Katz v. United States, 389 U.S. 347, 353 (united states 1967) (holding that "the underpinnings of Olmstead and Goldman have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling.").
[248] Financial Institutions Regulatory and Interest Rate Control Act of 1978, Pub. L. 95- 630, 92 Stat. 3641 (1978) (codified as amended at 12 U.S.C. §§ 3401-3422 (2000))
[249] 18 U.S.C. §§ 3121-27; see Kerr #10, 855
[250] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C §§ 2510-22, 2701-12, 3121-27 (2006)).
[251] Alexander Scolnik, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment Note*, 78 FORDHAM L. REV. 349, 375 (2009–2010).
[252] 18 U.S.C. §§ 2510-2522
[253] *Id.* at §§ 2701-2712
[254] *Id.* at §§ 3121-3127

computing service ("RCS"). It defines ECS as "any service which provides to users thereof the ability to send or receive wire or electronic communications"[255]; RCS are defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[256] Under the SCA, different rules govern each type of provider, so it matters greatly whether a provider is functioning as an ECS or an RCS.

The SCA governs compelled and voluntary disclosure of both content and non-content data.[257] Here, however, I focus on the SCA provisions relating to compelled disclosure of content and non-content data. The rules for compelled disclosure "operate like an upside-down pyramid."[258] That is, under the SCA, the government must at least follow the minimum process for a particular type of data (say, a simple subpoena) but could also use a more demanding process to obtain that data (a warrant, for example). This "greater includes the lesser" framework "allows the government to obtain only one court order—whatever process is greatest—and compel all of the information in one order all at once."[259]

With a simple subpoena, the government can compel the production of (non-content) subscriber information, including name, address, telephone connection records, length of service, telephone or instrument number, and payment information.[260] With a "specific and articulable

[255] *Id.* at § 2510(15); the statute defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" (18 U.S.C. § 2510(17)(A)) plus any backup copies of files in such temporary storage (18 U.S.C. § 2510(17)(B))
[256] 18 U.S.C. § 2711(2); the statute defines "electronic communications system" as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." (18 U.S.C. § 2510(14) (2000))
[257] *See* 18 U.S.C. § 2703(a)-(b) (compelled disclosure of content records); 18 U.S.C. § 2703(c)(1)-(2) (compelled disclosure of non-content records); 18 U.S.C. § 2702 (voluntary disclosure of content and non-content records).
[258] Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & (and) the USA Patriot Act: Surveillance Law: Reshaping the Framework*, 72 GEO. WASH. L. REV. 1208, 1222 (2003–2004).
[259] *Id.* at 1220.
[260] *See* 18 U.S.C. § 2703(c)(2)

facts" court order, known as a "2703(d)" order,[261] the government can compel all non-content records.[262] A simple subpoena plus prior notice to the subscriber[263] is sufficient to compel basic subscriber information,[264] *opened* emails or other permanently held files,[265] and content in temporary "electronic storage" such as *unretrieved* emails in storage for *greater* than 180 days.[266] With a 2703(d) order plus prior notice, the government can compel all non-content records,[267] *opened* emails or other permanently held files,[268] and content in temporary "electronic storage."[269] Finally, with a search warrant, the government can compel the production of all the aforementioned categories of information.[270] In other words, "a 2703(d) order plus prior notice compels everything except contents in temporary 'electronic storage' 180 days or less."[271] To compel information in that category, such as *unopened* emails *less* than 180 days old, investigators are required to obtain a search warrant.[272]

The problematic nature of the SCA becomes clear when one considers how its framework applies to various types of common data. The most obvious problem is the way in which the SCA rules apply to emails. The SCA affords a dramatically different level of protection to opened emails and unopened emails. For example, the government needs a warrant to gain access to unopened emails that are less than 180 days old. However, if the unopened emails are *older* than 180 days *or* if the emails are *opened*, the SCA requires only a simple subpoena plus

---

[261] *See* 18 U.S.C. § 2703(b)(1)(B)(ii); a "2703(d)" order requires the government to present "specific and articulable facts showing that there are reasonable grounds to believe" that the information sought is "relevant and material to an ongoing criminal investigation." (18 U.S.C. § 2703(d)).
[262] *See* 18 U.S.C. § 2703(c)(1)(B)]
[263] The SCA allows for notice to be delayed in various circumstances.
[264] *See* 18 U.S.C. § 2703(c)(2)
[265] *See Id.* § 2703(b) (under the rules governing RCS)
[266] *See Id.* § 2703(a)
[267] *See Id.* § 2703(c)(2)
[268] *See Id.* § 2703(b) (under the rules governing RCS)
[269] *See Id.* § 2703(a)
[270] *See Id.* § 2703(a)-(c)
[271] Kerr, *A User's Guide to SCA*, *supra* note 260, at 1223.
[272] See 18 U.S.C. § 2703(a)

prior notice. This odd result stems from the fact that when Congress drafted the SCA more than three decades ago, it expected that email would only rarely be retained for long periods of time. Today, however, "e-mail is routinely held on providers' servers for increasing periods of time, and, in some cases, even indefinitely."[273] Similarly, consider how the SCA applies to documents stored in the "cloud." While investigators would undoubtedly need a warrant to search a file cabinet and seize the physical version of a document, if the document is stored in the "cloud," the SCA requires only a subpoena plus prior notice. Scholars point to this and other oddities of the modern application of the SCA in concluding that the SCA rules are "hopelessly out of date."[274]

Second, courts have already begun to extend Fourth Amendment protections to areas regulated by the SCA. In *Warshak*, for example, the Sixth Circuit held that the government could not compel a provider to disclose the content of a subscriber's emails without a warrant and "to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional."[275] Similarly, the Ninth Circuit laid the groundwork for extending Fourth Amendment protection to text messages when it held that individuals have a reasonable expectation of privacy in their text messages.[276] The Supreme Court's 2018 ruling in *Carpenter*, discussed at length later on in Part IV, is the most definitive signal that the ship has sailed on judicial deference to legislative determinations regarding if and how best to protect individuals' privacy interests in light of technology development. There, the Court held that a 2703(d) order

[273] Scolnik, *supra* note 253, at 378–79.
[274] Solove, *supra* note 237, at 769.
[275] United States v. Warshak, 631 F. 3d 266, 288 (6th Cir. 2010).
[276] Quon v. Arch Wireless Operating Co., Inc., 529 F. 3d 892, 904 (9th Cir. 2008).

"is not a permissible mechanism for accessing historical cell-site records" and instead imposed a warrant requirement.[277]

As a normative matter, legislative regulation of third-party information would strike anyone who uses email or stores documents on the "cloud" as woefully insufficient. As I demonstrated, the SCA provides rather weak protections for a range of information whose physical analog the Fourth Amendment would undoubtedly protect. Moreover, the SCA's protections vary significantly based on time distinctions that may have been relevant when Congress enacted the Act but strike today's technology-users as a distinction without a difference. As a practical matter, lower court decisions extending Fourth Amendment protections to records governed by the SCA demonstrates that deference to Congress no longer represents a viable approach. Courts have and will continue to grapple with how to manage the intersection of the digital-era and third-party records, necessitating a reassessment of the third-party doctrine.

FOURTH AMENDMENT PROTECTION OF "DIGITAL PAPERS"

In this section, I argue that the Court ought to construe the Fourth Amendment's protection of "papers" to include "digital papers" stored or transmitted using third-party servers. I use the term "digital papers" to refer to data and information which third parties hold, store, or transport, *but do not create*. The paradigmatic example of "digital papers" are documents stored in the "cloud" and I submit that much of what has been traditionally understood as the "content" of communications—the body of emails and texts, for example—would similarly qualify as "digital papers." Courts could rely on traditional Fourth Amendment analogical reasoning to extend to the "digital papers" the same protections afforded to traditional papers. This approach

[277] Carpenter v. United States, 138 S.Ct. 2206, 2221 (2018).

would likely be sufficient to extend Fourth Amendment protections to some forms of "digital papers." However, as I noted in Part III, analogical reasoning may fall short where novel technology is concerned. Therefore, in this section, I propose a different, historically-based rationale that looks to the values underlying the Fourth Amendment's protection of "papers."

For much of the nation's history, personal documents, communications, photographs, and other personal "papers" and "effects" existed only in physical form. Today, cloud-computing technology is a central component of the digital world and what were once tangible "papers" stored in a file cabinet now exist as data on third-party servers. A defining aspect of the digital era "is the ability to 'outsource storage' to service providers like Google rather than saving things such as e-mails, photos, calendars, or other documents on a personal hard drive."[278] We are experiencing an "information migration," increasingly locating our letters, files, photos, and personal writings on corporate servers outside the home and office.[279] The growing reliance on "cloud computing" services raises the prospect that a broad reading of the third-party doctrine may result in a loss of Fourth Amendment protection for data in the cloud. Scholars rightly warn that if the third-party doctrine governs the Fourth Amendment's application to data stored in the cloud, "the results will be absurd."[280] Much of what individuals store on third-party servers would have once been protected "papers" or "effects" when stored in tangible form—letters, diaries, calendars, and the like. I argue that the history of the Fourth Amendment's protection of "papers" indicates a pathway to expanding the Fourth Amendment's protection of "papers" to include "digital papers."

---

[278] David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing Note*, 93 MINN. L. REV. 2205, 2215 (2009).
[279] Price, *supra* note 60, at 296.
[280] Jacob M. Small, *Storing Documents in the Cloud: Toward an Evidentiary Privilege Protecting Papers and Effects Stored on the Internet*, 23 GEO. MASON U. C.R. L.J. 255, 274 (2012–2013).

The history of the Fourth Amendment, particularly its protection of "papers," reveals "a long and storied relationship between the right to be free from unreasonable searches and seizures and the principles of free speech now enshrined in the First Amendment."[281] The link between the Fourth and First Amendments stemmed in large part from two colonial-era English cases—*Wilkes v. Woods* and *Entick v. Carrington*—and their impact on the Framer's intent in crafting the Fourth Amendment.

The *Wilkes v. Woods* grew out of the publication of the *North Briton* No. 45, an anonymous satirical pamphlet which criticized King George III. In response to the publication, the British Secretary of State, Lord Halifax, issued a general warrant commanding the king's messengers to seize the publications and printers and arrest the publishers. The general warrant resulted in the arrest of forty-nine individuals, including John Wilkes, a member of Parliament known for his criticism of the King's ministers. In addition to arresting Wilkes, the messengers seized his private papers, seeking to link him to the publication of the *North Briton.* Wilkes, in fact, had published the pamphlet and King George III ordered that he be tried for seditious libel. However, "as a sitting member of Parliament, Wilkes was judged to be immune from prosecution."[282]

Safe from prosecution, Wilkes sued the king's messengers for trespass and seizure of his papers. In resulting civil case, *Wilkes v. Woods*, Wilkes contended that the use of general warrants to seize personal papers represented a particularly abhorrent intrusion. "[O]f all offences that of a seizure of papers was the least capable of reparation," Wilkes declared, "for the promulgation of our most private concerns, affairs of the most secret personal nature, no

[281] Price, *supra* note 60, at 250.
[282] *Id.* at 252.

reparation whatsoever could be made."[283] The unrestrained ability of government to seize one's private papers "touched the liberty of every subject of this country, and if found to be legal, would shake that most precious inheritance of Englishmen," he proclaimed.[284]

Entick v. Carrington, which I introduced in Part I, also involved a civil suit against the king's messengers for trespass. In an effort to obtain evidence linking John Entick to the publication of a "very seditious" weekly paper known as the *Monitor*.[285] The king's messengers "read[] over, pry[ed] into, and examin[ed] [Entick's] private papers, books, etc." and carried them away.[286] Entick likened the seizure of his private papers to "racking his body to come at his secret thoughts."[287] He condemned the warrant, questioning what right Lord Halifax had to read and seize a man's private papers and thereby "see all a man's private letters of correspondence, family concerns, trade and business." Such power, Entick argued, "would be monstrous indeed!"[288]

In upholding the jury verdict in Entick's favor, Lord Camden referred to Entick's personal papers as "his dearest property."[289] A man's papers, Camden continued, "are so far from enduring a seizure, that *they will hardly bear an inspection*."[290] When a man's private papers are searched and seized, "his most valuable secrets are taken out of his possession."[291] Camden declared that "where private papers are removed and carried away, *the secret nature of those goods will be an aggravation of the trespass*, and demand more considerable damages in

[283] Wilkes v. Wood, 98 Eng. Rep. 489, 490 (1763)
[284] *Id.*
[285] *See* Entick v. Carrington*,* 19 Howell's State Trials, at 1031
[286] *See Id.*
[287] *Id.* at 1038
[288] *Id.*
[289] *Id.* at 1066
[290] *Id.* (emphasis added)
[291] *Id. at* 1064 (emphasis added)

that respect."[292] As William Stuntz notes, "the key to the cases was not the fact that the papers seized belonged to Entick and Wilkes; rather, the chief emphasis was on the fact that they were *papers*, and papers were of such a private nature."[293]

The *Wilkes* and *Entick* cases generated significant discussion in the American colonies. Colonial newspapers included "close coverage" of the *Wilkes* case "down to the names of counsel and the amount of damages, and includes multiple references, some by Wilkes himself, to *the distinct evil of seizing papers*."[294] John Adams, who is widely seen as the principle architect of the Fourth Amendment,[295] was "well aware" of the *Wilkes* and *Entick* cases and "the potential for unchecked powers of search and seizure to stifle speech as well as commerce."[296]

The particular concern for the security of private papers expressed in the *Wilkes* and *Entick* cases impacted the way in which Adams crafted Article 14 of the Massachusetts Declaration of Rights of 1780,[297] the language of which served as the basis for Fourth Amendment.[298] While the state constitutions of Virginia, Maryland, Delaware, and North

---

[292] *Id.* at 1066 (emphasis added)
[293] William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J 393, 399 (1995).
[294] Donald A. Dripps, *Dearest Property: Digital Evidence and the History of Private Papers as Special Objects of Search and Seizure Criminal Law*, 103 J. CRIM. L. & CRIMINOLOGY 49, 73–74 (2013) (providing a comprehensive summary of coverage of the Wilkes and Entick cases by colonial newspapers and publications).
[295] Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 979–80 (2011) ("Most of the language and structure of the Fourth Amendment was primarily the work of one man, John Adams… If the intent of the framers is a fundamental consideration in construing the Constitution, as the Court has repeatedly told us it is, then John Adams's knowledge and views should be considered an important source for understanding the Fourth Amendment.").
[296] Price, *supra* note 60, at 256.
[297] Article 14 stated:

> "Every subject has a right to be secure from all unreasonable searches and seizures of his person, his house, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation, and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the person or objects of search, arrest, or seizure; and no warrant ought to be issued but in cases, and with the formalities prescribed by the laws." (Mass. Declaration of Rights of 1780, art. XIV)

[298] Price, *supra* note 60, at 575.

Carolina abolished only general warrants,[299] Article 14 regulated search and seizures more broadly. Article 14 was the first to proclaim a "right to be secure" from "unreasonable" searches and seizures. Drawing from the Pennsylvania Constitution, Article 14 specifies four objects protected, including "papers" as a distinct category deserving of protection.[300]

The Fourth Amendment explicitly refers to "papers" because "the Founders understood the seizure of papers to be an outrageous abuse distinct from general warrants."[301] As the influential *Wilkes* and *Entick* cases demonstrate, "the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power."[302] The Fourth Amendment—and in particular its protection of "papers"— was crafted with the recognition "that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression."[303] Thus, there exists a close connection between the Fourth Amendment's guard against the search and seizure of "papers" and the principles of freedom of speech and association embodied in the First Amendment.

Indeed, for most of the Fourth Amendment's history, the Supreme Court interpreted the Fourth Amendment as "granting private papers an extraordinary exemption from seizure, even under warrant."[304] In the Court's 1886 decision in *Boyd*, the first important case interpreting the Amendment, the Court interpreted the Fourth Amendment to *prohibit* "compelling the production of [one's] private books and papers, to convict [one] of crime." Such a seizure, the *Boyd* Court asserted, "is contrary to the principles of a free government" and "cannot abide the

---

[299] *See* Va. Consta. of 1776 art. X; Md. Consta. of 1776 art. XXIII; Del. Consta. of 1776 art. XVII; N.C. Consta. of 1776 art. XI.
[300] *See* Clancy, *supra* note 297, at 1028.; Pa. Const. of 1776 art. X ("[T]he people have a right to hold themselves, their houses, papers, and possessions free from search and seizure.")
[301] Dripps, *supra* note 296, at 52.
[302] Marcus v. Search Warrant, 367 U.S. 717, 724 (1961).
[303] *Id.* at 729.
[304] Dripps, *supra* note 296, at 50.

pure atmosphere of political liberty and personal freedom."[305] The holding in *Boyd* established the basis for the "mere evidence" rule, which prohibited the government from seizing one's papers to use as evidence at trial.[306] In solidifying the "mere evidence" rule in a subsequent ruling, the Court singled out "papers" as "property of a most important character."[307] Though the Court eventually abandoned the "mere evidence" rule in 1967,[308] for more than 80 years, the Fourth Amendment was understood to afford heightened protection to "papers."

The history behind the Fourth Amendment's inclusion of "papers" as a distinct category of protected item demonstrates that the Framers sought to protect "papers" because of their fundamentally expressive and associational nature. In seeking to determine the extent to which the Fourth Amendment protects documents stored in the "cloud" or communications transmitted by third party services, courts should focus to the expressive and associational character of those categories of items. Rather than pointing to the structural similarities between traditional papers and "digital papers" to justify an extension of Fourth Amendment protections, courts should instead afford protections to categories of "digital papers" that are significantly expressive and associational in nature.[309]

Construing the Fourth Amendment's protection of "papers" to include "digital papers" based on their common expressive and associational value would not represent a novel method of constitutional interpretation. Indeed, the interpretation of the scope of the Amendment's

---

[305] Boyd v. United States, 116 U.S. 616, 631–32 (1886).
[306] Price, *supra* note 60, at 272.
[307] Gouled v. United States, 255 U.S. 298, 310 (1921).
[308] *See* Warden v. Hayden, 387 U.S. 294 (1967) (overruling the "mere evidence" rule) ("The Fourth Amendment allows intrusions upon privacy under these circumstances, and there is no viable reason to distinguish intrusions to secure 'mere evidence' from intrusions to secure fruits, instrumentalities, or contraband.").
[309] *See* Richards, *supra* note 222, at 1487 ("In translating the Fourth Amendment to the cloud, we should focus on the normative values that we want to protect. In particular, we should look to the Fourth Amendment's long association with the First Amendment as a guide to ensuring that its enduring values survive the translation to digital form.").

reference to "houses" has developed in much the same way.[310] Interpreting the term "houses" literally would severely constrict the scope of search and seizure protections. The Court, however, has read the term to include things beyond residential structures, finding that the Fourth Amendment applies to garages,[311] rented homes,[312] hotel suites,[313] factories and places of business,[314] private offices,[315] and mobile homes.[316] Similarly, the protection afforded to "houses" has long been understood as extending to the area surrounding the home itself, known as the "curtilage" of the home. The protection afforded to "houses" extends to this area because the curtilage "is intimately linked to the home, both physically and psychologically, and is where privacy expectations are most heightened."[317] In interpreting the term, the Court has also looked to the historical purpose of the protection of "houses." For example, in concluding that "it is untenable that the ban on warrantless searches was not intended to shield places of business as well as of residence," the Court noted that "to hold otherwise would belie the origin of that Amendment, and the American colonial experience."[318]

Thus, just as the historical interests motivating the protection of "houses" have served as a basis for extending the protection to areas outside the literal meaning of the term "houses," the recognition that the expressive and associational interest at the core of Fourth Amendment "papers" is equally present in "digital papers" provides a convincing basis for extending to the latter the same protection afforded to the former. Of course, much of the data that is disclosed to third parties may be expressive or associational to varying degrees; to what degree particular

---

[310] Price, *supra* note 60, at 271–72.
[311] *See* Taylor v. United States, 286 U.S. 1,5-6 (1932).
[312] *See* Chapman v. United States, 365 U.S. 610, 616-17 (1961).
[313] *See* Stoner v. California, 376 U.S. 483, 490 (1964).
[314] *See* Dow Chem. Co. v. United States, 476 U.S. 227, 236 (1986).
[315] *See* O'Connor v. Ortega, 480 U.S. 709, 718 (1987).
[316] *See* Soldal v. Cook Cty., Ill., 506 U.S. 56, 61 (1992).
[317] *See* Florida v. Jardines, 1415 (internal citations omitted).
[318] Marshall v. Barlow's, Inc., 436 U.S. 307, 311–12 (1978).

information or data held by third parties implicates a First Amendment interest could serve as one factor in determining whether Fourth Amendment protection applies. However, it is important to clarify that the rationale that I have articulated here does not involve weighing the significance of First Amendment interests against other factors. Rather, I contend that there is a subset of information and data—"digital papers"—for which the expressive and associational interest is *so fundamental* as to be dispositive of the Fourth Amendment question. For these types of information and data, the expressive and associational interest is as inherent and profound as it is with respect to traditional "papers."

Given this definition, in all likelihood relatively few types of third-party disclosures will qualify as "digital papers." However, three types of third-party disclosures have a strong claim to the status of "digital paper": things stored by a third party but which the third party had no hand in creating (such as a photocopy stored in the "cloud"); one's own writings or creations stored by a third party but which the third party had no hand in creating (such as a diary maintained on Google Drive); and communications directed to another which are transmitted through a third party's systems but which the third party had no hand in creating (such as emails and text messages). Of course, other types of data, information, and disclosures may come under the scope of "digital papers" and a focus on the expressive and associational interest involved will allow courts to determine when such cases occur. Even so, most forms of third-party disclosure, particularly passively conveyed information and data that exist in a third party's own records, will fall outside the scope of "digital papers." In these instances, a different and likely more complicated approach is required.

CARPENTER V. UNITED STATES: A NEW APPROACH TO PROTECTING METADATA?

When the Supreme Court handed down its decision in *Carpenter v. United States* in June of 2018, scholars and legal commentators were quick to recognize the groundbreaking nature of the ruling. In a *New York Times* opinion piece published on the day of the ruling, legal scholars Alex Abdo and Kate Klonick suggested that *Carpenter* "may be the most important privacy case of the digital era."[319] In the short time since the ruling, appreciation for the significance of the decision has only increased. Some have gone so far as to call *Carpenter* "the most important Fourth Amendment decision since *Katz v. United States*."[320]

Carpenter's outcome, which imposes a warrant requirement when the government seeks to compel a cell phone service provider to produce a subscriber's cell-site location information, certainly constitutes a major win for privacy advocates. Scholars contend that the decision represents "a revolution of legal reasoning"[321] and "signals a major break from the traditional understanding" of Fourth Amendment protection.[322] In the following section, I outline the facts of the case and then deconstruct the *Carpenter* majority's reasoning. I argue that while the decision undoubtedly represents a shift in the third-party doctrine, its implications for the Fourth Amendment's application to other types of third-party records remains unclear. I consider where the third-party doctrine stands after *Carpenter* and what questions it raises for the application of the doctrine in other contexts.

---

[319] Alex Abdo & Kate Klonick, *Opinion | The Supreme Court Takes On the Police Use of Cellphone Records*, THE NEW YORK TIMES, Jun. 81, 2018, https://www.nytimes.com/2018/06/22/opinion/carpenter-supreme-court-cellphone-records.html.
[320] Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J. L. & TECH. 1 (2019).
[321] *Id.* at 5.
[322] Orin S. Kerr, *Implementing Carpenter*, *in* THE DIGITAL FOURTH AMENDMENT (FORTHCOMING) 6 (2018).

The Carpenter *Majority's Reasoning*

In 2011, the government sought access to 152 days of historical cell site location information ("CSLI") for Timothy Carpenter and other suspects in a string of robberies. Rather than seek a warrant to access the records, the government instead obtained an order under §2703(d) of the SCA and compelled Carpenter's cell phone service providers to produce 127 days of cell-site records, which disclosed his approximate location when making or receiving a phone call. Carpenter moved to suppress the CSLI records on the theory that they were obtained without a warrant and in violation of the Fourth Amendment. The district court denied Carpenter's motion and he was later convicted of six robberies under the Hobbs Act along with five other counts. The Sixth Circuit Court of Appeals affirmed the judgement below, holding that the collection of CSLI records did not constitute a "search" because it fell squarely within the "third-party doctrine." Carpenter appealed to the Supreme Court. In a 5-4 decision, the Court ruled for Carpenter.

Writing for the majority, Chief Justice Roberts began by observing that the kind of data at issue in *Carpenter* "does not fit neatly under existing precedents."[323] Personal location information held by a third party implicates two lines of Fourth Amendment cases. One set of cases "addresses a person's expectation of privacy in his physical location and movements"[324] while a second set—the third-party doctrine cases—"draw[] a line between what a person keeps to himself and what he shares with others."[325] The majority's reasoning took each set of precedent in turn.

[323] Carpenter v. United States, 138 S.Ct. 2206, 2214 (2018).
[324] *Id.* at 2215.
[325] *Id.* at 2216.

The majority began with the question of "reasonable expectation of privacy." An individual, the Court concluded, "maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI" and therefore "the location information obtained from Carpenter's wireless carriers was the product of a search."[326] In reaching this conclusion, the majority first focused on the revealing nature of location data. Records of one's movements "hold for many Americans the privacies of life" and "provide[] an intimate window into a person's life."[327]The Court emphasized that a log of one's locations reveals "not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[328]

The second step in the majority's reasoning relied heavily on two concurring opinions in *United States v. Jones*. In *Jones*, "agents installed a GPS tracking device on the undercarriage of [Jones'] Jeep" without a valid warrant and "over the next 28 days, the Government used the device to track the vehicle's movements."[329] The GPS established the location of the car within 50 to 100 feet and "relayed more than 2,000 pages of data over the 4-week period."[330] In a unanimous ruling, the Court held that the warrantless installation of the GPS constituted a search in violation of the Fourth Amendment.[331] The majority opinion, written by Justice Scalia, located the Fourth Amendment violation in the government's physical intrusion or trespass of Jones' property.[332] Justice Alito, joined by three justices, concurred in judgement but wrote separately, contending that the Court should have analyzed the Fourth Amendment question "by asking

[326] *Id.* at 2217.
[327] *Id.* (internal quotations omitted).
[328] *Id.*; (quoting United States v. Jones, 132 S. Ct. 945, 415 [2012] [Sotomator, J., concurring]).
[329] *Jones*, 132 S. Ct. at 403.
[330] *Id.*
[331] *Id.* at 404–5.
[332] *Id.* ("The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted.").

whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove."[333] Justice Sotomayor filed a separate concurrence, taking issue with some aspects of Justice Alito's concurrence, but agreeing that, "at the very least, longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[334]

Pointing to the concurrences in *Jones*, the Court concluded that "a majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements." Writing for the majority, Chief Justice Roberts began by making an observation about the state of things "[p]rior to the digital age."[335] For much of the nation's history, law enforcement faced practical limitations to its ability to track a suspect for an extended period of time. While agents may have been able to monitor and record an individual's movements for a short stretch, to do so for a considerable length of time would be challenging and costly. Such operations were therefore "rarely undertaken." As a result, "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" a suspect made over a very long period.[336] Moreover, any effort to reconstruct a suspect's movements "were limited by a dearth of records and the frailties of recollection."[337]

Enter technology. The near-universal use of cell phones has fundamentally altered the state of play, the majority argued. Cell phones have produced location records that were simply not unavailable in the pre-digital world. Additionally, generating such records is "remarkably

[333] *Id.* at 419 (Alito, J., concurring in judgement).
[334] *Id.* at 415 (Sotomayor, J., concurring).
[335] Carpenter v. United States, 138 S.Ct. 2206, 2217 (2018).
[336] *Id.*; (*Jones*, 132 S. Ct. at 430 [Alito, J., concurring in judgement]).
[337] *Carpenter*, 138 S.Ct. at 2218.

easy, cheap, and efficient compared to traditional investigative tools." Moreover, due to the retrospective property of these location records, one "can now travel back in time to retrace a person's whereabouts."[338] According to the Court, the shift from a world in which location tracking was challenging, costly, and rare to one in which location tracking is easy, inexpensive, and common "contravene[d] that expectation" of privacy which society maintained in the pre-digital era.

Having concluded that individuals maintain a reasonable expectation of privacy in records of their movements, the Court turned to the second set of relevant Fourth Amendment precedent: the third-party doctrine. According to the majority, the third-party doctrine "partly stems from the notion that an individual has a *reduced* expectation of privacy in information knowingly shared with another."[339] However, the fact that a privacy interest is diminished "does not mean that the Fourth Amendment falls out of the picture entirely," the Court adds.[340] With this definition of third-party doctrine in hand, the Court turned to the government's principle assertion that the doctrine dictates the outcome of *Carpenter*.[341] At the outset, the majority acknowledged that because an individual discloses his location to his cell phone service provider, "the third-party principles of *Smith* and *Miller*" become implicated.[342] While accepting that the third-party doctrine applies to telephone numbers and bank records, the Court concluded that the logic of the doctrine does not obviously extend to cell-site location information, which it described as a "qualitatively different category" of records.[343]

[338] *Id.*
[339] *Id.* at 2219 (emphasis added).
[340] *Id.*; (quoting Riley v. California, 134 S. Ct. 2473, 2488 [2014]).
[341] *Carpenter*, 138 S.Ct. at 2219.
[342] *Id.* at 2216.
[343] *Id.* at 2217.

The Court stressed that *Carpenter* involved "novel circumstances."[344] Cell-site location records are of a "unique nature,"[345] constituting "an entirely different species of business record"[346] and implicating "a distinct category of information."[347] The majority contended that cell-site location records are distinguishable on the two measures employed in *Smith* and *Miller*. First, the Court asserted that the information and records at issue *Smith* and *Miller* are limited in their revealing nature. *Smith* noted the "limited capabilities of a pen register,"[348] which expose only the numbers dialed. "Call logs reveal little in the way of identifying information," the *Carpenter* majority suggested.[349] Similarly, *Miller* noted that the checks at issue were "not confidential communications but negotiable instruments to be used in commercial transactions."[350] In contrast, the Court asserted that "there are no comparable limitations on the revealing nature of [cell-site records]."[351] Second, the Court reasoned that cell-site location information is further differentiated because users do not "voluntarily expose" their location to their service provider in any meaningful sense. Cell phones and the functions they offer play such a central role in ordinary life "that carrying one is indispensable to participation in modern society." Moreover, a cell phone conveys location information to the service provider "by dint of its operation."[352] Incoming communications, automatic data connections, notification—indeed, nearly all activity—generates cell-site location data, even without the user taking any affirmative

[344] *Id.* at 2219.
[345] *Id.*
[346] *Id.* at 2222.
[347] *Id.* at 2219.
[348] *Id.*; (quoting Smith v. Maryland, 442 U.S. 735, 742 [1979]).
[349] *Carpenter*, 138 S.Ct. at 2219; (quoting Riley v. California, 134 S. Ct. 2473, 2493 [2014]) (internal quotations omitted).
[350] *Carpenter*, 138 S.Ct. at 2219; (quoting United States v. Miller, 425 U.S. 435, 442 [1976]).
[351] *Carpenter*, 138 S.Ct. at 2219.
[352] *Id.* at 2220.

action. Thus, the majority reasoned, a cell phone user does not in any actual sense "voluntarily 'assume the risk' of turning over a comprehensive dossier of his physical movements."[353]

Though leaving *Smith* and *Miller* intact, the Court declined to extend the third-party doctrine to the cell-site location information in *Carpenter*, concluding that doing so would amount to "a significant extension," not a "straightforward application," of the third-party doctrine to "a distinct category of information."[354] Due to the "unique nature of cell phone location information," the Court concluded, "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[355] The acquisition of Carpenter's cell phone location records constituted a search; in this case and in general, the government must obtain a warrant supported by probable cause to acquire such records.[356]

Carpenter—*A Clear Shift with Unclear Implications*

What does *Carpenter* mean for the Fourth Amendment's application to other types of third-party records? Does Carpenter provide a new framework for assessing which third-party records deserve protection and which continue to be governed by the third-party doctrine? *Carpenter*'s implications remain somewhat unclear. However, the Court's reasoning introduces a new approach to the "expectation of privacy" inquiry, represents a notable shift from the traditional understanding of the third-party doctrine, and relies of a measure of voluntariness that has implications for the doctrine's application in the future.

[353] *Id.*; (quoting *Smith*, 442 U.S. at 745).
[354] *Carpenter*, 138 S.Ct. at 2219–20.
[355] *Id.* at 2217.
[356] *Id.* at 2221.

Carpenter*'s "Expectation of Privacy" Inquiry*

The first important aspect of *Carpenter*'s 'expectation of privacy' inquiry is in its treatment of the object of the expectation—cell-site location data. The Court asked not whether Carpenter maintained an expectation of privacy in a record of his location at any one particular moment but rather whether he had such an expectation in the whole of his movement—that is, the *aggregation* of his particular location at many moments in time. The question is not about "a person's movement at a particular time" but rather "about a detailed *chronicle* of a person's physical presence *compiled* every day, every moment, over several years."[357] The inquiry, therefore, focused on cell-site location information as *a category of information*. Approaching the question from this perspective has obvious appeal: after all, the records in *Carpenter*—and third-party records in general—represent an aggregation of information.

Second, while the *Carpenter* majority quoted heavily from Justice Alito's *Jones* concurrence, it proceeded to articulate a "novel way" of establishing the existence of a reasonable expectation of privacy.[358] Recall how the Court came to find an 'reasonable expectation of privacy' in the whole of one's movements. "Prior to the digital age," law enforcement simply could not endlessly follow an individual and record his movements; therefore, society expected that law enforcement would not and could not create such a record. Permitting them to access cell-site records "contravenes" that expectation, the Court reasoned.[359] Kerr contends that this component represents the "key move" of the *Carpenter* decision: the Court reasoned that the capability of modern technology eliminated the expectation of privacy that society maintained before.[360] This approach to the reasonable expectation question is

[357] *Id.* at 2220.
[358] Kerr, *Implementing Carpenter*, *supra* note 324, at 7.
[359] *Carpenter*, 138 S.Ct. at 2217.
[360] Kerr, *Implementing Carpenter*, *supra* note 324, at 7.

markedly different from the one ordinarily followed. Under the *Katz* test, courts looked to whether an action violated one's reasonable expectation of privacy in a specific thing or area. "*Carpenter* asks a different question: Has technology changed expectations of *what the police can do*?"[361] In considering the broader implications of *Carpenter*, one question that arises is the extent to which the logic of the decision is limited to third-party records that result only from "seismic shifts in digital technology."[362] Kerr contends that the major shift in technology represents a central part of the Court's reasoning, suggesting that in applying the logic of *Carpenter* to other third-party records, the "first requirement…should be that the records collected are available because of digital technology."[363] Indeed, the Court described cell-site records as "an entirely different species"[364] of record, which certainly lends support to Kerr's view that the decision is premised "on the theory that digital records are *categorically* different."[365] This limitation would, of course, decrease the range of third-party records to which the *Carpenter* Court's reasoning might apply.

Carpenter*'s Redefinition of the Third-Party Doctrine*

The Court articulated a formulation of the third-party doctrine that was subtly yet meaningfully different from the prevailing interpretation. *Carpenter* fundamentally redefines the meaning of the third-party doctrine by holding that "an individual has a *reduced* expectation of privacy in information knowingly shared with another."[366] The notion that disclosure only *reduces* rather than *entirely eliminates* an expectation of privacy represents a deviation from the

[361] *Id.* (emphasis in original).
[362] *Carpenter*, 138 S.Ct. at 2219.
[363] Kerr, *Implementing Carpenter*, *supra* note 324, at 12.
[364] *Carpenter*, 138 S.Ct. at 2222.
[365] Kerr, *Implementing Carpenter*, *supra* note 324, at 12 (emphasis added).
[366] *Carpenter*, 138 S.Ct. at 2219 (emphasis added).

typical understanding of the third-party doctrine. Most importantly, this interpretation transforms the way in which the third-party doctrine functions, shifting it from a categorical rule to a balancing test. Consider the common understanding of the doctrine: "By disclosing to a third party, the subject gives up *all* of his Fourth Amendment rights in the information revealed…In other words, a person *cannot* have a reasonable expectation of privacy in information disclosed to a third party. The Fourth Amendment simply does not apply."[367]Additionally, "[r]ather than acknowledge gradations in the sensitivity of information citizens disclose to others," the doctrine has generally been understood to dictate that disclosure vitiates any reasonable expectation of privacy in the information revealed, "no matter how sensitive that information may be."[368] This interpretation of the doctrine—one which reads *Miller* and *Smith* as establishing a categorical rule—has long been the dominant understanding among scholars and jurists alike.[369]

Carpenter rightly rejects the categorical reading of the doctrine and properly frames third-party disclosure as a factor that tends to reduce an individual's expectation of privacy. Understanding the doctrine as categorical doctrine cannot be squared with the fact that both *Smith* and *Miller* considered whether the individual possessed a "reasonable expectation of privacy" in the *contents* of the records. In *Miller*, for example, the Court reasoned that it "must examine the nature of the particular documents sought to be protected in order to determine

[367] Kerr, *supra* note 96, at 563 (emphasis added); *See* Solove, *supra* note 7, at 1135 (interpreting Miller and Smith to "establish a general rule that if information is in the hands of third parties, then an individual can have no reasonable expectation of privacy in that information, which means that the Fourth Amendment does not apply.").
[368] Michael Gentithes, *The End of Miller's Time: How Sensitivity Can Categorize Third-Party Data After Carpenter*, GA. L. REV. 2, 13 (2019).
[369] See e.g. *Ulbricht*, 858 F. 3d 71, at 96 (2nd Cir. 2017) (citing *Miller* and *Smith* in concluding that "[t]he Supreme Court has long held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."); United States v. Caira, 833 F. 3d 803, at 806 (7th Cir. 2016) (interpreting *Miller* and *Smith* as establishing "a bright-line application of the reasonable-expectation-of-privacy test."); *Jones*, 132 S. Ct. at 417 (Sotomayor, J., concurring) (citing *Miller* and *Smith* as establishing "the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.")

whether there is a legitimate 'expectation of privacy' concerning their contents."[370] If the third-party doctrine were entirely categorical, it would seem unnecessary for the Court to inquire into whether one has a reasonable expectation of privacy in the information voluntarily conveyed to another. The act of disclosing would be dispositive of the Fourth Amendment question. However, the doctrine now appears to function as somewhat of a balancing test, though the Court did not indicate what factors might be balanced in future cases beyond voluntariness, comprehensiveness, and the revealing nature of the information.

Carpenter*'s Measure of Voluntariness*

Carpenter's broader implications may depend in part on how lower courts understand the Court's discussion of voluntariness. As noted, the Court provided two reasons to differentiate the voluntariness of the disclosure in *Carpenter* from that in *Smith* and *Miller*: first, carrying a cell phone is "indispensable to participation in modern society" and second, cell phone transmits location information "without any affirmative act on the part of the user beyond powering up."[371] With the first reason, the Court makes a normative judgement: modern Americans rely greatly on the device and the services it provides. The recognition of what one might call "societal necessity," while certainly welcome, does make it somewhat difficult to determine how far *Carpenter* might extend. While the Court uses societal necessity to differentiate cell-site records from *Smith* and *Miller*, the distinction appears to be a slim one. Indeed, the dissenters in both cases raised the same points about societal necessity. With reference to landline telephones in *Smith*, Justice Marshall asserted that "unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of

[370] United States v. Miller, 425 U.S. 435, 442 (1976).
[371] *Carpenter*, 138 S.Ct. at 2220.

surveillance."[372] In *Miller*, Justice Brennan offered a similar observation about banks: "For all practical purposes, the disclosure [of one's] financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account."[373] What then is the threshold something must meet to quality as societal necessity? *Carpenter* does not elaborate, leaving a challenging normative evaluation for lower courts considering how *Carpenter* ought to impact the Fourth Amendment protection afforded to other third-party records.

The Court's second reason—that cell phones can disclose the user's location automatically—recognizes the difference in knowledge that I identified earlier in critiquing the "assumption of risk" rationale. When *combined* with the first reason, the Court provides a fairly solid basis on which to differentiate cell-site location information from the records in *Smith* and *Miller*. However, by providing two reasons for excepting cell-site information from the third-party doctrine, the Court raises another question: is each reason *independently* sufficient to undermine the voluntariness of a third-party disclosure or rather must *both* be true to deem a disclosure involuntary and escape the third-party doctrine? *Carpenter* leaves this question unanswered, making more uncertain if and how the Court's reasoning might impact other third-party records since the likely outcome would seem to shift depending on whether lower courts understand the two factors to function together or independently. If a disclosure must be *both* societally necessary *and* automatic, *Carpenter*'s implications become rather limited. Credit cards, for example, would seem to qualify as societally necessary but not automatic. Smart watches, however, may disclose location or health information automatically but certainly appear less necessary to participation in modern life than cell phones (or credit cards, for that matter).

---

[372] Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting).
[373] *Miller*, 425 U.S. at 451 (Brennan, J., dissenting) (citation omitted).

On the other hand, if lower courts understood societal necessity and automatic disclosure as functioning *independently*, *Carpenter* may have wide-reaching implications, extending Fourth Amendment protections to records resulting from the use of credit cards, smart watches, and internet browsing, for instance. Yet, this interpretation might also call into question the Court's holdings in *Smith* and *Miller* because both phones and banks are arguably societally necessary, as the dissenters in both cases suggested.[374]

CONCLUSION

The third-party doctrine poses a threat to the Fourth Amendment's ability to meaningfully protect privacy in the digital era. From the start, the doctrine rested on an unstable foundation, standing at odds with the guiding framework of *Katz* and relying on an "assumption of risk" rationale that translates poorly to the context in which the government *compels* third parties to reveal information and to an era in which using technology is unavoidable. In the digital era, where revealing information to third parties is nearly unavoidable, the third-party doctrine exposes the most intimate parts of an individual's life to government observation. Distinguishing between content and non-content no longer serves to distinguish between that which the Fourth Amendment ought to protect and that which the third-party doctrine governs. In the context of modern technology, the lines become blurred. Legislative fixes prove similarly inadequate to patch the holes in Fourth Amendment protection that the third-party doctrine has made. Like the distinction between content and non-content, statutory distinction quickly become outdated as technology becomes more complex.

[374] *See* Evan Caminker, *Location Tracking and Digital Data: Can Carpenter Build a Stable Privacy Doctrine?*, 2019 SUPREME COURT REVIEW 28 (2019).

The third-party doctrine requires a constitutional solution. In some instances, the Fourth Amendment's historical role in protecting First Amendment associational and expressive interests provides a guide. As I have argued, this link provides a basis for expanding the definition of Fourth Amendment "papers" to include "digital papers" for which the associational and expressive interest is equally strong. Modernizing the Fourth Amendment will prove to be a difficult task, one which cannot be resolved by rethinking the definition of "papers" alone. The Court's recent ruling in *Carpenter v. United States* provides a starting point. Analyzing the Court's reasoning, I have identified questions and factors that ought to inform future cases and which deserve scholarly focus.

The third-party doctrine implicates far more than just the rights of the criminally accused or targets of government investigation. At its core, the protection against "unreasonable searches and seizures" enshrined in the Fourth Amendment relates to the balance of power between individuals and the government; it implicates the interests of the innocent as much as it does the interests of the accused. Reforming the third-party doctrine ensures that the Fourth Amendment's protection does not diminish with technological progress. Justice Brandeis' question remains as relevant as ever: "Can it be that the Constitution affords no protection against such invasions of individual security?"[375]

[375] Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

BIBLIOGRAPHY

Abdo, Alex, and Kate Klonick. "Opinion | The Supreme Court Takes On the Police Use of Cellphone Records." *The New York Times*, June 81, 2018, sec. Opinion. https://www.nytimes.com/2018/06/22/opinion/carpenter-supreme-court-cellphone-records.html.

Alter, Alexandra. "Your E-Book Is Reading You." *Wall Street Journal*, July 0, 2012, sec. Life and Style. https://www.wsj.com/articles/SB10001424052702304870304577490950051438304.

Amar, Akhil Reed. "Fourth Amendment First Principles." *Harv. L. Rev.* 107, no. 4 (1994): 757–819.

Arcila, Fabio Jr. "GPS Tracking out of Fourth Amendment Dead Ends: United States v. Jones and the Katz Conundrum." *N.C. L. Rev.* 91 (2012): 1–78.

Ashdown, Gerald G. "Fourth Amendment and the Legitimate Expectation of Privacy, The." *Vand. L. Rev.* 34 (1981): 1289–1346.

Backer, Joy L. "Stop Waiting on the World to Change: Compelled Disclosure of Email Content under the Stored Communications Act Note." *Suffolk U. L. Rev.* 48 (2015): 379–400.

Bambauer, Jane. "Other People's Papers." *Tex. L. Rev.* 94, no. 2 (2015): 205–64.

Barrett, Edward L. "Personal Rights, Property Rights, and the Fourth Amendment." *The Supreme Court Review* 1960 (1960): 46–74.

Baude, William, and James Y. Stern. "The Positive Law Model of the Fourth Amendment." *Harv. L. Rev.* 129 (2016): 1821–89.

Bedi, Monu. "Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply." *B.C. L. Rev.* 54 (2013): 1–72.

———. "The Fourth Amendment Disclosure Doctrines Symposium: Big Data, National Security, and the Fourth Amendment." *Wm. & Mary Bill Rts. J.* 26 (2017–2018): 461–94.

Bellia, Patricia L. "The Memory Gap in Surveillance Law Symposium: Surveillance." *U. Chi. L. Rev.* 75 (2008): 137–80.

Bellovin, Steven M., Matt Blaze, Susan Landau, and Stephanie K. Pell. "It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law." *Harv. J. L. & Tech.* 30, no. 1 (2016): 1–102.

Blass, Megan. "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." *Hastings Const. L.Q.* 42 (2014–2015): 577–600.

Blitz, Marc Jonathan. "The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Space." *Am. U. L. Rev.* 63 (2013–2014): 21–86.

Brennan, Christopher R. "Katz Cradle: Holding on to Fourth Amendment Parity in an Age of Evolving Electronic Communication Note." *Wm. & Mary L. Rev.* 53 (2011–2012): 1797–1824.

Brenner, Susan W., and Leo L. Clarke. "Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data." *J.L. & Pol'y* 14, no. 1 (2006): 211–80.

Brill, Adam W. "Kyllo v. United States: Is the Court's Bright-Line Rule on Thermal Imaging Written in Disappearing Ink Case Note." *Ark. L. Rev.* 56 (2003–2004): 431–54.

Caminker, Evan. “Location Tracking and Digital Data: Can Carpenter Build a Stable Privacy Doctrine?” *Supreme Court Review* 2019 (2019). https://papers.ssrn.com/abstract=3304775.
Casey, Timothy. “Electronic Surveillance and the Right to Be Secure Symposium - Katz v. U.S.: 40 Years Later: Rights and Remedies.” *U.C. Davis L. Rev.* 41 (2007–2008): 977–1034.
Chambers, John Grayson. “Simon Didn’t Say: When Reconstruction of a Private Search Goes Awry under the Private Search Doctrine Notes.” *Ga. L. Rev.* 51 (2016–2017): 557–84.
Chokshi, Niraj. “Amazon Knows Why Alexa Was Laughing at Its Customers.” *The New York Times*, March 1, 2018, sec. Business. https://www.nytimes.com/2018/03/08/business/alexa-laugh-amazon-echo.html.
———. “Most Americans See Artificial Intelligence as a Threat to Jobs (Just Not Theirs).” *The New York Times*, June 184, 2018, sec. U.S. https://www.nytimes.com/2018/03/06/us/artificial-intelligence-jobs.html.
Clancy, Thomas K. “Coping with Technological Change: Kyllo and the Proper Analytical Structure to Measure the Scope of Fourth Amendment Rights Essay.” *Miss. L.J.* 72 (2002–2003): 525–64.
———. “The Framers’ Intent: John Adams, His Era, and the Fourth Amendment.” *Ind. L.J.* 86 (2011): 979–1062.
———. “What Does the Fourth Amendment Protect: Property, Privacy, or Security?” *Wake Forest L. Rev.* 33, no. 2 (1998): 307–70.
———. “What Is a Search within the Meaning of the Fourth Amendment.” *Alb. L. Rev.* 70 (2006): 1–54.
Cloud, Morgan. “Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment.” *Miss. L.J.* 72, no. 1 (2002): 5–50.
———. “The Fourth Amendment during the Lochner Era: Privacy, Property, and Liberty in Constitutional Theory.” *Stan. L. Rev.* 48, no. 3 (1996): 555–631.
Cohn, Cindy. “Protecting the Fourth Amendment in the Information Age: A Response to Robert Litt.” *Yale L.J. F.* 126 (2016–2017): 107–17.
Colb, Sherry F. “A World without Privacy: Why Property Does Not Define the Limits of the Right against Unreasonable Searches and Seizures Correspondence.” *Mich. L. Rev.* 102 (2003–2004): 889–903.
———. “What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy.” *Stan. L. Rev.* 55, no. 1 (2002): 119–90.
Cole, Kevin. “Privileges, Justifications, and the Positive Law Model of the Fourth Amendment,” San Diego Legal Studies Paper No. 18-334, 2018. https://papers.ssrn.com/abstract=3131246.
Congressional Research Service, Library of Congress. *The Constitution of the United States of America: Analysis and Interpretation*. Centennial Edition (S. Doc. 112-9). Washington: U.S. Government Printing Office. 2017.
Conley, Chris. “Non-Content Is Not Non-Sensitive: Moving beyond the Content/Non-Content Distinction.” *Santa Clara L. Rev.* 54 (2014): 821–42.
Conom, Derek T. “Sense-Enhancing Technology and the Search in the Wake of Kyllo v. United States: Will Prevalence Kill Privacy Comments.” *Willamette L. Rev.* 41 (2005): 749–76.
Cooley, Thomas McIntyre. *A Treatise on the Constitutional Limitations Which Rest upon the Legislative Power of the States of the American Union.* 6th ed., with Large additions, Giving the results of the recent cases /. Boston : 1890.

Cosby, Teresa Nesbitt. “The Expectation of Privacy: An Unreasonable Standard in an Era of Rapid Innovations in Technology.” *Charleston L. Rev.* 12, no. 3 (2018): 337–52.
Couillard, David A. “Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing Note.” *Minn. L. Rev.* 93, no. 6 (2009): 2205–39.
Crocker, Thomas P. “The Political Fourth Amendment.” *Wash. U. L. Rev.* 88 (2010–2011): 303–80.
Crowther, Brandon T. “(Un)Reasonable Expectation of Digital Privacy.” *BYU L. Rev.* 2012, no. 1 (2012): 343–70.
D’Addario, Alicia A. “Policing Protest: Protecting Dissent and Preventing Violence through First and Fourth Amendment Law.” *N.Y.U. Rev. L. & Soc. Change* 31 (2006–2007): 97–130.
Davies, Thomas Y. “Recovering the Original Fourth Amendment.” *Mich. L. Rev.* 98, no. 3 (1999): 547–750.
———. “The Supreme Court Giveth and the Supreme Court Taketh Away: The Century of Fourth Amendment Search and Seizure Doctrine Centennial Symposium: A Century of Criminal Justice - Justice in Action.” *J. Crim. L. & Criminology* 100 (2010): 933–1042.
DeFilippis, Andrew J. “Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence Note.” *Yale L.J.* 115 (2005–2006): 1086–1121.
Donohue, Laura K. “Bulk Metadata Collection: Statutory and Constitutional Considerations.” *Harv. J. L. & Pub. Pol’y* 37 (2014): 757–900.
———. “The Fourth Amendment in a Digital World.” *N.Y.U. Ann. Surv. Am. L.* 71 (2017): 553–686.
Dripps, Donald A. “Dearest Property: Digital Evidence and the History of Private Papers as Special Objects of Search and Seizure Criminal Law.” *J. Crim. L. & Criminology* 103 (2013): 49–110.
Epstein, Richard A. “Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations.” *Berkeley Tech. L.J.* 24, no. 1 (2009): 1199–1228.
Ettinger, Craig. “Does the History behind the Adoption of the Fourth Amendment Demand Abolishing the Third-Party Doctrine.” *Geo. Mason U. C.R. L.J.* 29 (2018–2019): 1–42.
Ferguson, Andrew Guthrie. “Personal Curtilage: Fourth Amendment Security in Public.” *Wm. & Mary L. Rev.* 55 (2013–2014): 1283–1364.
———. “The Smart Fourth Amendment.” *Cornell L. Rev.* 102 (2016–2017): 547–632.
Freiwald, Susan, and Stephen Wm. Smith. “The Carpenter Chronicle: A near-Perfect Surveillance The Supreme Court 2017 Term: Comments.” *Harv. L. Rev.* 132 (2018–2019): 205–35.
Friedland, Steven I. “Drinking from the Fire Hose: How Massive Self-Surveillance from the Internet of Things Is Changing the Face of Privacy 2017 Evolving Investigative Technologies and the Law Symposium.” *W. Va. L. Rev.* 119 (2016–2017): 891–914.
Friedman, Barry, and Cynthia Benin Stein. “Redefining What’s Resasonable: The Protections for Policing.” *Geo. Wash. L. Rev.* 84 (2016): 281–353.
Garrett, Brandon L. “Constitutional Reasonableness.” *Minn. L. Rev.* 102 (2017–2018): 61–126.
Gentithes, Michael. “The End of Miller’s Time: How Sensitivity Can Categorize Third-Party Data After Carpenter.” *Ga. L. Rev.*, 2019. https://papers.ssrn.com/abstract=3155644.

Geverd, Timothy J. “Bulk Telephony Metadata Collection and the Fourth Amendment: The Case for Revisiting the Third-Party Disclosure Doctrine in the Digital Age.” *J. Marshall J. Info. Tech. & Privacy L.* 31 (2014–2015): 191–237.
Ghoshray, Saby. “Privacy Distortion Rationale for Reinterpreting the Third-Party Doctrine of the Fourth Amendment.” *Fla. Coastal L. Rev.* 13, no. 1 (2011): 33–84.
Gizzi, Michael C., and R. Craig Curtis. *The Fourth Amendment in Flux: The Roberts Court, Crime Control, and Digital Privacy*. Lawrence, Kansas: University Press of Kansas. 2016.
Gray, David. *The Fourth Amendment in an Age of Surveillance*. Cambridge, United Kingdom; New York, NY: Cambridge University Press. 2017.
Gray, David, and Danielle Keats Citron. “A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy.” *N.C. J.L. & Tech.* 14 (2012–2013): 381–430.
Gruber, Aya. “Garbage Pails and Puppy Dog Tails: Is That What Katz Is Made Of?” *U.C. Davis L. Rev.* 41, no. 3 (2008): 781–838.
Guzik, JoAnn. “Assumption of Risk Doctrine: Erosion of Fourth Amendment Protection through Fictitious Consent to Search and Seizure, The Fourth Amendment Symposium.” *Santa Clara L. Rev.* 22 (1982): 1051–86.
Harper, Jim. “Reforming Fourth Amendment Privacy Doctrine Left out in the Cold - The Chilling of Speech, Association, and the Press in Post-9/11 America September 20-21, 2007.” *Am. U. L. Rev.* 57 (2007–2008): 1381–1404.
Harris, David A. “Riley v. California and the Beginning of the End for the Third-Party Search Doctrine.” *U. Pa. J. Const. L.* 18, no. 3 (2016): 895–932.
Haynes, Derek. “Search Protocols: Establishing the Protections Mandated by the Fourth Amendment against Unreasonable Searches and Seizures in the World of Electronic Evidence Comment.” *McGeorge L. Rev.* 40 (2009): 757–76.
Heffernan, William C. “Fourth Amendment Privacy Interests Criminal Law.” *J. Crim. L. & Criminology* 92 (2001): 1–126.
Henderson, Stephen E. “After United States v. Jones, after the Fourth Amendment Third Party Doctrine.” *N.C. J.L. & Tech.* 14, no. 2 (2013): 431–60.
———. “Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too.” *Pepp. L. Rev.* 34, no. 4 (2007): 975–1026.
———. “Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search.” *Cath. U. L. Rev.* 55, no. 2 (2006): 373–438.
———. “Nothing New under the Sun - A Technologically Rational Doctrine of Fourth Amendment Search.” *Mercer L. Rev.* 56 (2004–2005): 507–64.
———. “The Timely Demise of the Fourth Amendment Third Party Doctrine Comment.” *Iowa L. Rev. Bull.* 96 (2010): 39–51.
Hodge, Matthew J. “The Fourth Amendment and Privacy Issues on the New Internet: Facebook.Com and Myspace.Com.” *S. Ill. U. L.J.* 31, no. 1 (2006): 95–122.
Holland, H. Brian. “A Cognitive Theory of the Third-Party Doctrine and Digital Papers.” *Temp. L. Rev.* 91 (2018): 55–106.
Hu, Margaret. “Orwell’s 1984 and a Fourth Amendment Cybersurveillance Nonintrusion Test.” *Wash. L. Rev.* 92 (2017): 1819–1904.

Julie, Richard S. “High-Tech Surveillance Tools and the Fourth Amendment: Reasonable Expectations of Privacy in the Technological Age.” *Am. Crim. L. Rev.* 37, no. 1 (2000): 127–44.
Kahn-Fogel, Nicholas A. “The Benefits of Using Investigative Legislation to Interpret the Fourth Amendment: A Response to Orin Kerr.” *Ala. C.R. & C.L. L. Rev.* 9 (2018): 379–406.
Kamin, Sam. “The Private Is Public: The Relevance of Private Actors in Defining the Fourth Amendment.” *B.C. L. Rev.* 46 (2004–2005): 83–148.
Kattan, Ilana R. “Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud Note.” *Vand. J. Ent. & Tech. L.* 13 (2010–2011): 617–56.
Katz, Lewis R. “In Search of a Fourth Amendment for the Twenty-First Century.” *Ind. L.J.* 65 (1989–1990): 549–90.
Kerr, Orin S. “A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & (and) the USA Patriot Act: Surveillance Law: Reshaping the Framework.” *Geo. Wash. L. Rev.* 72 (2003–2004): 1208–43.
———. “An Equilibrium-Adjustment Theory of the Fourth Amendment.” *Harv. L. Rev.* 125, no. 2 (2011): 476–543.
———. “Applying the Fourth Amendment to the Internet: A General Approach.” *Stan. L. Rev.* 62, no. 4 (2010): 1005–50.
———. “Congress, the Courts, and New Technologies: A Response to Professor Solove Symposium.” *Fordham L. Rev.* 74, no. 2 (2005): 779–90.
———. “Defending the Third-Party Doctrine: A Response to Epstein and Murphy Symposium: Security Breach Notification Six Years Later.” *Berkeley Tech. L.J.* 24 (2009): 1229–38.
———. “Do We Need a New Fourth Amendment?” *Michigan Law Review* 107, no. 6 (April 2009): 951–66.
———. “Four Models of Fourth Amendment Protection.” *Stan. L. Rev.* 60, no. 2 (2007): 503–52.
———. “Implementing Carpenter.” In *The Digital Fourth Amendment (Forthcoming)*. Rochester, NY: Social Science Research Network. 2018.
———. “Initial Reactions to Carpenter v. United States,” USC Law Legal Studies Paper No. 18-14, July 6, 2018. https://papers.ssrn.com/abstract=3209587.
———. “Internet Surveillance Law after the USA Patriot Act: The Big Brother That Isn’t.” *Nw. U. L. Rev.* 97 (2002–2003): 607–74.
———. “‘Katz’ Has Only One Step: The Irrelevance of Subjective Expectations.” *U. Chi. L. Rev.* 82, no. 1 (2015): 113–34.
———. “Lifting the Fog of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law Symposium: Enforcing Privacy Rights.” *Hastings L.J.* 54 (2002–2003): 805–46.
———. “The Case for the Third-Party Doctrine.” *Mich. L. Rev.* 107, no. 4 (2009): 561–602.
———. “The Curious History of Fourth Amendment Searches.” *Sup. Ct. Rev* 2012, no. 1 (2013): 67–97.
———. “The Effect of Legislation on Fourth Amendment Protection.” *Mich. L. Rev.* 115 (2016–2017): 1117–66.
———. “The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution.” *Mich. L. Rev.* 102, no. 5 (2004): 801–88.

———. “The Mosaic Theory of the Fourth Amendment.” *Mich. L. Rev.* 111, no. 3 (2012): 311–54.
Kozinski, Alex, and Eric S. Nguyen. “Has Technology Killed the Fourth Amendment.” *Cato Sup. Ct. Rev.* 2011–2012 (2011–2012): 15–30.
Ku, Raymond Shih Ray. “The Founders’ Privacy: The Fourth Amendment and the Power of Technological Surveillance Symposium: Modern Studies in Privacy Law.” *Minn. L. Rev.* 86, no. 6 (2002): 1325–78.
Kugler, Matthew B., and Lior Jacob Strahilevitz. “Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory.” *The Supreme Court Review* 2015, no. 1 (January 1, 2016): 205–63.
Lawless, Matthew D. “Third Party Doctrine Redux: Internet Search Records and the Case for a ‘Crazy Quilt’ of Fourth Amendment Protection.” *UCLA J.L. & Tech.* Spring 2007 (May 7, 2007).
Levy, Leonard W. *Origins of the Bill of Rights*. New Haven: Yale University Press. 1999.
Lin, Wei Chen. “Where Are Your Papers: The Fourth Amendmnet, the Stored Comunications Act, the Third Party Doctrine, the Cloud and Encryption Comments.” *DePaul L. Rev.* 65 (2015–2016): 1093–1138.
Lipman, Rebecca. “The Third Party Exception: Reshaping an Imperfect Doctrine for the Digital Age Student Note.” *Harv. L. & Pol’y Rev.* 8 (2014): 471–90.
Litt, Robert S. “The Fourth Amendment in the Information Age.” *Yale L.J. F.* 126 (2016–2017): 8–20.
Loewy, Arnold H. “The Fourth Amendment as a Device for Protecting the Innocent.” *Michigan Law Review* 81, no. 5 (1983): 1229–72.
Lofgren, Zoe. “Do Modern Americans Have Fourth Amendment Protection.” *Santa Clara L. Rev.* 54 (2014): 901–30.
Logan, Wayne A. “Fourth Amendment Localism.” *Ind. L.J.* 93 (2018): 369–420.
Maccarone, Sheryl. “Moving Past the General Public Use Standard: Addressing Fourth Amendment Policy Concerns Amidst the Development of New Surveillance Technology Notes & Comments.” *Sw. L. Rev.* 45 (2015–2016): 199–218.
Mannheimer, Michael J. Zydney. “The Contingent Fourth Amendment.” *Emory L.J.* 64 (2014–2015): 1229–92.
McAllister, Marc. “The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning.” *S. Ill. U. L.J.* 36 (2011–2012): 475–530.
Michael, M. Blane. “Reading the Fourth Amendment: Guidance from the Mischief That Gave It Birth Madison Lecture.” *N.Y.U. L. Rev.* 85 (2010): 905–31.
Murphy, Erin. “The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr.” *Berkeley Tech. L.J.* 24, no. 3 (2009): 1239–53.
———. “The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions.” *Mich. L. Rev.* 111 (2012–2013): 485–546.
Ohm, Paul. “The Many Revolutions of Carpenter.” *Harv. J. L. & Tech.* 32, no. (forthcoming) (2019). https://doi.org/10.31228/osf.io/bsedj.
O’Leary, Kaitlyn R. “What the Founders Did Not See Coming: The Fourth Amendment, Digital Evidence, and the Plain View Doctrine Note.” *Suffolk U. L. Rev.* 46, no. 1 (2013): 211–42.

Ormerod, Peter C., and Lawrence J. Trautman. "A Descriptive Analysis of the Fourth Amendment and the Third-Party Doctrine in the Digital Age." *Alb. L.J. Sci. & Tech.* 28, no. 2 (2018): 73–149.
Park, Eunice. "Objects, Places and Cyber-Spaces Post-Carpenter: Extending The Third-Party Doctrine Beyond CSLI: A Consideration of IoT and DNA." *Yale J.L. & Tech* 21, no. 1 (2019).
Pesciotta, Daniel T. "I'm Not Dead Yet: Katz, Jones, and the Fourth Amendment in the 21st Century Note." *Case W. Res. L. Rev.* 63 (2012–2013): 187–256.
Pew Research Center. "Demographics of Mobile Device Ownership and Adoption in the United States," February 5, 2018. http://www.pewinternet.org/fact-sheet/mobile/.
Plourde-Cole, Haley. "Back to Katz: Reasonable Expectation of Privacy in the Facebook Age Note." *Fordham Urb. L.J.* 38 (2010–2011): 571–628.
Press, Associated. "Google Records Your Location Even When You Tell It Not To." *The Guardian*, August 0, 2018, sec. Technology. https://www.theguardian.com/technology/2018/aug/13/google-location-tracking-android-iphone-mobile.
Price, Michael W. "Rethinking Privacy: Fourth Amendment Papers and the Third-Party Doctrine." *J. Nat'l Sec. L. & Pol'y* 8, no. 2 (2016): 247–300.
Raviv, Emma. "Homing in: Technology's Place in Fourth Amendment Jurisprudence." *Harv. J. L. & Tech.* 28, no. 2 (2015): 593–618.
Reidenberg, Joel R. "Privacy in Public." *U. Miami L. Rev.* 69 (2014–2015): 141–60.
Richards, Neil. "The Third Party Doctrine and the Future of the Cloud Washington University Law Professor Spotlight." *Wash. U. L. Rev.* 94 (2016–2017): 1441–92.
Robison, William Jeremy. "Free at What Cost: Cloud Computing Privacy under the Stored Communications Act Note." *Geo. L.J.* 98 (2009–2010): 1195–1240.
Rosenthal, Lawrence. "Binary Searches and the Central Meaning of the Fourth Amendment." *Wm. & Mary Bill Rts. J.* 22 (2014): 881–940.
Rozenshtein, Alan Z. "Surveillance Intermediaries." *Stan. L. Rev.* 70 (2018): 99–190.
Rubenfeld, Jed. "The End of Privacy." *Stan. L. Rev.* 61, no. 1 (2008): 101–62.
Schlabach, Gabriel R. "Privacy in the Cloud: The Mosaic Theory and the Stored Communications Act Note." *Stan. L. Rev.* 67 (2015): 677–722.
Scolnik, Alexander. "Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment Note." *Fordham L. Rev.* 78 (2009–2010): 349–98.
Seamon, Richard H. "Kyllo v. United States and the Partial Ascendance of Justice Scalia's Fourth Amendment." *Wash. U. L. Q.* 79 (2001): 1013–34.
Serafino, Laurie Buchan. "I Know My Rights, So You Go'n Need a Warrant for That: The Fourth Amendment, Riley's Impact, and Warrantless Searches of Third-Party Clouds." *Berkeley J. Crim. L.* 19 (2014): 154–205.
Short, Reginald. "The Kyllo Conundrum: A New Standard to Address Technology That Represents a Step Backward for Fourth Amendment Protections Comment." *Denv. U. L. Rev.* 80 (2002–2003): 463–86.
Sklansky, David A. "Back to the Future: Kyllo, Katz, and Common Law." *Miss. L.J.* 72, no. 1 (2002): 143–212.
———. "The Fourth Amendment and Common Law." *Colum. L. Rev.* 100, no. 7 (2000): 1739–1814.

Sklansky, David Alan. “Too Much Information: How Not to Think about Privacy and the Fourth Amendment.” *Calif. L. Rev.* 102 (2014): 1069–1122.
———. “Two More Ways Not to Think about Privacy and the Fourth Amendment.” *The University of Chicago Law Review* 82, no. 1 (2015): 223–42.
Slobogin, Christopher. “Is the Fourth Amendment Relevant in a Technological Age?,” Vanderbilt Public Law Research Paper No. 10-64, 2011. https://ssrn.com/abstract=1734755.
———. *Privacy at Risk the New Government Surveillance and the Fourth Amendment*. Chicago: University of Chicago Press. 2007.
———. “Subpoenas and Privacy Symposium - Privacy and Identity: Constructing, Maintaining, and Protecting Personhood.” *DePaul L. Rev.* 54 (2004–2005): 805–46.
———. “Transaction Surveillance by the Government Symposium: The Search and Seizure of Computers and Electronic Evidence.” *Miss. L.J.* 75 (2005–2006): 139–92.
Slobogin, Christopher, and Joseph E. Schumacher. “Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at Understandings Recognized and Permitted by Society.” *Duke L.J.* 42 (1992–1993): 727–75.
Small, Jacob M. “Storing Documents in the Cloud: Toward an Evidentiary Privilege Protecting Papers and Effects Stored on the Internet.” *Geo. Mason U. C.R. L.J.* 23 (2012–2013): 255–82.
Solove, Daniel J. “A Taxonomy of Privacy.” *U. Pa. L. Rev.* 154, no. 3 (2005): 477–564.
———. “Digital Dossiers and the Dissipation of Fourth Amendment Privacy.” *S. Cal. L. Rev.* 75 (2002): 1083–1168.
———. “Fourth Amendment Codification and Professor Kerr’s Misguided Call for Judicial Deference.” *Fordham L. Rev.* 74, no. 2 (2005): 747–78.
———. “Fourth Amendment Pragmatism.” *B.C. L. Rev.* 51, no. 5 (2010): 1511–38.
———. *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press. 2004.
Steinberg, David E. “Sense-Enhanced Searches and the Irrelevance of the Fourth Amendment.” *Wm. & Mary Bill Rts. J.* 16 (2007–2008): 465–96.
Stover, Andrew J. “Privacy vs. Protection: Why Tracking Mobile-Device Location Data without a Warrant Requires a Fourth Amendment Exception.” *Cath. U. J. L. & Tech* 26 (2017–2018): 1–51.
Stubbs, Blake. “Technological Ubiquity and the Evolution of Fourth Amendment Rights.” *Drake L. Rev.* 62 (2014): 575–98.
Stuntz, William J. “The Substantive Origins of Criminal Procedure.” *Yale L.J* 105, no. 2 (1995): 393–447.
Swire, Peter P. “Katz Is Dead, Long Live Katz.” *Mich. L. Rev.*, o, 102, no. 5 (2004): 904–32.
Thai, Joseph T. “Is Data Mining Ever a Search under Justice Stevens’s Fourth Amendment Symposium: The Jurisprudence of Justice Stevens: Panel I: Criminal Justice.” *Fordham L. Rev.* 74 (2005–2006): 1731–58.
Tokson, Matthew. “Automation and the Fourth Amendment.” *Iowa L. Rev.* 96 (2010–2011): 581–648.
———. “Blank Slates.” *B.C. L. Rev.* 59 (2018): 591–654.
———. “Knowledge and Fourth Amendment Privacy.” *Nw. U. L. Rev.* 111 (2016–2017): 139–204.

Tokson, Matthew J. “The Content/Envelope Distinction in Internet Law.” *Wm. & Mary L. Rev.* 50, no. 6 (2008): 2105–76.

Tomkovicz, James J. “Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures.” *Miss. L.J.* 72 (2002–2003): 317–446.

Valentino-DeVries, Jennifer, Natasha Singer, Michael H. Keller, and Aaron Krolik. “Your Apps Know Where You Were Last Night, and They’re Not Keeping It Secret.” *The New York Times*, December 10, 2018, sec. Business. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

Walsh, Courtney E. “Surveillance Technology and the Loss of Something a Lot Like Privacy: An Examination of the Mosaic Theory and the Limits of the Fourth Amendment Criminal Law Issue: Features Contributors.” *St. Thomas L. Rev.* 24 (2011–2012): 169–247.

Warren, Samuel D., and Louis D. Brandeis. “The Right to Privacy.” *Harv. L. Rev.* 4, no. 5 (1890): 193–220.

Weaver, Russell L. “The Fourth Amendment, Privacy and Advancing Technology The James Otis Lectures: Lecture.” *Miss. L.J.* 80 (2010–2011): 1131–1228.

Wells, R. Bruce. “The Fog of Cloud Computing: Fourth Amendment Issues Raised by the Blurring of Online and Offline Content Comment.” *U. Pa. J. Const. L.* 12 (2009–2010): 223–40.

———. “The Fog of Cloud Computing: Fourth Amendment Issues Raised by the Blurring of Online and Offline Content Comment.” *U. Pa. J. Const. L.* 12 (2009–2010): 223–40.

William Mack, Donald J. Kiser, and Francis J. Ludes. “Searches and Seizures.” In *C.J.S*, Vol. 79, n.d.

Winn, Peter. “Katz and the Origins of the Reasonable Expectation of Privacy Test.” *McGeorge L. Rev.* 40 (2009): 1–12.

Young, Mark G. “What Big Eyes and Ears You Have: A New Regime for Covert Governmental Sureveillance Note.” *Fordham L. Rev.* 70 (2001–2002): 1017–1110.

Zimmer, Samantha G. “Cell Phone or Government Tracking Device: Protecting Cell Site Location Information with Probable Cause.” *Duq. L. Rev.* 56, no. 1 (2018): 107–40.

Unsigned Note: The Right to Privacy in Nineteenth Century America Notes.” *Harv. L. Rev.* 94, no. 8 (1981): 1892–1910.