ARTICLES

Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine

Michael W. Price*

INTRODUCTION

Most Americans now live in a world where nearly every call or click online leaves a digital trail that can be stored, searched, and stitched together to reveal an intimate portrait of private life. But current law affords little privacy protection to information about these activities, undermining First and Fourth Amendment safeguards that are essential to individual freedoms and a robust democracy. The so-called third-party doctrine[1] has created a privacy gap by denying Fourth Amendment protection to expressive and associational data processed by third parties, including communications information and data stored in the "cloud." Exacerbated by rapid advances in information technology and a proliferation of third-party records, the gulf continues to widen.

Congress has not stepped in to fill the void. The laws that govern online privacy are older than the World Wide Web.[2] It is a frequent and wholly justified criticism of the American legal system that a great number of the people in charge of making the rules for modern information technology have little or no experience using email, sending a text, or reading a blog.[3] And federal courts have been reluctant to delve into the business of regulating electronic surveillance,[4] with the exception of two recent Supreme Court decisions that hint at a new way forward.[5]

---

* Counsel, Liberty & National Security Program, Brennan Center for Justice at NYU School of Law.

1. *See* United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979).

2. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.) (2013); Robert Cailliau, *A Little History of the World Wide Web*, WC3 (1995), http://www.w3.org/History.html (first web browser used in December of 1990).

3. P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 31–32, 39–40 (2014); *Your Own Personal Internet*, WIRED (June 30, 2006), http://www.wired.com/2006/06/your_own_person/ (according to the late Senator Ted Stevens, the Internet is "a series of tubes"); Will Oremus, *Elena Kagan Admits Supreme Court Justices Haven't Quite Figured Out Email Yet*, SLATE (Aug. 20, 2013), http://www.slate.com/blogs/future_tense/2013/08/20/elena_kagan_supreme_court_justices_haven_t_gotten_to_email_use_paper_memos.html (Supreme Court Justices exchange messages via paper memo; Court "hasn't really 'gotten to' email."); *The Luddite atop U.S. Cybersecurity*, CNN (Sept. 28, 2012), http://security.blogs.cnn.com/2012/09/28/the-luddite-atop-us-cybersecurity/ (Department of Homeland Security Secretary Janet Napolitano acknowledged she does not use email "at all").

4. Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶¶ 1–3 (2007).

5. *See* Riley v. California, 134 S. Ct. 2473 (2014); United States v. Jones, 132 S. Ct. 945 (2012).

The Executive Branch, for its part, has taken advantage of the legal turmoil.[6] As we now know, in the aftermath of 9/11, the National Security Agency began collecting phone records and online metadata in bulk,[7] relying in large part on *Smith v. Maryland* – a 1979 Supreme Court case that involved one crime and one suspect's phone records.[8] And while there is a bipartisan push in Congress to update the decades-old law that gives electronic communications a patchwork of inconsistent and illogical protections, it remains to be seen whether the reform package will become law.

There is a strong temptation to blame the current privacy gap on a divide between so-called digital natives and digital immigrants – those who grew up using computers and the Internet, and those who did not.[9] Of course, it is the older generation, the digital immigrants, who make the rules (at least for the moment). Perhaps a new crop of tech-savvy judges and politicians will set things straight? This presumes a great deal about yet-to-be-invented technologies and how different people will use them. And it also assumes that there will be no generational divide in the future.

The problem with privacy today is doctrinal, not generational. If the Supreme Court intends to afford greater privacy protection to personal data stored electronically, as it seems inclined to do,[10] then it may want to consider a new analytical framework for the job. Existing Fourth Amendment tests are not fit for the digital long haul.

This article posits a supplemental approach to data privacy, one grounded in the history and text of the Fourth Amendment and easily applicable by all jurists – even those who lack a degree in information technology. The framework is compatible with existing Fourth Amendment tests; there is no need to displace them entirely. But the proliferation of highly personal third-party data

---

6. *See, e.g.*, *In re* Prod. of Tangible Things from [redacted], No. BR 08-13, at 4–18 (FISA Ct. Mar. 2, 2013) (Walton, J.), *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf (discussing "systemic problems" with the NSA's metadata collection and retention policies); [redacted], No. PR/TT [redacted], at 3–4 (FISA Ct. [redacted]) (Bates, J.) *available at* http://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf (stating the NSA "exceeded the scope of authorized acquisition continuously" during the term of the metadata collection orders and noting the government's "frequent failures to comply with [the authorizations'] terms"). *See generally* [redacted], No. PR/TT [redacted] (FISA Ct. [redacted]) (Kollar-Kotelly, J.), *available at* http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf (explaining legal rationale for initial bulk collection of telephonic metadata).

7. *See, e.g.*, Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/16program.html.

8. *See* Smith v. Maryland, 442 U.S. 735, 737 (1979) (discussing pen register that was installed only to record phone numbers dialed from the suspect's home phone).

9. SINGER & FRIEDMAN, *supra* note 3, at 4.

10. Michael Price & Amos Toh, *The Supreme Court's Wisdom on Metadata*, AL JAZEERA (June 28, 2014), http://america.aljazeera.com/opinions/2014/6/supreme-court-cellphonessearchwarrantriley california.html.

demands an avenue for Fourth Amendment analysis that is cognizant of its role in society.[11]

Section I is a brief history of the Fourth Amendment, focusing on its ties to First Amendment values in the development of search and seizure law. It tells the story of the Court's doctrinal evolution from a focus on property rights and trespass law to the "reasonable expectation of privacy" test developed in *Katz v. United States*. The trespass approach is well established and well suited to determining whether the search of a home is constitutional. Similarly, the *Katz* test may be most appropriate when the issue involves searches of the person[12] or even access to medical records.[13] But neither of these approaches provides an adequate Fourth Amendment framework for assessing the privacy interest in expressive and associational data held by third parties. A third way may be necessary in order to account for twenty-first-century "papers."

Section II dissects the third-party doctrine, a prime example of how the *Katz* test led the Court astray on information privacy. I deconstruct the origins of the doctrine and discuss its modern consequences, which have been devastating for digital privacy due to rapid changes in technology and the proliferation of third-party records. The doctrine was a misstep nearly forty years ago, but its full effect has now come into sharp relief and necessitates a course correction.

Section III proposes a new, supplemental Fourth Amendment analysis centered on the privacy of one's "papers," which enjoy equal billing with "persons," "houses," and "effects" in text, if not in practice.[14] The Supreme Court has not been eager to articulate how the Fourth Amendment should apply to "papers" independent of their physical location in a "constitutionally protected area"[15] like a home or office. But in light of the history and purpose of the Fourth Amendment, it is fair to say that "papers" should be read to protect expressive and associational data, regardless of its form, how it is created, or where it is located. Fourth Amendment "papers" may be pamphlets and letters in hard copy, or they may be digital files stored on a cell phone, hosted in "the cloud," or even generated by a third party.

Of course, not all third-party records have significant expressive or associational value. An online search for political or religious commentary may be followed by one with no clear First Amendment value whatsoever. Embarrassing, perhaps. But is it really the kind of speech the Framers fought a revolution to protect? The truth is that no one can begin to tell before looking, and that is

---

11. *See* Michael Price, *I'm Terrified of My New TV: Why I'm Scared to Turn This Thing On – And You'd Be, Too*, SALON (Oct. 30, 2014), http://www.salon.com/2014/10/30/im_terrified_of_my_new_tv_why_im_scared_to_turn_this_thing_on_and_youd_be_too/.

12. *See, e.g.*, Terry v. Ohio, 392 U.S. 1 (1968).

13. *See, e.g.*, Or. Prescription Drug Monitoring Program v. U.S. Drug Enforcement Admin., No. 3:12-cv-02023-HA, 2014 WL 562938, at *6 (D. Or. Feb. 11, 2014).

14. U.S. CONST. amend. IV.

15. *See* Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013); United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J. concurring); Silverman v. United States, 365 U.S. 505, 512 (1961).

precisely the problem. Consequently, the constitutional default for searching or seizing such categories of data must be Fourth Amendment protection, that is, a warrant based on probable cause.

Section IV returns to the third-party doctrine and analyzes two common categories of third-party data using the test proposed in Section III. I articulate how the theory would apply to data stored in the cloud and to communications data, while seeking to avoid the pitfalls of existing approaches. I conclude that both types of data, as well as their associated metadata, should be protected under the Fourth Amendment and that law enforcement should be required to get a warrant before searching or seizing them.

Finally, I discuss the potential limits of this approach. Certain types of third-party records that we intuitively believe to be private, such as medical and financial records, do not always have obvious First Amendment value. At the same time, it is not difficult to imagine scenarios where there is in fact a First Amendment component. Thus, we must acknowledge their First Amendment potential and recognize that the inability to pre-determine content means that the default should be set to privacy.

I. A BRIEF HISTORY OF FOURTH AMENDMENT SEARCH & SEIZURE LAW

The Fourth Amendment is not long or particularly convoluted. It contains a mere fifty-four words and its scope boils down to just four nouns: "persons, houses, papers, and effects."[16] How broadly or narrowly one interprets these four categories has a tremendous impact on privacy rights and is the subject of nearly constant constitutional debate. The history and purpose of the Fourth Amendment, however, have long been a lodestar to help interpret and define its boundaries. And one of the most essential aspects of that history and purpose is the strong connection between the First and Fourth Amendments.

A. Freedom of Speech and the Fourth Amendment

The history of the Fourth Amendment 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. The Fourth Amendment was born out of colonial revulsion toward "writs of assistance" and "general warrants" used by agents of the British Empire. While the infamous writs of assistance helped enforce tax laws in the colonies, general warrants were systematically used to enforce libel laws and suppress dissent in England.[17] The Framers found common cause with popular English dissidents, notably John Wilkes, united in their opposition to arbitrary and invasive searches and seizures. The English experience helped sow the seeds of colonial resis-

16. U.S. CONST. amend. IV.

17. Stanford v. Texas, 379 U.S. 476, 482 (1965) (noting that general warrants were "systematically used" in "enforcing the laws licensing the publication of literature and, later, in prosecutions for seditious libel").

tance and was one of the driving forces behind the Fourth Amendment.

There is a long history in England of suppressing dissent through the use of broad powers to search and seize "unlicensed" or otherwise offending works. Shortly after the first printing press arrived at Westminster in 1476, the Crown established a primitive scheme of licensing, copyright, and censorship for printed material.[18] The king would grant licenses to favored printers and prosecute the others for publishing unsanctioned works; ecclesiastics were in charge of censorship. The law functioned as both a sword and shield. It allowed the Crown to promote press that served its interests while suppressing unwanted speech.[19]

Beginning with the Tudors and continuing into the Stuart era, the power to police printing fell to the Stationers' Company and the Star Chamber. The Stationers' Company was a consortium of printers permitted to incorporate and maintain a monopoly on printing in exchange for suppressing undesirable material.[20] The company and its agents had unbridled power to search for and seize "unlicensed" tracts, authorized "to open all packs and trunks of papers and books brought into the country, to search in any warehouse, shop, or any other place where they suspected a violation of the laws of printing to be taking place [and] to seize the books printed contrary to law."[21] The notorious Star Chamber developed a reputation as a political instrument to prosecute dissent,[22] having created the crime of libel for printing objectionable words.[23] Criticism of the Crown was considered "seditious libel." King Charles I used the chamber to prosecute the Puritans,[24] who fled to the American colonies.

---

18. *See generally*, FREDRICK S. SIEBERT, FREEDOM OF THE PRESS IN ENGLAND, 1476–1776: THE RISE AND DECLINE OF GOVERNMENT CONTROL 21–63 (1965).

19. *Id.* at 64 ("It is almost impossible to disentangle the efforts of the printers to maintain their 'copy-rights' from the complacent cooperation in suppressing 'unlawful' printing.").

20. *Id.* at 66.

21. NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 24 (1937); *see also* Marcus v. Search Warrant of Prop. at 104 E. Tenth St., Kansas City, Mo., 367 U.S. 717, 724–25 (1961) ("The Stationers' Company was incorporated in 1557 to help implement that system and was empowered 'to make search whenever it shall please them in any place, shop, house, chamber, or building or any printer, binder or bookseller whatever within our kingdom of England or the dominions of the same of or for any books or things printed, or to be printed, and to seize, take hold, burn, or turn to the proper use of the foresaid community, all and several those books and things which are or shall be printed contrary to the form of any statute, act, or proclamation, made or to be made . . . ").

22. SIEBERT, *supra* note 18, at 31.

23. At the time, libel included speech that defamed public officials, dishonored the monarchy, or smeared private individuals' reputations. *See* John M. Kang, *In Praise of Hostility: Anti-Authoritarianism as Free Speech Principle*, 35 HARV. J.L. & PUB. POL'Y 351, 371 (2012). Truth was not considered a defense; it was an aggravating factor. *See* DAVID A. COPELAND, THE IDEA OF A FREE PRESS: THE ENLIGHTENMENT AND ITS UNRULY LEGACY 38 (2006).

24. The case of William Prynne, a prominent Puritan, is among the better-known instances of excessive punishment for seditious libel. Prynne was convicted twice of publishing libelous works against the state and the king. As a part of his punishment, his ears were cut off in the pillories at Westminster and Cheapside and his forehead was branded with an S.L., for "Seditious Libeller." *See generally*, Edward P. Cheyney, *The Court of Star Chamber*, 18 AM. HIST. REV., 727, 747–748 (1913).

Parliament eventually abolished the Star Chamber and the Stationers' Company, but the prohibition against seditious libel remained alive and well in English common law, as did the practice of issuing "general warrants" to search and seize papers.[25] This was the scene in 1763 when Lord Halifax, the British Secretary of State, issued a general warrant that ordered the king's messengers to "apprehend and seize the printers and publishers" of an anonymous satirical pamphlet, the *North Briton* No. 45, which was critical of King George III.[26] The warrant was "general" because it did not specify the places to be searched, the papers to be seized, or the persons to be arrested. Forty-nine people were arrested in three days, some dragged from their beds.[27]

One of those forty-nine people was John Wilkes, a member of Parliament – and, as it turned out, the author of the pamphlet. In searching for evidence that Wilkes was the author, the messengers "fetched a sack and filled it" with Wilkes's private papers.[28] While the search was nominally justified by charges of sedition, it in fact swept much more broadly. Lord Halifax ordered that, "all must be taken, manuscripts and all."[29]

Wilkes, for his part, was not shy of controversy. Indeed, he made his political name as a provocateur, known for lampooning the King's ministers.[30] The *North Briton* was a thoroughly scandalous satire designed to mock a government-friendly newspaper, the *Briton*, a publication backed by Wilkes's perennial political rival, the Earl of Bute. The *North Briton* was also tremendously popular, with a weekly circulation of nearly ten times that of the *Briton.*[31] Issue No. 45, however, appeared to cross a line by criticizing the king directly instead of his ministers. Incensed, George III ordered Wilkes to be arrested and tried for seditious libel. But as a sitting member of Parliament, Wilkes was judged to be immune from prosecution.[32]

Never one to quit while ahead, Wilkes proceeded to sue the messengers for trespass and the seizure of his private papers. In fact, Wilkes had anticipated the case, writing a year prior that he would fight a general warrant and seek to

25. R. H. Clark, *Historical Antecedents of the Constitutional Right to Privacy*, 2 U. DAYTON L. REV. 157, 165–166 (1977).

26. Huckle v. Money, (1763) 95 Eng. Rep. 768 (K.B.); 2 Wils. K. B. 206. *See generally* STEPHEN J. SCHULHOFER, MORE ESSENTIAL THAN EVER: THE FOURTH AMENDMENT IN THE TWENTY-FIRST CENTURY 24–30 (2012) (describing the history of *The North Briton,* No. 45).

27. Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 1007 (2011); RAYMOND W. POSTGATE, THAT DEVIL WILKES 54 (1956).

28. Wilkes v. Wood, (1763) 98 Eng. Rep. 489 (C.P.) 490; Lofft 1, 5.

29. Entick v. Carrington, (1765) 19 How. St. Tr. 1029 (K.B.) 1065 ("[I]n the case of Wilkes against Wood, when the messengers hesitated about taking all the manuscripts, and sent to the secretary of state for more express orders for that purpose, the answer was, 'that all must be taken, manuscripts and all.' Accordingly, all was taken, and Mr. Wilkes's private pocketbook filled up the mouth of the sack.").

30. *See generally* POSTGATE, *supra* note 27.

31. Jack Lynch, *Wilkes, Liberty, and Number 45*, COLONIAL WILLIAMSBURG J., Summer 2003, *available at* http://www.history.org/foundation/journal/summer03/wilkes.cfm.

32. SIEBERT, *supra* note 18, at 359; POSTGATE, *supra* note 27, at 60.

prosecute Lord Halifax.[33] When the king's messengers arrived, he quarreled with them over the legality of the warrant, sent for his friends to bear witness, and made a public spectacle of his arrest. Refusing to walk from his house, Wilkes "insisted on a sedan-chair being brought; he entered it and was ceremoniously carried from one doorstep to the other."[34] He adored the spotlight and promised a packed courtroom that his case would be a test "to determine at once whether English liberty shall be a reality or a shadow."[35] When the criminal charges against him were dismissed, a "deafening yell of delight" erupted with the cry of "Wilkes and Liberty!"[36] – a slogan that would echo across the Atlantic.

In *Wilkes v. Wood*, his civil suit against the messengers, Wilkes condemned the use of general warrants as enabling the "promulgation of our most private concerns, affairs of the most secret personal nature," signifying "an outrage to the constitution itself."[37] He identified the search and seizure of his private papers as the most grievous offense against him and the "least capable of reparation," likening it to the Spanish Inquisition.[38] Wilkes maintained that, as a member of Parliament, more caution ought to have been used in seizing his papers, but he framed his case as one that "touched the liberty of every subject of this country."[39] He presented it as a "wound given to the constitution, and demanded damages accordingly," stressing that his "papers had undergone the inspection of very improper persons to examine his private concerns."[40] It took a jury just thirty minutes to find in his favor and award Wilkes the hefty sum of £1,000.[41]

Wilkes' success inspired others afflicted by general warrants to sue the messenger. Dryden Leach and William Huckle, also suspected of printing *North Briton* No. 45, recovered significant damages for the invasion of their homes and seizure of their papers.[42] Although their actual property damage was minimal, the awards reflected great concern for the harm to English liberty. In fact, the damages in these cases established the modern doctrine of "exemplary" or punitive damages.[43]

Entick v. Carrington was the second significant English case to challenge the use of general warrants. Similar to Wilkes, John Entick was suspected of authoring several editions of another "very seditious" weekly paper known as

33. POSTGATE, *supra* note 27, at 53.
34. *Id.* at 55.
35. *Id.* at 59.
36. *Id.* at 60.
37. Wilkes v. Wood, (1763) 98 Eng. Rep. 489 (C.P.) 490; Lofft 1, 3.
38. *Id.*
39. *Id.*
40. *Id.* at 498.
41. *Id.* at 499.
42. *See* Money v. Leach, (1765) 97 Eng. Rep. 1075 (K.B.) 1077; Huckle v. Money, (1763) 95 Eng. Rep. 768 (K.B.).
43. *See, e.g.*, Lake Shore & M.S. Ry. Co. v. Prentice, 147 U.S. 101, 106–107 (1893).

the *Monitor*.[44] True to form, Lord Halifax issued a warrant for the arrest of its authors and the seizure of their private papers. Unlike the Wilkes affair, however, it was widely known that Entick wrote for the *Monitor*.[45] As a result, the warrant identified Entick by name and was thus not a "true" general warrant.[46] Nonetheless, it was seen as even more egregious than the others, being "directly aimed at [a] political dissenter[] and political papers."[47] In the course of the search, the investigators "read over, pryed into, and examined all [of Entick's] private papers, books, etc.," a process compared to "racking his body to come at his secret thoughts."[48]

Like Wilkes, Entick brought a civil suit against the messengers for trespass and recovered £1,000 in damages.[49] The celebrated Lord Camden (who also presided over the *Wilkes* case) found that Entick's papers were "his dearest property" and "so far from enduring a seizure, that they will hardly bear an inspection."[50] "[W]here private papers are removed and carried away," Camden continued, "the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect."[51] Although *Wilkes* became known as "the Case of General Warrants," *Entick* was called "the case of Seizure of Papers,"[52] and it was one of the most influential cases shaping the Fourth Amendment. According to the Supreme Court, it was a "'monument of English freedom' 'undoubtedly familiar' to 'every American statesman' at the time the Constitution was adopted, and considered to be 'the true and ultimate expression of constitutional law.'"[53]

Indeed, it is an understatement to say that the *Entick* and *Wilkes* cases generated significant interest in the nascent American states.[54] By most ac-

---

44. Entick v. Carrington, (1765) 95 Eng. Rep. 807 (K.B.) 808; 2 Wils. 275, 276.

45. SIEBERT, *supra* note 18, at 377.

46. *Compare* James Otis, Address Before the Superior Court of Massachusetts (Feb. 24, 1761) (transcript available at http://www.constitution.org/bor/otis_against_writs.htm) (describing general warrants as those allowing officers to search "suspected houses" without listing which homes it applied to, while saying that special warrants described the specific locations that could be searched based on specific suspicion), *with* Minnesota v. Dickerson, 508 U.S. 366, 378 (1993) ("Where, as here, an officer who is executing a valid search for one item seizes a different item, this Court rightly has been sensitive to the danger . . . that officers will enlarge a specific authorization, furnished by a warrant or an exigency, into the equivalent of a general warrant to rummage and seize at will." (internal quotation marks and citations omitted)), *and* Berger v. New York, 388 U.S. 41, 58 (1967) (stating that the concern with general warrants is they allow "the seizure of one thing under a warrant describing another").

47. Akhil Reed Amar, *The Fourth Amendment, Boston, and the Writs of Assistance*, 30 SUFFOLK U. L. REV. 53, 78 (1996).

48. *Entick*, 95 Eng. Rep. at 812; 2 Wils. at 282.

49. POSTGATE, *supra* note 27, at 378.

50. Entick v. Carrington, (1765) 19 How. St. Tr. 1029 (K.B.) 1029.

51. *Id.*

52. Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. CRIM. L. & CRIMINOLOGY 49, 67 (2013).

53. Brower v. Cnty. of Inyo, 489 U.S. 593, 596 (1989) (quoting Boyd v. United States, 116 U.S. 616, 626 (1886)).

54. SCHULHOFER, *supra* note 26, at 27.

counts, they were the talk of every town in the colonies.[55] According to historian Jack Lynch:

> Colonial newspapers buzzed with information about the persecuted friend of liberty . . . . Wilkes-Barre, Pennsylvania, and Wilkesboro, North Carolina, took their names from the author of No. 45. Citizens of Virginia and Maryland resolved to send Wilkes forty-five hogsheads of tobacco, and forty-five women in Lexington, Massachusetts, joined to spin American linen to protest British policies. When news of Wilkes's release from prison reached Charleston, Club Forty-Five met at 7:45, drank forty-five toasts, and adjourned at 12:45. Sometimes the adulation was almost religious.[56]

At the time, American colonists were engaged in their own struggle against arbitrary searches and seizures.[57] British officials in pursuit of untaxed goods used writs of assistance to search homes and seize property with impunity. Somewhat surprisingly, prosecutions for seditious libel were rare. In 1735, the Crown prosecuted Peter Zenger, a New York newspaper printer, for libel. Despite overwhelming evidence against him, it took an American jury just ten minutes to acquit Zenger, after which the decision was widely praised in the press.[58] Zenger's attorney, Andrew Hamilton, won the case through jury nullification, humiliating the Crown.[59]

Although the American search and seizure experience revolved around smuggling rather than seditious libel,[60] popular aversion to arbitrary searches and seizures bridged the ocean. In Massachusetts, James Otis emerged as a champion against the writs of assistance, which he likened to the much-maligned general warrants in England.[61] Otis resigned his post as Massachusetts Attorney General in protest over the writs and then delivered a rousing oration against them on behalf of Boston merchants. Known as *Paxton's Case* or the "Writs of

---

55. *See, e.g.*, Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. Rev 112, 134 (2007); Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 563–565 (1999).

56. *See* Lynch, *supra* note, at 31.

57. *See* DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 147 (2011).

58. KENNETH SHEAR, UNORIGINAL MISUNDERSTANDING: PRESS FREEDOM IN EARLY AMERICA AND INTERPRETATION OF THE FIRST AMENDMENT 14 (2009) (citing N.Y. WKLY. J., Aug. 18, 1735, at 1).

59. *See* Phillip B. Scott, *Jury Nullification: An Historical Perspective on a Modern Debate*, 91 W. VA. L. REV. 389, 413–415 (1988).

60. Osmond K. Fraenkel, *Concerning Searches and Seizures*, 34 HARV. L. REV. 361, 362–366 (1921).

61. 2 JOHN ADAMS, *Notes of the Argument of Counsel in the Cause of Writs of Assistance, And of the Speech of James Otis, in* THE WORKS OF JOHN ADAMS, SECOND PRESIDENT OF THE UNITED STATES 521, 524 (Charles C. Little & James Brown, eds. 1850) ("Your Honors will find in the old books concerning the office of a justice of the peace precedents of general warrants to search suspected houses. But in more modern books you will find only special warrants to search such and such houses, specially named, in which the complainant has before sworn that he suspects his goods are concealed; and will find it adjudged that special warrants only are legal. In the same manner I rely on it, that the writ prayed for in this petition, being general, is illegal."); *see also* WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 380–94 (2009).

Assistance Case," Otis nearly succeeded in persuading the court of the writs' illegality, but the court reserved judgment until it could receive advice from England on how to proceed.[62] Not surprisingly, the Crown's ministers ordered the court to issue the writs.[63]

Otis' argument, however, proved to be the beginning of a revolution that would culminate with the Fourth Amendment. John Adams, then a young lawyer, was in the courtroom taking notes and pronounced it "the first scene of opposition" to the Crown. Adams later wrote that, "[t]hen and there the child Independence was born."[64] Otis articulated a legal framework for warrants that required specificity as to the persons, places, and things to be searched and seized.[65] Adams, the future president, borrowed this principle from Otis nineteen years later when he drafted Article Fourteen of the Massachusetts Declaration of Rights, the model for the Fourth Amendment.[66]

Adams was also well aware of the Wilkes affair and the potential for unchecked powers of search and seizure to stifle speech as well as commerce. He was a vocal critic of the Stamp Act of 1765, which imposed a tax on all printed materials, including legal documents, magazines, and newspapers, requiring them to carry an official stamp.[67] Adams publicly denounced the Stamp Act as designed to "strip us in a great measure of the means of knowledge, by loading the press, the colleges, and even an almanac and a newspaper, with restraints and duties," enforced through writs of assistance and courts of admiralty that operated without a jury.[68] The Act was reminiscent of the old English licensing schemes, and Adams publicly compared it to the Star Chamber.[69]

Colonialists roundly despised the Stamp Act. It hurt newspaper production, inspired one of the first attempts at libel prosecution since Peter Zenger,[70] and led to the formation of the Stamp Act Congress, the first coordinated political

---

62. Fraenkel, *supra* note 60, at 365.

63. *Id.*

64. Letter from John Adams to Judge Tudor (1818), *in* ANNALS OF THE AMERICAN REVOLUTION 223, 225 (Jedidiah Morse ed., 1824).

65. Thomas K. Clancy, *The Importance of James Otis*, 82 MISS. L. J. 487, 488 (2013); CUDDIHY, *supra* note 61, at 382.

66. THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION 39–40 (2008).

67. *See generally* Roger P. Mellen, *The Colonial Virginia Press and the Stamp Act*, 38 JOURNALISM HIST. 74, 75–76 (2012).

68. 3 JOHN ADAMS, *Dissertation on the Canon and the Feudal Law,* BOS. GAZETTE, Aug. 26, 1765, *reprinted in* THE WORKS OF JOHN ADAMS, SECOND PRESIDENT OF THE UNITED STATES 447, 464 (Charles C. Little & James Brown eds. 1851).

69. *Id.* at 470 ("[How could one be] against the Star-Chamber and High Commission, and yet remain an advocate for the newly-formed courts of admiralty in America?").

70. *See* SHEAR, *supra* note 58, at 33 (describing attempted libel prosecutions against Isaiah Thomas, a prominent Stamp Act opponent and editor of *The Massachusetts Spy*); David Copeland, *America: 1750–1820*, *in* PRESS, POLITICS AND THE PUBLIC SPHERE IN EUROPE AND NORTH AMERICA, 1760–1820 at 150 (Hannah Barker & Simon Burrows eds. 2002) ("[F]ew charges of seditious libel were brought against newspaper printers from 1735 – the year of the famous libel trial of New York printer John Peter Zenger – to the Revolution. As colonial legislatures gained more power, however, they did use libel laws in an attempt to control criticism in the volatile post–Stamp Act years of 1765–6.").

action against British rule.[71] Opposition to the Stamp Act also spawned the Sons of Liberty, whose mission was to incite resistance to the tax through protests, intimidation, and harassment of stamp agents.[72] The Sons of Liberty treated Wilkes like a folk hero and identified him with their cause.[73] Toasts to "Wilkes and Liberty" could be heard from one end of the colonies to the other.[74] John Adams wrote him fan mail.[75]

Against this backdrop, it is not surprising that Adams set out to craft a broad prohibition against unreasonable searches and seizures in Article 14 of the Massachusetts Declaration of Rights of 1780. Unlike the state constitutions of Virginia, Delaware, Maryland, and North Carolina, which abolished only general warrants,[76] Adams sought to regulate searches and seizures more generally. He used the Pennsylvania Constitution as a model, which specified that "the people have a right to hold themselves, their houses, papers, and possessions free from search and seizure."[77] Article 14 was the first to articulate a "right to be secure" from "unreasonable" searches and seizures,[78] and it too specified "papers" as a category worthy of special protection.[79] Adams' language is widely credited as the basis for the Fourth Amendment.[80]

By design, therefore, a paramount purpose of the Fourth Amendment was to serve as a guardian of individual liberty and free expression.[81] In other words, it

---

71. James Otis was nearly elected chair of the Stamp Act Congress. *See* CLINTON A. WESLAGER, THE STAMP ACT CONGRESS 59–66 (1976) (general overview of Otis's involvement in the Stamp Act Congress).

72. *See* 3 MURRAY N. ROTHBARD, CONCEIVED IN LIBERTY 140-42 (1975).

73. Clancy, *supra* note 27, at 1012; ARTHUR CASH, JOHN WILKES: THE SCANDALOUS FATHER OF CIVIL LIBERTY 232 (2008).

74. MERRILL JENSEN, THE FOUNDING OF A NATION: A HISTORY OF THE AMERICAN REVOLUTION, 1763–1776, at 317 (1968).

75. Committee of the Boston Sons of Liberty to John Wilkes, June 6, 1768, *in* PAPERS OF JOHN ADAMS 214–15 (1977).

76. *See* VA. CONST. of 1776 art. X; MD. CONST. of 1776 art. XXIII; DEL. CONST. of 1776 art. XVII; N.C. CONST. of 1776 art. XI.

77. PA. CONST. of 1776 art. X; *see also* VT. CONST. of 1777 art. XI.

78. CLANCY, *supra* note 66, at 40.

79. MASS. CONST. art. XIV.

80. CLANCY, *supra* note 66, at 39; LEONARD W. LEVY, ORIGINAL INTENT AND THE FRAMERS' CONSTITUTION 238–39 (2000); JACOB W. LANDYNSKI, SEARCH AND SEIZURE AND THE SUPREME COURT: A STUDY IN CONSTITUTIONAL INTERPRETATION 38 (1966) ("Next to the last and the most comprehensive, of the state declarations which antedated the Fourth Amendment was Article XIV of the Massachusetts Declaration of Rights adopted in 1780 . . . [H]ere is to be found for the first time in a constitution the phrase 'unreasonable searches' and this article apparently served as the model for the Fourth Amendment."); CUDDIHY, *supra* note 61, at 607–08; TELFORD TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 42 (1969) (crediting Article 14 of the Massachusetts Constitution of 1780 as the ancestor of the Fourth Amendment, noting that "the substance of the Massachusetts clause is identical").

81. Marcus v. Search Warrants of Prop. at 104 E. Tenth St., Kan. City, Mo., 367 U.S. 717, 729 (1961) ("This history was, of course, part of the intellectual matrix within which our own constitutional fabric was shaped. The Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression. For the serious hazard of suppression of innocent expression inhered in the discretion confided in the officers authorized to exercise the power.").

was intended to function as a barrier to government overreach and as a catalyst for other constitutional rights, notably freedom of speech and freedom of association, which are essential to a healthy democracy.[82]

In light of this history, the Supreme Court has recognized that First Amendment values are inextricably tied to powers of search and seizure.[83] However, the Court's *doctrinal* analysis of searches and seizures has centered on the need to protect property rights and, more recently, a person's privacy interests. The first approach focuses on property rights and trespass, articulating a vision of "constitutionally protected areas" that centers on the privacy of the home. The privacy-based analysis, on the other hand, turns on one's "reasonable expectation of privacy." As I will show, both approaches appear inadequate to protect information privacy in the digital age.

B. The Property-Based Approach

The sanctity of the home is the oldest and most well-established strain of search and seizure law. It was central to the *Wilkes* and *Entick* cases in England, and in *Paxton's Case*, James Otis argued for the maxim that "a man's house is his castle."[84] Indeed, for the first 175 years of Fourth Amendment history, the right against unreasonable searches and seizures was synonymous with the "right of a man to retreat into his own home and there be free from unreasonable government intrusion."[85]

The Supreme Court has reinforced this doctrine time and again, making it one of the rare well-defined rules of Fourth Amendment jurisprudence. The Court's insistence on drawing a "firm line at the entrance to the house" compels sharp distinctions between the privacy of the home and the ostensibly public nature of everything outside of it.[86] For example, the Court has ruled that the police must obtain a warrant to bring drug-sniffing dogs to someone's front porch, as they are effectively intruding into the area immediately surrounding the home, or its

82. ANDREW E. TASLITZ, RECONSTRUCTING THE FOURTH AMENDMENT: A HISTORY OF SEARCH AND SEIZURE, 1789–1868, at 58 (2006); *see also* David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J. L. & TECH. 381, 383 (2013) ("In keeping with our commitments to . . . liberty, we provide broad constitutional protections for freedom of speech, conscience, and religion.").

83. *Marcus*, 367 U.S. at 724. ("The use by government of the power of search and seizure as an adjunct to a system for the suppression of objectionable publications is not new. Historically 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."), *accord* United States v. U.S. Dist. Court, 407 U.S. 297, 313–14 (1972).

84. Otis, *supra* note 46 ("A man's house is his castle; and whilst he is quiet, he is as well guarded as a prince in his castle. This writ, if it should be declared legal, would totally annihilate this privilege. Custom-house officers may enter our houses when they please; we are commanded to permit their entry. Their menial servants may enter, may break locks, bars, and everything in their way; and whether they break through malice or revenge, no man, no court can inquire. Bare suspicion without oath is sufficient.").

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

86. Payton v. New York, 445 U.S. 573, 590 (1980).

"curtilage."[87] In contrast, the Court has permitted police to rummage through garbage left for collection *outside* the curtilage. According to the Court, residents give up privacy in their garbage when they place it on a sidewalk "readily accessible to animals, children, scavengers, snoops, and other members of the public."[88]

It may be helpful to think of the property-based approach as protecting "privacy in private."[89] It has dominated throughout most of American history because it was possible to draw a relatively neat distinction between public and private. Private things were kept locked inside; private conversations took place in person behind closed doors – at least for those who could afford locked doors and private spaces. Indeed, the search of one's home was seen as particularly offensive because it impinged on the things we hold most dear, especially our private papers.[90] But as technology began to render the castle walls of the home obsolete, the Court searched for another option.

C. From Places to Persons: What Is a Reasonable Expectation of Privacy?

The idea that there could be any "privacy in public" was foreign to the early judiciary. The first modern computer was not invented until 1936; the first successful satellite launch was not until 1957; and the first email was not sent until 1971.[91] At least for a time, the Supreme Court could afford to be technology-blind. But the invention of the telephone eventually proved to be a turning point. In 1928, the Court decided *Olmstead v. United States*, the first

87. Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013). On occasion, courts have held that even the curtilage is not automatically protected, instead conducting a fact-specific inquiry into the extent of a homeowner's attempts to protect his curtilage – an inquiry that would not seem to be supported by the Court's traditional approach. *See* United States v. Pineda-Moreno, 591 F.3d 1212, 1215 (9th Cir. 2010), *cert. granted, judgment vacated*, 132 S. Ct. 1533 (2012), *aff'd on reh'g*, 688 F.3d 1087 (9th Cir. 2012) (permitting attachment of GPS device to car in driveway because homeowner had not taken sufficient steps to protect curtilage).

88. California v. Greenwood, 486 U.S. 35, 40 (1988).

89. HELEN NISSENBAUM, PRIVACY IN CONTEXT 89–102 (2010); LAWRENCE LESSIG, CODE: VERSION 2.0, at 201 (2006), *available at* https://www.socialtext.net/codev2/Privacy ("The traditional question of 'privacy' was the limit the law placed upon the ability of others to penetrate your private space. What right does the government have to enter your home, or search your papers? What protection does the law of trespass provide against others beyond the government snooping into your private stuff? This is one meaning of Brandeis's slogan, 'the right to be left alone.' From the perspective of the law, it is the set of legal restrictions on the power of others to invade a protected space." (internal citation omitted)).

90. *See* Entick v. Carrington, (1765) 19 How. St. Tr. 1029 (K.B.) 1066 ("Papers are the owner's goods and chattels: they are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection"); *see also* CLANCY, *supra* note 66, at 48.

91. *See* RAYMOND WILLIAMS, TELEVISION: TECHNOLOGY & CULTURAL FORM, 9–11 (1990) (describing the development of television and moving video); Jack B. Copeland, *The Modern History of Computing*, STANFORD ENCYCLOPEDIA OF PHILOSOPHY (last modified June 9, 2006), http://plato.stanford.edu/archives/fall2008/entries/computing-history/ (describing Alan Turing's idea of a modern computing device, published in 1936); SPUTNIK AND THE DAWN OF THE SPACE AGE, http://history.nasa.gov/sputnik/, (last modified Oct. 10, 2007); Craig Partridge, *The Technical Development of Internet Email*, IEEE ANNALS HIST. COMPUTING, Apr.–June 2008, at 3, *available at* http://www.ir.bbn.com/craig/email.pdf.

high court case to address warrantless wiretapping.[92] From a property law perspective, the telephone was highly problematic because it blurred the line between public and private. It was suddenly possible to have a conversation without meeting in person or shouting from the rooftops, to speak in whispers with someone a town apart.

The Court grappled with how to handle the situation and fumbled its first attempt. Justice Taft denied in *Olmstead* that the Fourth Amendment could be "extended and expanded to include telephone wires reaching to the whole world."[93] Instead of looking at how the technology worked and the role it played in society, Taft fell back on property law, finding it dispositive that the "intervening wires are not part of his house or office any more than are the highways along which they are stretched."[94]

The Court doubled down on its restrictive approach to the Fourth Amendment in *Goldman v. United States*, holding that the police were free to listen in on a conversation in a private office by means of a "detectaphone" – a device that when held up to the outside wall of an office magnified the sounds inside.[95] The Court found that there was no "reasonable or logical distinction" between the wiretapping in *Olmstead* and the use of the detectaphone.[96] In both cases, as the Court in *Olmstead* had explained, evidence "was secured by the use of the sense of hearing and that only" – there was "no entry of the houses or offices of the defendants."[97]

Both decisions were products of the Court's failure to give weight to new technology and the way that it functions in society. The Court also failed to recognize the practical consequences of its decisions – namely, that its approach would result in the protection of far fewer communications than the Fourth Amendment originally covered, simply because of the technology involved.[98] In his dissent in *Goldman*, Justice Murphy warned that "science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears."[99] Even though modern surveillance methods did not entail a physical intrusion into a constitutionally protected area, "the privacy of the citizen is

92. Olmstead v. United States, 277 U.S. 438 (1928), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

93. *Id.* at 465.

94. *Id.*

95. Goldman v. United States, 316 U.S. 129, 135 (1942), *overruled in part by Katz*, 389 U.S. 347.

96. *Id.*

97. *Olmstead*, 277 U.S. at 464.

98. Jim Harper, *Escaping Fourth Amendment Doctrine After* Jones*: Physics, Law, and Privacy Protection*, *in* 2011–2012 CATO SUP. CT. REV. 219, 230–38 (Ilya Shapiro ed., 2012).

99. *Goldman*, 316 U.S. at 139 (Murphy, J., dissenting); *see also Olmstead,* 277 U.S. at 474 (Brandeis, J., dissenting) ("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 house.").

equally invaded by agents of the Government and intimate personal matters are laid bare to view."[100]

Justice Murphy's dissent was prescient. When *Olmstead* was decided, less than forty percent of American households were using telephones.[101] By the early 1960s, however, over eighty percent of households had phones.[102] Telecommunication networks were rapidly expanding, and the telephone soon became an indispensable part of society. If there were to be any future for privacy in telecommunications, the Court had no choice but to reconsider its position in *Olmstead*.

That moment arrived in 1967 with *Katz v. United States*.[103] In *Katz*, the Court ruled that the government's use of an electronic device to record conversations inside a telephone booth without a warrant violated the Fourth Amendment.[104] Declaring that the Fourth Amendment "protects people, not places," the Court made a decisive shift away from the traditional concepts of property and trespass that had long dominated its jurisprudence.[105] The Court looked beyond the picket fence and explicitly articulated for the first time that what a person "seeks to preserve as private" may be constitutionally protected "in an area accessible to the public."[106] Even though a pedestrian could *see* Katz speaking into the telephone, Katz had excluded the "uninvited ear" and preserved the privacy of his conversations by shutting the door behind him.[107] When government agents eavesdropped on Katz, they violated the privacy "upon which he justifiably relied."[108]

While the Court's recognition of "privacy in public" was groundbreaking, it did not provide guidance on how the Fourth Amendment protects such privacy beyond the telephone booth. Perhaps dissatisfied with the majority's limited holding, Justice Harlan sought to establish a general Fourth Amendment standard of privacy in his now famous concurrence:

> My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person has exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable."[109]

---

100. *Goldman*, 316 U.S. at 139 (Murphy, J., dissenting).

101. U.S. CENSUS BUREAU, *in* COMMUNICATIONS 775, 783 (1970), *available at* http://www2.census.gov/prod2/statcomp/documents/CT1970p2-05.pdf (U.S. Census report stating there were slightly more than 18.5 million phones in American homes in 1927).

102. *Id.* (estimating that nearly 81 million phones were in use by 1962, which included more than eighty percent of households).

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

104. *Id.* at 359.

105. *Id.* at 351.

106. *Id.* at 350–51.

107. *Id.* at 352.

108. *Id.* at 353.

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

This "reasonable expectation of privacy" formula has become the litmus test of Fourth Amendment protection in many cases, especially those involving electronic surveillance.[110] In theory, this rule maintains a flexible conception of privacy that allows courts to adapt Fourth Amendment protections to evolving technologies and social norms.[111] But in practice, such discretion places an onerous burden on judges first to determine whether a person actually expected privacy in a particular circumstance and then to divine whether society as a whole is prepared to accept that expectation as "reasonable."

Over the years, the "reasonable expectations" test has attracted sharp criticism for weakening the protection of "the People" against increasingly invasive police searches and seizures. In his influential 1974 lecture on the Fourth Amendment, Anthony Amsterdam pronounced that the "needless" inquiry into what society expects to be private "destroys the spirit of *Katz* and most of *Katz*'s substance."[112] Amsterdam observed that the government could easily diminish our expectations of privacy by "announcing half-hourly on television that . . . we were all forthwith being placed under comprehensive electronic surveillance."[113]

Many scholars have similarly criticized the ease with which the government can overcome expectations of privacy. "Existing expectations," Stephen Schulhofer observes, "are shaped by the police practices that the law allows."[114] If courts decide what the law allows "by looking to existing expectations, we end up chasing ourselves in a circle."[115] This circularity, according to Daniel Solove, is compounded by advancements in technology that allow widespread information sharing.[116] Such technology "gradually erode[s] what people expected to be private," paving the way for "more invasive" government searches of our information.[117] Indeed, Justice Alito has criticized the circularity of the

110. *See, e.g.*, United States v. Larios, 593 F.3d 82, 93 (1st Cir. 2010) (applying twofold reasonable expectation of privacy test to audio recordings of conversations in a motel room); United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007) (applying twofold reasonable expectation of privacy test to personal computers used on a university computer network); *In re* U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 119–20 (E.D.N.Y. 2011) (holding cell phone users have an objectively reasonable expectation of privacy in "long-term cell-site-location records").

111. *See* United States v. U.S. Dist. Court, 407 U.S. 297, 313 (1972) ("Though physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed, its broader spirit now shields private speech from unreasonable surveillance.").

112. Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 383 (1974).

113. *Id.* at 384.

114. SCHULHOFER, *supra* note 26, at 121.

115. *Id.* Jim Harper makes a similar argument when he criticizes the "essential circularity" of Harlan's formulation: "Societal expectations are guided by judicial rulings, which are supposedly guided by societal expectations, which in turn are guided by judicial rulings, and so on." *Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U. L. REV. 1381, 1392 (2008).

116. Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511 (2010).

117. *Id.* at 1524.

Katz test, drily noting that it is "not without its own difficulties."[118] The end result, according to Jim Harper of the Cato Institute, is that Harlan's formula stacks the deck in favor of law enforcement, "revers[ing] the Fourth Amendment's focus from the reasonableness of government action . . . to the reasonableness of the [privacy] interests the amendment was meant to protect."[119] Indeed, as Orin Kerr concludes, subjective expectations are largely irrelevant; in operation, *Katz* is "only a one-step test."[120]

Empirical studies have also demonstrated that the Supreme Court is at best unreliable when it comes to determining the actual privacy expectations of the average person. While the Court's presumptions and individuals' reactions align when it comes to some kinds of searches, in others the Court woefully underestimates the actual privacy impact.[121] The fact that the Justices know whether defendants have turned out to be murderers or priests, drug dealers or passing innocents, adds an additional wrinkle. While the rules should be the same for all, the indistinct contours of the "reasonable expectation of privacy" test allows the Court to be swayed by its knowledge that the people involved are guilty of the charges lodged, and its opinions sometimes suggest that its interpretations of the Fourth Amendment have been tailored to reach the desired outcomes.[122]

New technologies have a habit of making these problems worse.[123] The *Katz* test takes technology into account, but it does so through the lens of "reasonable

---

118. United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring).

119. Harper, *supra* note 115, at 1386.

120. Orin Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 114 (2014).

121. *See*, *e.g.*, Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 277, 279 (2002) (reporting results of survey in which, for instance, people believed helicopters flying over their backyard at a height of 400 feet to be intrusive, contrary to the Supreme Court's holdings in *California v. Ciraolo,* 476 U.S. 207 (1985), and *Florida v. Riley,* 488 U.S. 445 (1989)); Christopher Slobogin & Joseph Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727, 738, 740 (1993) (conducting similar survey in which, for instance, respondents reported that they would find governmental access to their bank records to be intrusive, contrary to the line of cases building on the Supreme Court's holding in United States v. Miller, 425 U.S. 435, 441–43 (1976)).

122. *See*, *e.g*, Slobogin & Schumacher, *supra* note 121, at 734–35 (noting that searches are generally perceived to be less intrusive if the reason for the search or the specific evidence being sought is described, suggesting that judges will tend to find many searches to be less intrusive than the general public would because most Fourth Amendment cases involve evidence suppression hearings where judges already know the crime being investigated and what evidence was found). In *Florida v. Riley*, Justice Brennan expressed his concern that the majority's decision, which found that a warrantless flyover of a defendant's backyard from 400 feet overhead, was in part motivated by the fact that the defendant was growing pot in the yard. *See* 488 U.S. 445, 464, 466 (Brennan, J., dissenting) ("The principle enunciated in this case determines what limits the Fourth Amendment imposes on aerial surveillance of any person, for any reason . . . . The Fourth Amendment demands that we temper our efforts to apprehend criminals with a concern for the impact on our fundamental liberties of the methods we use.").

123. *See generally*, Colin Shaff, Note, *Is the Court Allergic to* Katz*? Problems Posed by New Methods of Electronic Surveillance to the "Reasonable-Expectation-of-Privacy" Test*, 23 S. CAL. INTERDISC. L.J. 409 (2014).

expectations." That analysis requires judges to understand exactly how technology works and properly weigh its implications in a democratic society. In short, the test is technology dependent. Everything turns on expectations about the way technology works – and the ways that people and the government use it – at the moment the case is decided. This has led to some rather incongruous decisions. The *Kyllo* Court, for example, determined that police need a warrant to use thermal imaging on the exterior of a private home because "the technology in question is not in general public use."[124] But in *Florida v. Riley*, the Justices ruled that no warrant is required to use a helicopter to hover 400 feet above a backyard because "private and commercial flight by helicopter is routine."[125] In both cases, the Court focused on the use of technology and whether there was a physical trespass, ignoring the reality that for most laypeople, the privacy intrusion visited by both tactics is quite substantial. Moreover, the rules appear subject to change as new technology becomes integrated in society. Thus, in *City of Ontario v. Quon*, Justice Kennedy cautioned 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," citing *Olmstead* and *Katz* to illustrate his point.[126]

Post-*Katz*, the Court has struggled to craft a coherent vision of how the Fourth Amendment should apply to electronic communications and other forms of digital information. While *Katz* acknowledged the "vital role that the public telephone has come to play in private communication[s]" and required a warrant for police to eavesdrop,[127] just twelve years later, the Court ruled that those Fourth Amendment safeguards do not extend to the digits dialed or to other data that may be recorded for billing purposes.[128] This is the "third-party doctrine," and it is responsible for generating precedents that are an ill fit for modern technology or modern times, leaving things like email and online browsing records with little constitutional protection. As I argue next, it is the mistake that keeps on taking.

II. THE THIRD-PARTY DOCTRINE

The "third-party doctrine" originated with two Supreme Court decisions in the late 1970s, *United States v. Miller*[129] and *Smith v. Maryland*.[130] *Miller* involved government access to financial records held by a bank, and *Smith*

124. *See* Kyllo v. United States, 533 U.S. 27, 28 (2001).

125. *See Riley*, 488 U.S. at 445; *accord* California v. Ciraolo, 476 U.S. 207, 213–214 (1986) (holding no warrant is required for aerial surveillance of a residence at 1,000 feet because "[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed").

126. City of Ontario v. Quon, 560 U.S. 746, 759 (2010).

127. Katz v. United States, 389 U.S. 347, 352 (1967).

128. Smith v. Maryland, 442 U.S. 735, 742 (1979).

129. 425 U.S. 435 (1976).

130. 442 U.S. 735 (1979).

involved government access to telephone records held by a telephone company. Together, they are known for the rule that there is no Fourth Amendment interest in information knowingly and voluntarily revealed to "third parties."[131]

In this context, a "third party" includes any non-governmental institution or entity established by law.[132] Thus, under an aggressive reading of the third-party doctrine, the Fourth Amendment would not guarantee the privacy of any personal data held by any private company.[133] This would include virtually all records of electronic communications, web browsing activity, and cloud data, to name just a few examples.

In practice, congressional alarm over the implications of this theory has resulted in legislation affording privacy to some categories of third-party records. In 1978, Congress passed the Right to Financial Privacy Act in response to *Miller*,[134] and in 1986, it passed the Electronic Commutations Privacy Act (ECPA) following *Smith*.[135] Lawmakers have also created more targeted laws aimed at protecting the privacy of cable subscribers[136] and video store customers.[137] But these efforts have been scattershot and often hobbled by changing technologies. ECPA, for example, was ahead of its time in many respects,[138] but it is now woefully outdated and in need of an overhaul to account for changes in the communications technology we use and how we use it.[139]

The third-party doctrine has encountered a growing chorus of criticism as people live more of their lives online, divulging personal information and generating third-party records in the course of everyday tasks.[140] Justice So-

131. *Smith*, 442 U.S. at 743–44; *Miller*, 425 U.S. at 442–44.

132. *See* STANDARDS FOR CRIMINAL JUSTICE: LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS §1.1(e) (3d ed. 2013), *available at* http://www.americanbar.org/groups/criminal_justice/standards/law_enforcement_access.html (defining an "institutional third party" as "(i) any nongovernmental entity, including one that receives government funding or that acquires information from government sources; and (ii) any government institution functioning in a comparable capacity, such as a public hospital or a public university").

133. Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 638–39 (2011).

134. Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401, et seq. (2013).

135. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.) (2013).

136. Cable Communications Privacy Act of 1984, 47 U.S.C. § 551 (2013).

137. Video Privacy Protection Act of 1988, 18 U.S.C. §§2710–2711 (2013).

138. *ECPA Part 1: Lawful Access to Stored Content: Hearing on S. 1452 Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 113th Cong. 47 (2013) (written statement of Richard Salgado, Director, Law Enforcement and Information Security, Google Inc.).

139. Under current law, for example, email older than six months is presumed to be abandoned and therefore accessible to law enforcement without a warrant. *See* 18 U.S.C. §2703. Even the Department of Justice has acknowledged that there is no longer any principled reason for the rule and agrees that parts of the statute need to be updated. *ECPA Part 1: Lawful Access to Stored Content: Hearing on S. 1452 Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 113th Cong. 14 (2013) (testimony of Elana Tyrangiel, Acting Asst. Att'y Gen., Office of Legal Policy, Dept. of Justice).

140. *See, e.g.*, Orin Kerr & Greg Nojeim, *The Data Question: Should the Third-Party Records Doctrine Be Revisited?*, A.B.A. J. (Aug. 1, 2012, 4:20 AM), http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited/.

tomayor is among the most prominent critics, describing the rule as "ill suited to the digital age" and suggesting that it may be necessary to reconsider the premise altogether.[141] Indeed, modern technology has dramatically expanded the scope of the third-party doctrine to reach far beyond records of bank transactions and telephone calls. Even if the doctrine made sense in the 1970s, its ever-widening reach is no longer consistent with the history and purpose of the Fourth Amendment.

A. Origins of the Third-Party Doctrine

Miller and *Smith* were not on particularly sound constitutional footing in the first place. In *Miller*, the Supreme Court found no reasonable expectation of privacy in the contents of checks and deposit slips processed by a bank.[142] The Court reasoned that the "depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[143]

The Court decided *Smith* three years after *Miller*, approving the warrantless use of a "pen register" to produce a list of telephone numbers dialed by a criminal suspect over the course of a day.[144] The Court determined that there was no Fourth Amendment violation because the suspect "voluntarily conveyed" the information to the phone company. Accordingly, he "assumed the risk" that the company would reveal that information to police.[145]

The Court took a wrong turn in crafting a rule that treats "third parties," such as phone companies, as if they were a part of the conversation. For one thing, the doctrine stems from a line of cases that has nothing to do with third parties. These decisions instead involved secret agents and invited informants – where the interlocutor was an actual participant in the conversation, not a communications carrier.[146]

In *Hoffa v. United States*, for example, the FBI used an informant wearing a wire to obtain evidence used to convict Jimmy Hoffa of attempting to bribe a grand juror.[147] Hoffa appealed his conviction to the Supreme Court, arguing that the FBI had violated the Fourth Amendment by placing the informant (and therefore the wire) in his hotel suite.[148] The Court found it dispositive that the informant was in Hoffa's suite by invitation, as well as the fact that "every conversation which he heard was either directed to him or knowingly carried on

141. United States v. Jones, 132 S.Ct. 945, 957 (2012) (Sotomayor, J., concurring).

142. United States v. Miller, 425 U.S. 435, 442–43 (1976).

143. *Id.* at 443 (citing United States v. White, 401 U.S. 745, 751–52 (1971)).

144. Smith v. Maryland, 442 U.S. 735, 737 (1979).

145. *See id.* at 743–44 (quoting *Miller*, 425 U.S. at 442–44).

146. *Id.* at 744 (citing *Miller*, 425 U.S. at 442–44; Couch v. United States, 409 U.S. 322, 335–36 (1973); *White*, 401 U.S. at 752; Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427 (1963)); *see also* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 567–69 (2009).

147. *Hoffa*, 385 U.S. at 296.

148. *Id.* at 300.

in his presence."[149] Had the FBI bugged the minibar, they would have had to get a warrant.[150] But because Hoffa invited the informant to participate in the conversation, the Court found no Fourth Amendment defect, instead faulting Hoffa's misplaced confidence in the informant.[151]

Lopez v. United States, decided just a few years earlier, is also an invited informant case with no third party involved.[152] The case involved German Lopez, an innkeeper who attempted to bribe an IRS agent twice in three days.[153] The agent wore a wire to their second meeting, creating a recording that was used to convict Lopez.[154] Again, the determinative factors for the Supreme Court were that Lopez had invited the agent into his office for a conversation, that the agent did not seize anything without the innkeeper's knowledge, and that the evidence at trial consisted of statements that Lopez "knew full well could be used against him" by an avowed IRS agent.[155] The Court reaffirmed this holding in *United States v. White*, which involved an invited informant who wore a wire that transmitted audio in real time to federal agents.[156]

Smith and *Miller* were a significant departure from cases involving conversations with "companions," "colleagues," and "associates."[157] The Court equated the phone company and the bank with invited informants,[158] but it is not clear that the assumption of risk rationale supports this leap. Unlike the informants in *Hoffa* and *Lopez*, the phone company is an intermediary that is neither a part of the call nor entirely excludable from it. When making a call, there is simply no choice but to involve the phone company. It is likewise impossible to fully participate in modern economic life without involving a bank to execute transactions. Because this third-party interaction is unavoidable, it undermines the assumption of risk rationale.

Everyone has to make decisions about whom to talk to and whom to trust with private information. Sometimes people make mistakes – just ask Jimmy Hoffa. But at least there is a choice. By creating a third-party rule for banks and communications carriers, the Court mistakes necessity for choice. Of course, one could refrain from making phone calls altogether, or revert to using carrier pigeons and gold coins, but this is not a realistic option in a modern society.

---

149. *Id.* at 302.

150. *See id.* at 317 (Warren, C.J., dissenting) (approving the issuance of a warrant to equip an undercover officer with a recording device).

151. *Id.* at 302. Five years later, the Court decided *White*, 401 U.S. at 746–47, which also involved an invited informant wearing a wire. Unlike in *Hoffa*, the wire in *White* transmitted real time audio to the FBI, but the Court dismissed this distinction and reiterated its holding in *Hoffa*. *See* 385 U.S. at 751.

152. Lopez v. United States, 373 U.S. 427 (1963).

153. *Id.* at 429–32.

154. *Id.* at 430–31.

155. *Id.* at 438.

156. *White*, 401 U.S. at 751–52.

157. Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976).

158. *See Miller*, 425 U.S. at 443.

B. Third-Party Records Today

Even if the assumption of risk rationale made sense in *Miller* and *Smith*, applying the third-party rule in today's world is inconsistent with the history and purpose of the Fourth Amendment. Almost every aspect of online life now leaves a trail of digital breadcrumbs in the form of third-party records. Every phone call, every email, every search and click online can create a third-party record. Google, for example, keeps a copy of every search it is asked to make and, if possible, links each search to a particular user.[159] There are even records of what people *do not* read and *do not* click.[160] If courts take the third party doctrine seriously, then police can lawfully obtain all of this information without a warrant or probable cause. It is no hyperbole to say that even a person's mere curiosity could and would be monitored. As Daniel Solove observes, "[T]his state of affairs poses one of the most significant threats to privacy in the twenty-first century."[161]

The third-party doctrine is especially problematic in the digital age because it treats privacy as a binary equation: either information is completely secret, or it is absolutely public. This principle is at odds with the way that people share information online. As with other types of personal interaction, sharing digital data is not an all-or-nothing endeavor; it is more like a sliding scale that users may control (although not always with success). Depending on the social media context, one may opt to comment anonymously, to send a message to just a few friends, or to post a public video on YouTube in search of worldwide Internet fame.[162] The third-party doctrine disregards this nuance, treating everything as public.

As more of life takes place online, the doctrine becomes more devastating to freedom of speech and association. Imagine a society where every thought,

---

159. LESSIG, *supra* note 89, at 203–04.

160. Alexandra Alter, *Your E-Book Is Reading You*, WALL ST. J. (July 19, 2012), http://online.wsj.com/news/articles/SB10001424052702304870304577749095005143830; *see also Click Heatmaps*, MOUSEFLOW, https://mouseflow.com/tour/heatmaps/.

161. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1087 (2002).

162. *See, e.g.*, Kirsty Hughes, *A Behavioural Understanding of Privacy and its Implications for Privacy Law*, 75 MOD. L. REV. 806, 806 (2012) ("Privacy is a multi-faceted concept which derives its meaning in particular situations from the social context and the ways in which people experience and respond to those situations."); Danah Boyd & Alice E. Marwick, *Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies*, Presented at A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, Sept. 22, 2011, http://ssrn.com/abstract=1925128 ("Privacy is both a social norm and a process; it is not something that is had so much as something that is negotiated."); George R. Milne & Shalini Bahl, *Are There Differences Between Consumers' and Marketers' Privacy Expectations? A Segment- and Technology-Level Analysis*, 29 J. PUB. POL'Y & MARKETING 138, 139 (2010) ("Research has shown that consumers have varying levels of privacy concerns."); Lisa Nelson, *Privacy and Technology: Reconsidering a Crucial Public Policy Debate in the Post–September 11 Era*, 64 PUB. ADMIN. REV. 259, 266 (2004) ("Increasingly, privacy relates to the diverse modes by which people, personal information, certain personal property, and personal decision making are made less accessible to others. While privacy is protected by law, it is also governed by culture, ethics, and business and professional practices.").

every utterance, every behavior conveyed through digital means is "public" information, cataloged in a database, just waiting for the police to request it.[163] The resulting chill to freedom of speech and association would cause an ice age.

Given this context, it is imperative that the Supreme Court establish new rules for government access to third-party records.[164] Property law and the antiquated trespass doctrine are not promising springboards. The "reasonable expectations" framework is likewise prone to error whenever new technology is involved. Although both approaches continue to provide some measure of protection against traditional methods of search and seizure, they have also struggled to respond to the realities of the digital age. Instead, the Court should contemplate a new paradigm for the information age, another *Olmstead-Katz* moment.[165]

This is not a call to abandon the property-oriented and reasonable expectation tests. It makes sense to talk about home searches in terms of property rights, for example. At the same time, situations that do not involve physical trespass into the home may remain subject to the *Katz* analysis.[166] When it comes to data privacy, however, the Court may want to incorporate a third way that will co-exist with and complement existing approaches.[167]

---

163. *See* Osborn v. United States, 385 U.S. 323, 353–54 (1966) (Douglas, J., dissenting) ("The time may come when no one can be sure whether his words are being recorded for use at some future time; when everyone will fear that his most secret thoughts are no longer his own, but belong to the Government; when the most confidential and intimate conversations are always open to eager, prying ears. When that time comes, privacy, and with it liberty, will be gone. If a man's privacy can be invaded at will, who can say he is free? If his every word is taken down and evaluated, or if he is afraid every word may be, who can say he enjoys freedom of speech? If his every association is known and recorded, if the conversations with his associates are purloined, who can say he enjoys freedom of association? When such conditions obtain, our citizens will be afraid to utter any but the safest and most orthodox thoughts; afraid to associate with any but the most acceptable people. Freedom as the Constitution envisages it will have vanished.").

164. *See* United States v. Jones, 132 S. Ct. 945, 957 (2011) (Sotomayor, J., concurring) ("I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.").

165. *See, e.g.*, Brief for Nat'l Assoc. of Crim. Def. Lawyers et al. as Amici Curiae Supporting Appellant, at 6, Ohio v. Johnson, 964 N.E.2d 426 (Ohio 2012) (No. 2011-0033), 2011 WL 2456552, at *VII ("[The law is at] a watershed moment in Fourth Amendment jurisprudence, very much akin to the '*Olmstead-Katz*' moment.").

166. *Jones*, 132 S. Ct. at 953.

167. As Justice Scalia explained in *Jones*, the trespass and "reasonable expectation of privacy" tests are not mutually exclusive. 132 S. Ct. at 950–51 ("[F]or most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates. *Katz* did not repudiate that understanding . . . . [It was not] intended to withdraw any of the protection which the Amendment extends to the home . . . ." (quoting Alderman v. United States, 394 U.S. 165, 180 (1969))); *see also* Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013) ("By reason of our decision in *Katz* . . . , property rights are not the sole measure of Fourth Amendment violations, . . . but though *Katz* may add to the baseline, it does not subtract anything from the Amendment's protections when the Government *does* engage in [a] physical instruction of a constitutionally protected area . . . ." (citations and internal quotation marks omitted)).

III. A FIRST AMENDMENT THEORY OF THE FOURTH AMENDMENT

In this section, I outline what a supplemental framework might look like. I turn to the text, history, and purpose of the Fourth Amendment, focusing on its ties to First Amendment rights, to develop a test focused on the privacy of one's "papers." In Section IV, I return to the third-party records issue and apply the test to two common types of records: data stored in the cloud and electronic communications. Under this rubric, such records of expressive activity would receive full Fourth Amendment protection, on par with the privacy of one's house or person.

The Fourth Amendment framework proposed here is a three-step test for data privacy, analytically distinct from both the trespass and reasonable expectation tests. The first step asks whether the data at issue falls under the Fourth Amendment umbrella of "papers." The answer rests on the history and purpose of the Fourth Amendment, which dictate a duty to safeguard expressive and associational materials from unreasonable government intrusion.[168] One way to do this is by designating entire categories of data, such as communications data and cloud data, for Fourth Amendment protection. Step two asks whether there was a search or seizure of that data. In this context, a search occurs when accessing or revealing information that is not available to the general public. A seizure occurs when there is some meaningful interference with an individual's possessory interests in the information, which includes the copying of data. Step three considers whether a warrant should be required and urges a presumption in favor of a warrant requirement for access to protected data.

A. Expressive and Associational Data as Fourth Amendment "Papers"

The Fourth Amendment provides for the "right of the people to be secure in their *persons*, *houses*, *papers*, and *effects*, against unreasonable searches and seizures."[169] While there is a large body of precedent concerning searches of the home or person, the Supreme Court has not fully explored the contours of Fourth Amendment "papers," apart from their physical presence on a person or in a "constitutionally protected area."[170] But when digital records are at issue, it seems intuitive that the place to look for Fourth Amendment protection is in the privacy of one's "papers." In *Riley v. California*, a unanimous Court hinted toward this logic in recognizing the difference between a warrantless pat down incident to arrest and a digital search of the data on an arrestee's cell phone.[171] While such physical searches have long been permissible without a warrant, the

168. *See* Stanford v. Texas 379 U.S. 476, 485 (1965) (stating that the Fourth Amendment must be applied with "scrupulous exactitude" when significant First Amendment rights are at stake); *see also* Zurcher v. Stanford Daily, 436 U.S. 547, 564 (1978) (citing Stanford v. Texas, 379 U.S. at 485).

169. U.S. CONST. amend. IV (emphasis added).

170. *See infra* note 312.

171. Riley v. California, 134 S. Ct. 2473, 2489 (2014).

Court concluded that "any extension of that reasoning to digital data has to rest on its own bottom."[172]

The theory proposed here is that the inclusion of "papers" in the text of the Fourth Amendment provides independent protection against warrantless searches and seizures of data likely to have significant expressive or associational interest. Of course, it is not immediately clear what kinds of data would fall under the aegis of Fourth Amendment "papers." In general, I contend that the history and purpose of the Fourth Amendment require a flexible reading of "papers" that would encompass clear categories of potentially expressive and associational data.[173] As I elaborate in Section IV, personal files stored in the cloud, as well as communications data and metadata would fall into this basket.

In order to illustrate how Fourth Amendment "papers" might expand to include data held by a third party, consider the evolution of the Supreme Court's jurisprudence on "houses." A literal reading of the term could limit the scope of the Fourth Amendment quite significantly. Yet the Court has consistently extended constitutional protection far beyond the four walls of a private residence to include garages,[174] boarding houses,[175] rented houses,[176] hotel rooms,[177] park cabins,[178] factories,[179] private offices,[180] and mobile homes.[181] Indeed, the Court has said that it is "unnecessary and ill-advised" to determine the scope of Fourth Amendment freedoms based on "subtle distinctions" in property law, the validity of which is "largely historical."[182] Instead, the Court assumes a "duty to see that this historic provision receives a construction sufficiently liberal and

172. *Id.*

173. The Fourth Amendment is no mere statute; it is a part of the United States Constitution. And as such, it would be folly to read its words too literally and without regard to context and intent. Goldman v. United States, 316 U.S. 129, 138 (1947) (Murphy, J., dissenting) ("[I]t has not been the rule or practice of this Court to permit the scope and operation of broad principles ordained by the Constitution to be restricted, by a literal reading of its provisions, to those evils and phenomena that were contemporary with its framing."), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967). As Justice Marshall warned in *McCulloch v. Maryland*, "we must never forget that it is a *constitution* we are expounding." 17 U.S. 316, 407 (1819).

174. Taylor v. United States, 286 U.S. 1, 5–6 (1932).

175. *See* McDonald v. United States, 335 U.S. 451, 454 (1948).

176. Chapman v. United States, 365 U.S. 610, 616–17 (1961).

177. Stoner v. California, 376 U.S. 483, 490 (1964); Johnson v. United States, 333 U.S. 10, 12, 15 (1948).

178. Flippo v. West Virginia, 528 U.S. 11, 12, 15 (1999) (per curiam).

179. *See* Dow Chem. Co. v. United States, 476 U.S. 227, 236 (1986) (finding no Fourth Amendment violation in the warrantless aerial photography of the exterior of a chemical plant, but emphasizing that "Dow plainly has a reasonable, legitimate, and objective expectation of privacy within the interior of its covered buildings, and it is equally clear that expectation is one society is prepared to observe").

180. O'Connor v. Ortega, 480 U.S. 709, 718 (1987).

181. Soldal v. Cook Cty., Ill., 506 U.S. 56, 61 (1992). *But see* California v. Carney, 471 U.S. 386, 392–93 (1985) (finding a reduced expectation of privacy in a mobile home capable of being used on the highway and not located in a place regularly used for residential purposes).

182. *Stoner*, 376 U.S. at 488 (quoting Jones v. United States, 362 U.S. 257, 266–67 (1960)).

elastic to make it serve the needs and manners of each succeeding generation."[183]

The history and purpose of the Fourth Amendment must therefore play a critical role in determining whether digital data should be considered "papers." Of course, the fact that the Framers could not have envisioned telephones, email, computers, or Tinder is beside the point. As Justice Burger put it, while the Framers "focused on the wrongs of that day," they also "intended the Fourth Amendment to safeguard fundamental values which would far outlast the specific abuses which gave it birth."[184] For the colonialists, the chief evil on this side of the Atlantic may have been the writs of assistance in search of smuggled goods. But, as detailed in Section I, John Adams and the Sons of Liberty were well aware of the Wilkes affair and had his struggle in mind when specifying "papers" for constitutional protection.

The Framers understood that the First Amendment values of free speech and freedom of association are essential to a democratic society, and they understood that one of the most important ways to safeguard those rights was through the Fourth Amendment. In fact, the privacy protection afforded to "papers" was once so absolute that the Supreme Court prohibited their seizure for use as "mere evidence" at trial.[185] The Court abandoned this approach in 1967, ostensibly because this did a poor job of protecting privacy and created "considerable confusion in the law."[186] But it is nonetheless a strong indication of the historical importance attached to the privacy of one's papers, as well as the strong relationship between the First and Fourth Amendments.

Indeed, the Supreme Court continues to recognize that First Amendment values permeate the Fourth Amendment, requiring courts to apply the Fourth Amendment with "scrupulous exactitude" when significant First Amendment rights are at stake.[187] In case after case, the Court has hearkened back to the historical underpinnings of the Fourth Amendment and the First Amendment values that gave it shape.[188]

---

183. Goldman v. United States, 316 U.S. 129, 138 (1942) (Murphy, J., dissenting), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

184. United States v. Chadwick, 433 U.S. 1, 9 (1977), *abrogated by* California v. Acevedo, 500 U.S. 565 (1991).

185. Boyd v. United States, 116 U.S. 616, 623 (1886) ("The search for and seizure of stolen or forfeited goods, or goods liable to duties and concealed to avoid the payment thereof, are totally different things from a search for and seizure of a man's private books and papers for the purpose of obtaining information therein contained, or of using them as evidence against him. The two things differ *toto coelo*. In the one case, the government is entitled to the possession of the property; in the other it is not."); *see also* Gouled v. United States, 255 U.S. 298, 264–65 (1921) (outlining the contours of the "mere evidence" rule).

186. Warden v. Hayden, 387 U.S. 294, 309 (1967).

187. Stanford v. Texas, 379 U.S. 476, 485 (1965); *see also* Zurcher v. Stanford Daily, 436 U.S. 547, 564 (1978) (citing *Stanford*, 379 U.S. at 485).

188. *See, e.g.*, New York v. P. J. Video, Inc., 475 U.S. 868, 873 (1986) ("We have long recognized that the seizure of films or books on the basis of their content implicates First Amendment concerns not raised by other kinds of seizures. For this reason, we have required that certain special conditions be met before such seizures may be carried out."); Roaden v. Kentucky, 413 U.S. 496, 504 (1973) (noting that the Court examines the question of reasonableness under the Fourth Amendment "in the light of the

Thus, in determining what data qualifies as a "paper" for the purposes of the Fourth Amendment, the focus should be on whether there is an expressive or associational interest in the data, consistent with First Amendment values. Of course, it is no simple task to distinguish, *ex ante*, between data that is and is not of First Amendment value.[189]

It is clear enough that an email convening a political protest has both expressive and associational qualities, but an online search for "toe rot" or "schizophrenia" may be less obvious. Every phone call is not a matter of political, artistic, or religious debate; it may be a reminder to pick up milk on the way home from work. Until someone listens to that conversation, there is no way to make a determination about its First Amendment value.

Nor is it a solution to decide the question in court after the fact. The constitutional harm lies in the first instance of search and seizure. Instead, as in the wiretap context, the Supreme Court should recognize categories of data for Fourth Amendment protection that are likely to include protected expressive and associational information, even if the substance is not always the epitome of First Amendment speech. Section IV identifies two such categories: (1) personal data stored in the cloud, and (2) communications data. I argue that this data, as well as its associated metadata, should be treated like private "papers" for purposes of the Fourth Amendment.

In this framework, the particular form or format of the data is not terribly important. The inquiry, in other words, should be technology-neutral. If "papers" include private correspondence in the mail, then the same constitutional protection should carry forward to new and alternative modes of communication, whatever they may be. Phone calls, for example – sound waves transmitted over copper wire – are an essential form of private communication, deserving

---

values of freedom of expression"); *Stanford*, 379 U.S. at 482 (describing the history of the Fourth Amendment as "largely a history of conflict between the Crown and the press"); Lopez v. United States, 373 U.S. 427, 469–70 (1963) (Brennan, J., dissenting) ("[W]e must bear in mind that historically the search and seizure power was used to suppress freedom of speech and of the press . . . ." (internal citations omitted)); Marcus v. Search Warrants of Prop. at 104 E. Tenth St., 367 U.S. 717, 724 (1961) ("Historically 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."); Frank v. Maryland, 359 U.S. 360, 376 (1959) (Douglas, J., dissenting) (stating that the First, Fourth, and Fifth Amendments "are indeed closely related, safeguarding not only privacy and protection against self-incrimination but conscience and human dignity and freedom of expression as well" (internal citations and quotation marks omitted)); *see also* Yale Kamisar, *The Fourth Amendment and Its Exclusionary Rule*, THE CHAMPION, Sept.-Oct. 1991, at 20, 21 ("What good is freedom of speech or freedom of religion or any other freedom if law enforcement officers have unfettered power to violate a person's privacy and liberty when he sits in his home or drives his car or walks the streets?").

189. *See Marcus,* 367 U.S. at 731 ("[T]he use of these warrants implicates questions whether the procedures leading to their issuance and surrounding their execution were adequate to avoid suppression of constitutionally protected publications . . . . The separation of legitimate from illegitimate speech calls for . . . sensitive tools." (internal quotation marks omitted)); *see also* Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring) ("I shall not today attempt further to define the kinds of material I understand to be embraced within that shorthand description; and perhaps I could never succeed in intelligibly doing so. But I know it when I see it . . . .").

equal Fourth Amendment protection as parchment sealed with wax. Privacy should not become a casualty of technology. Letters, telegraphs, phone calls, emails, and text messages – they are all forms of private communication and would therefore be treated as "papers" for Fourth Amendment purposes.

Such a technology-neutral approach is efficient and dynamic. It operates at a level of abstraction that facilitates adaptation to different circumstances, and thus aims to avoid the need for litigation over every new app or gadget. Uncertainty in the law is bad for businesses that develop and market new technologies and bad for consumers who want to understand the legal risks before using them. Neither judges nor the general public will need to understand technical details or wait and see how the technology becomes integrated into daily life to determine whether society has a reasonable expectation of privacy in its use.

For personal files stored in the cloud, it is not difficult to imagine them as twenty-first-century "papers." In most cases, the difference between cloud data and a document in the filing cabinet is a matter of hitting "print." Just as Fourth Amendment "houses" may include a rented apartment,[190] a hotel room,[191] or a storage locker,[192] so too should Fourth Amendment "papers" include personal files stored on a remote commercial server.

Metadata, of course, is the elephant in the room. Every electronic communication contains so-called content and non-content data. The audio of a phone call, the body of an email, and the characters in a text message fall in the "content" camp, for example. But for each communication, there is also a range of non-content data associated with it, often referred to as "metadata." Phone calls generate logs with the phone company that track the numbers dialed, the length of the call, and the location of the caller. Every email contains a "header" full of metadata about how, when, and where the message is transmitted.[193] It indicates who sent the message, who received it, and what it was about (depending on the descriptiveness of the subject line).[194]

Under the third-party doctrine, none of this metadata would receive Fourth Amendment protection. The text of the Fourth Amendment, however, does not actually draw a distinction between one's private papers and information about those papers, between data and metadata.[195] Viewed another way, metadata is just additional private data that happens to be stored by a third party. Thus, the

---

190. Chapman v. United States, 365 U.S. 610, 616–17 (1961).

191. Stoner v. California, 376 U.S. 483, 490 (1964) (internal citation omitted); Johnson v. United States, 333 U.S. 10, 12, 15 (1948).

192. United States v. Karo, 468 U.S. 705, 720 n.6 (1984).

193. *See, e.g.*, Gmail Help, *Reading Full Email Headers*, GOOGLE, https://support.google.com/mail/answer/29436?hl=en.

194. *Id.*

195. *See* JAY STANLEY, THE CRISIS IN FOURTH AMENDMENT JURISPRUDENCE, AM. CONSTITUTION SOC'Y FOR LAW & POLICY 4 (2014), https://www.acslaw.org/publications/issue-briefs/the-crisis-in-fourth-amendment-jurisprudence-0 ("The Court has created a distinction, not found in the Constitution, between 'addressing' or 'transactional' data, and content data, with the former receiving no constitutional protection.").

constitutional analysis proposed here does not rest on the fading line between content and non-content or data and metadata. At the end of the day, it is all data, all zeros and ones. For our purposes, the most important question is whether the metadata, like any other kind of data or third-party record, implicates significant First Amendment expressive and associational rights.[196]

I specifically address communications metadata in Section IV. But suffice it to say here that metadata generally is quite capable of revealing information about one's political or religious associations, interests and dislikes, or habits and predilections that would otherwise be difficult to determine.[197] That is precisely why law enforcement and intelligence agencies are so eager to collect and analyze it.[198] Analyzing a cache of metadata over time can be more telling than the content of the messages themselves. The metadata associated with a single email to a group of supporters could easily reveal the membership list of a political organization. It is possible to map entire social networks, identify influential members, or see who is on the outs.[199] It is likely to reveal relationships with lawyers, lovers, religious counselors, and political organizations.[200] What's more, the use of sophisticated computer algorithms to detect patterns and anomalies reduces this task to a few mouse clicks.[201] This type of intrusion

196. *See* Zurcher v. Stanford Daily, 436 U.S. 547, 564 (1978) ("A seizure reasonable as to one type of material in one setting may be unreasonable in a different setting or with respect to another kind of material." (quoting Roaden v. Kentucky, 413 U.S. 496, 501 (1973))).

197. *See, e.g.*, Dahlia Lithwick & Steve Vladeck, *Taking the "Meh" Out of Metadata*, SLATE (Nov. 22, 2013), http://www.slate.com/articles/news_and_politics/jurisprudence/2013/11/nsa_and_metadata_how_the_government_can_spy_on_your_health_political_beliefs.html; Kieran Healy, *Using Metadata to Find Paul Revere*, KIERANHEALY.ORG (June 8, 2013), http://kieranhealy.org/blog/archives/2013/06/09/using-metadata-to-find-paul-revere/; Nilay Patel, *Yo: Why the Silliest App in Tech Makes the NSA Look Ridiculous*, VOX (July 21, 2014), http://www.vox.com/2014/7/21/5922781/yo-why-the-silliest-app-in-tech-makes-the-nsa-look-ridiculous (describing a messaging application in which the content is *always* "Yo!" and the meaning derived solely from contextual information, such as the identity of the sender or the time the message was sent – i.e., metadata only).

198. *See generally*, Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741 (2008).

199. *See, e.g.*, Kashmir Hill, *Here's a Tool to See What Your Email Metadata Reveals About You*, FORBES (July 10, 2013), http://www.forbes.com/sites/kashmirhill/2013/07/10/heres-a-tool-to-see-what-your-email-metadata-reveals-about-you/.

200. Jennifer Granick, *Debate: Metadata and the Fourth Amendment*, JUST SECURITY (Sept. 23, 2013), http://justsecurity.org/927/metadata-fourth-amendment/.

201. Charles Duhigg, *How Companies Learn Your Secrets,* N.Y. TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html (describing Target and other companies' controversial development and use of algorithms to decipher and predict customers' shopping habits); Matt Blaze, *Phew, NSA Is Just Collecting Metadata. (You Should Still Worry)*, WIRED (June 19, 2013), http://www.wired.com/2013/06/phew-it-was-just-metadata-not-think-again/ ("Metadata, on the other hand, is ideally suited to automated analysis by computer. Having more of it just makes it the analysis more accurate, easier, and better. So while the NSA quickly drowns in data with more voice content, it just builds up a clearer and more complete picture of us with more metadata."); Declaration of Professor Edward W. Felten at 8, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 13-CV-3994) ("[T]he structured nature of metadata makes it very easy to analyze massive datasets using sophisticated data-mining and link-analysis programs . . . . Sophisticated computing tools permit the analysis of large datasets to identify embedded patterns and relationships, including personal details, habits, and behaviors. As a result, individual pieces of data that previously carried less potential to expose private

can implicate First Amendment freedom of expression and association with even greater force and ease than slogging through the actual content of communications.[202] Thus, metadata associated with protected content should receive the same Fourth Amendment protection as the content itself. The same should hold true for the metadata generated by cloud computing.

B. Was There a Search or Seizure?

Assuming the Fourth Amendment protects one's "papers," however defined, the next question is how to determine when there is a search of them. One of the great difficulties with the *Katz* test is that it conflates the search or seizure question with a normative inquiry about whether people believe something should be private. The test here seeks to disentangle those two questions. It frontloads (and simplifies) the normative issue by asking whether digital data should receive Fourth Amendment protection as a form of "papers." After that point, the doctrinal heavy lifting is over. Step two, determining whether a search or seizure has occurred, should be fact-based and objective.

1. Searches

According to the *Katz* test, a search requires both a subjective (individual) expectation of privacy and a legal determination that society is prepared to accept that expectation as reasonable. Under the test proposed here, the inquiry is a verifiable question of fact: Was the data actually and voluntarily disclosed to the general public?

The underlying premise is that information privacy is about control over personal information.[203] Sometimes we choose to reveal that information to the world, as when speaking from the proverbial soapbox or sending a tweet. At the other extreme, there may be some information we choose to take to our graves (please provide your own example). Privacy is a matter of degree, not absolutes. There is a whole lot in between the soapbox and the coffin. And that space between is the stuff of friendship and familial bonds, of business and professional relationships, and of political and religious associations. It is absolutely essential to a free and democratic society.[204]

---

information may now, in the aggregate, reveal sensitive details about our everyday lives – details that we had no intent or expectation of sharing.").

202. Katherine J. Strandburg, *Membership Lists, Metadata, and Freedom of Association's Specificity Requirement*, 10 I/S: A J. OF L. & POL'Y 327, 328 (2014).

203. *See generally*, DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 166, 170 (2007) ("Privacy is a complicated set of norms, expectations, and desires that goes far beyond the simplistic notion that if you're in public, you have no privacy . . . . It involves establishing control over personal information, not merely keeping it completely secret.").

204. NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958) ("Inviolability of privacy in group association may in many circumstances be indispensible to preservation of freedom of association, particularly where a group espouses dissident beliefs."); *see also* Brown v. Socialist Workers '74 Campaign Comm., 459 U.S. 87, 91–93 (1982); Shelton v. Tucker, 364 U.S. 479, 488 (1960); Bates v. Little Rock, 361 U.S. 516, 523–24 (1960).

In order to protect these First Amendment freedoms, the Fourth Amendment search question should focus on whether the data was otherwise made available to the general public. If it was, then there can be no logical claim to privacy. If it was not, then the information was, at least to some extent, private. It might have been known to only close friends or family, or perhaps to a larger political or religious group, or even to a giant telecommunications corporation. But the individual did not reveal it publicly, voluntarily or otherwise.[205] When the government takes steps to frustrate that control over private data, it should be considered a search.

Under this formulation, a search can occur directly, for example, by accessing the information stored on personal electronic device without consent, but it can also happen indirectly by obtaining the information from a third party, such as a phone company or Internet service provider.

Determining whether there is a search is a fact-intensive inquiry, but it escapes the subjectivity inherent in the *Katz* reasonable expectations rubric. Courts may hear testimony to determine whether particular data was actually available to the general public. Most people, for example, do not publicize their emails; nor do they publicize with whom, where, or when they communicate. Of course, recipients of these emails know some of this information, and communications service providers may know even more. I might not remember where I was when checking my inbox, but my service provider certainly does. Yet short of requesting those records from the company and posting them online, that information is in no way available to the general public.

The key here is that the default is set to privacy. The burden is on the government to demonstrate that the data was actually available to the general public.[206] Individuals would not need to prove they had a subjective expectation of privacy, which might otherwise impose unreasonable strains on modern communications. Military-grade encryption should not be required to send a private love note. Nor should people be required to forego the conveniences of modern technology in order to maintain their privacy. Just as hacking into a hard drive would be a search by most measures, so too is compelling disclosure from a third-party service provider.

---

205. This is not to suggest that the principle in *Hoffa* must be overturned. A third-party service provider is not a confidant or the intended recipient of most electronic communications; it is an inescapable intermediary, a part of the communications machinery. In this light, the "assumption of risk" rationale underlying *Hoffa* makes little sense when applied to third parties and should not defeat an individual's attempt to control the privacy of personal communications. *See infra* notes 142-158 and accompanying text.

206. Here, the question is whether the data itself was available to the general public, not whether the technology that generated or captured it is in general use. *Cf.* Kyllo v. United States, 533 U.S. 27, 34 (2001). Thus, even though plug-and-play computer hacking software may be widely available online (and it is), that reality should not diminish the privacy interest in personal data. *See, e.g.*, Scott Neuman, *Hacking Made Easier, Thanks to User-Friendly Tools*, NPR (Sept. 16, 2011), http://www.npr.org/2011/09/16/140540913/hacking-made-easier-thanks-to-new-tools.

2. Seizures

The Supreme Court defines the seizure of property as the "meaningful interference with an individual's possessory interest in that property."[207] I do not propose to disrupt that doctrine here, but rather to address the outstanding question concerning whether copying data counts as a seizure.[208] When the police copy a hard drive, they do not need to cart away the device and deprive the owner of his right to possess or access the information stored therein. Instead, they can make a bitstream copy[209] on the spot and leave with all the information they need to conduct a search offsite, often using sophisticated forensic software that is unavailable in the field.

Arizona v. Hicks is the physical-world case most cited for the proposition that a warrant is not required to copy data.[210] In *Hicks*, the Court held that copying the serial number from a stereo system believed to be stolen was not a seizure because it did not "meaningfully interfere" with the suspect's possessory interest in the serial numbers or the equipment.[211] The Court was right with respect to use of the stereo. It was not sitting in an evidence locker; Hicks was still free to use it. But there is a strong argument against extending this logic to cases where the possessory interest does not lie in the use of a tangible item, but in control over the information itself.[212]

Katz and its progeny support the position that the Fourth Amendment protects an individual's possessory interest in information itself, and not just the paper or disc on which it may be recorded.[213] Therefore, photographing or otherwise copying the contents of expressive materials or data interferes with this possessory interest, regardless of whether or not police seize the physical medium.[214] A contrary rule, as some courts have acknowledged, would "significantly degrade the right to privacy."[215] It would also contradict established rules of

---

207. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

208. *See generally*, Orin Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L. J. 700, 724 (2010) (arguing that copying data "seizes" it under the Fourth Amendment when copying occurs without human observation and interrupts the stream of possession or transmission).

209. A "bitstream copy" is a mirror-image copy of the entire hard disk of a computer. These copies are also sometimes referred to as "evidence grade" backups. *Bitstream Copy*, EDRM GLOSSARY (2015), http://www.edrm.net/resources/glossaries/glossary/b/bitstream-copy.

210. Arizona v. Hicks, 480 U.S. 321 (1987); *see also* Bills v. Aseltine, 958 F.2d 697, 707 (6th Cir. 1992) (holding that photographs taken during the execution of search warrant were not a seizure under the Fourth Amendment).

211. *Hicks*, 480 U.S. at 324.

212. *See* United States v. Jefferson, 571 F. Supp. 2d 696, 703–704 (E.D. Va. 2008); Kerr, *supra* note 210, at 706–709; Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39, 111 (2002); Randolph S. Sergent, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181, 1186 (1995).

213. *Jefferson*, 571 F. Supp. 2d at 702.

214. *Id.*

215. *Id.* at 703–04 (noting that if protection "does not extend to the information contained in books and documents," police would be free to enter a home pursuant to a lawful warrant and then evade the warrant's limitations by copying every scrap of paper in search for evidence of unrelated crimes); *In re* A Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@Gmail.Com

intellectual property law, which dictate that the act of copying data itself interferes with possessory rights in that property.[216]

Following this logic, copying data is also a seizure even if the government never actually looks at it. Consider, for example, the NSA's bulk collection of phone records under Section 215 of the PATRIOT Act.[217] In *ACLU v. Clapper*, the Justice Department argued that a group of plaintiffs had no standing to sue the NSA on the theory that they could not prove the government had actually "reviewed" the phone records copied from service providers.[218] But as the Second Circuit observed, the collection of phone records is properly understood in the first instance as a Fourth Amendment seizure, given that a "violation of the [Fourth] Amendment is fully accomplished at the time of an unreasonable governmental intrusion."[219] In other words, "collection matters."[220]

Although the Supreme Court has yet to weigh in on this question, it seems persuasive to analogize between computer files and written documents or telephone calls. The value of the data lies in the information it contains and the ability to exclude others from accessing it.[221] Consequently, copying a file

---

Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386, 392 (S.D.N.Y. 2014) (copying of electronic evidence equates to an "exercise of dominion essentially amount[ing] to a 'seizure' even if the seizure takes place at the premises searched and is only temporary"); United States v. Taylor, 764 F. Supp. 2d 230, 237 (D. Me. 2011) (obtaining copies of emails from internet service provider "for subsequent searching" is a seizure); United States v. Bowen, 689 F. Supp. 2d 675, 684 (S.D.N.Y. 2010) (copying of entire email account described as a seizure). *But see* United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026 at *3 (W.D. Wash. May 23, 2001) (holding that the act of copying data from computers was not a seizure because the data remained "intact and unaltered" and was still "accessible to Defendant and any co-conspirators"); *In re* U.S. for a Search Warrant for Contents of Elec. Mail & for an Order Directing a Provider of Elec. Commc'n Servs. to not Disclose the Existence of the Search Warrant, 655 F. Supp. 2d 1210, 1222 (D. Or. 2009) (suggesting that "the nature of electronic information" leaves no possibility for meaningful interference with possessory interests because email "can be accessed from multiple locations, by multiple people, simultaneously").

216. *See* Copyright Act, 17 U.S.C. § 106 (2013) ("[T]he owner of copyright under this title has the exclusive rights to do and to authorize any of the following: (1) to reproduce the copyrighted work in copies . . . ."); Hoehling v. Universal City Studios, 618 F.2d 972, 980 (2d Cir. 1980) ("A verbatim reproduction of another work . . . even in the realm of nonfiction, is actionable as copyright infringement."); SHL Imaging, Inc. v. Artisan House, Inc., 117 F. Supp. 2d 301, 318 (S.D.N.Y. 2000) (finding infringement for copying photographs "verbatim").

217. *See* USA PATRIOT ACT of 2001, Pub. L. No. 107–56, § 215.

218. ACLU v. Clapper, 785 F.3d 787, 800 (2d Cir. 2015).

219. *Id*. at 801 (quoting United States v. Verdugo-Urquidez, 494 U.S. 259, 264 (1990)) (internal quotation marks omitted).

220. Jennifer Daskal, *The Substance of the Second Circuit on 215: Four Key Takeaways*, JUST SECURITY (May 8, 2015), http://justsecurity.org/22875/substance-circuit-215-key-takeaways/; *see also* Faiza Patel, *How the Second Circuit's Decision in Clapper Informs the Section 215 Discussion*, JUST SECURITY (May 11, 2015), http://justsecurity.org/22944/clapper-section-215-discussion/ (observing that even though the court's decision dealt only with standing to sue the NSA, "the analysis of standing is intertwined with the merits question of whether there has been an invasion of a protected privacy interest," per Rakas v. Illinois, 439 U.S. 128, 139-40 (1978)).

221. As in copyright law, the essence of ownership is the right to exclude others. *See* eBay Inc. v. MercExchange L.L.C., 547 U.S. 388, 392 (2006) ("Like a patent owner, a copyright holder possesses 'the right to exclude others from using his property.'" (citing Fox Film Corp. v. Doyal, 286 U.S. 123, 127 (1932))). Copyright infringement occurs at the moment of duplication, regardless of the purpose.

should constitute a seizure under the Fourth Amendment.

C. Is a Warrant Required?

The "ultimate touchstone" of the Fourth Amendment is that a search and seizure must be reasonable.[222] And a search or seizure is only reasonable if the government first obtains a warrant, subject to "a few specifically established and well-delineated exceptions."[223] This basic framework has sustained multiple jurisprudential and scholarly attacks, but its role in protecting our privacy from arbitrary government intrusion is now more important than ever.[224] Consequently, I propose here a presumption in favor of a warrant requirement for access to data involving expressive and associational activities.

Exceptions to the warrant requirement are threatening to swallow the rule, especially in the digital world. The Supreme Court has candidly acknowledged that the police search suspects far more frequently without a warrant than with one.[225] Outside the realm of law enforcement, intelligence agencies sweep up the international communications of law-abiding Americans *en masse*.[226] At the border, immigration authorities are empowered to search travelers' laptops, cell phones, and iPads without any suspicion of wrongdoing.[227] Even routine law

---

See Rosner v. Codata, 917 F. Supp. 1009, 1018 (S.D.N.Y. 1996) ("When a defendant copies a plaintiff's work, the infringement occurs at the moment of copying . . . ."); *see also* Auscape Int'l v. Nat'l Geographic Soc'y, 409 F. Supp. 2d 235, 247 (S.D.N.Y. 2004) (finding that the injury occurs at the moment of infringement); Sergent, *supra* note 214, at 1186.

222. Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

223. Katz v. United States, 389 U.S. 347, 357 (1967); *see also* Coolidge v. New Hampshire, 403 U.S. 443, 454–55 (1971) (quoting *Katz*, 389 U.S. at 357).

224. Several Fourth Amendment scholars have questioned the historical accuracy of placing such great emphasis on the warrant clause. *See, e.g.*, Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547 (1999); Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757 (1994). For example, there is considerable debate about whether the Framers even approved of specific warrants in the first place. *See* Davies, *supra*, at 553–54; Amar, *supra*, at 773–74. And if they did, it is disputed whether the Framers anticipated the warrant to be the exclusive protection of our right to be secure in all instances of search and seizure. Davies, *supra*, at 738–39. However, as the foregoing discussion demonstrates, the "value of recovering the authentic history of search and seizure doctrine lies largely in the broader perspective it provides" – namely, the historic need to proscribe arbitrary invasions of our privacy by overzealous government officials. *Id.* at 748. Even assuming that colonial history does not support a warrant requirement, "the question remains whether circumstances have changed sufficiently" to support it. Carol S. Steiker, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820, 830 (1994). Professor Steiker persuasively argues that the rise of the modern police state and the consequent expansion of the government's investigative powers render judicial warrants a necessary safeguard against the kinds of abuses that preoccupied the Framers. *Id.* at 830–44. In other words, the warrant requirement has become a modern guarantee of sacred principles.

225. Riley v. California, 134 S. Ct. 2437, 2482 (2014).

226. *See generally* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (2014), *available at* https://www.pclob.gov/Library/215-Report_on_the_Telephone_Records_Program-2.pdf.

227. *See, e.g.*, Abidor v. Napolitano, 990 F. Supp. 2d 260, 277–79 (E.D.N.Y. 2013). *But see* United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013) (concluding forensic searches of electronic devices require reasonable suspicion of criminal activity).

enforcement investigations that begin with a warrant threaten to spiral into generalized searches of our digital data under an exception known as the "plain view" doctrine.[228]

This state of affairs has prompted criminal procedure scholar Thomas Davies to observe that Fourth Amendment doctrine has evolved away from "a sense of the individual's right to be secure from government intrusions and toward an ever-enlarging notion of government authority to intrude."[229] Part of the problem lies in how courts determine whether a warrantless intrusion is constitutionally reasonable. When the government invokes a well-established exception to the warrant requirement, like administrative searches or border security, courts default to a general inquiry of "reasonableness."[230] In other words, courts assess, "on the one hand, the degree to which [the warrantless search or seizure] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[231]

This balancing analysis is often not a fair fight. In a growing number of cases, courts have established a one-way ratchet in favor of the government – the more important the government interest, the reasoning goes, the "greater the intrusion that may be constitutionally tolerated."[232] For example, the Foreign Intelligence Surveillance Court has signed off on dragnet surveillance operations on the theory that the government should be given as wide latitude as possible to gather foreign intelligence.[233] In its estimation, the gravity of the national security interest dwarfs "the risk that government officials will not operate in good faith" in the absence of external safeguards.[234]

Such unstinting deference to the government's interests unmoors the criterion of reasonableness from the "central fact about the Fourth Amendment" – namely, that it was a safeguard against the recurrence of abuses of unfettered executive power "so deeply felt by the Colonies as to be one of the potent causes of the Revolution."[235] History teaches that our duty to remain faithful to this safeguard

228. *See, e.g.*, United States v. Williams, 592 F.3d 511, 524 (4th Cir. 2010) (finding seizure of child pornography during search for electronic evidence of online harassment lawful since all electronic files come into "plain view" during a computer search).

229. Davies, *supra* note 226, at 749.

230. *See, e.g.*, Camara v. Municipal Court, 387 U.S. 523, 536–37 (1967) ("Unfortunately, there can be no ready test for determining reasonableness other than by balancing the need to search against the invasion which the search entails."); United States v. Ramsey, 431 U.S. 606, 619 (1977) ("Border searches, then, from before the adoption of the Fourth Amendment, have been considered to be 'reasonable' by the single fact that the person or item in question had entered into our country from outside.").

231. Wyoming v. Houghton, 526 U.S. 295, 300 (1999); *see also* Riley v. California, 134 S. Ct. 2473, 2478 (2014).

232. *In re* Directives [redacted] Pursuant to Sec. 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008) (citing Michigan v. Summers, 452 U.S. 692, 701–05 (1981)).

233. *See id.* at 1006, 1012. The Supreme Court has not definitively ruled that there is a foreign intelligence exception to the warrant requirement. *See generally* ELIZABETH GOITEIN & FAIZA PATEL, BRENNAN CTR. FOR JUSTICE, THE PROBLEM WITH THE FISA COURT (2015).

234. *In re Directives [redacted]*, 551 F.3d at 1014.

235. United States v. Rabinowitz, 339 U.S. 56, 69 (1950) (Frankfurter, J., dissenting).

is *heightened* during moments of crisis. It is no coincidence that the Fourth Amendment was forged during deep unrest and "controversies involving not very nice people."[236] When the government perceives that its investigative duty is more urgent than usual, the temptation of overreach is also stronger, placing our privacy in "greater jeopardy."[237] Courts are duty-bound as the primary enforcers of the Fourth Amendment to stand guard against this "greater jeopardy."

Thus, courts should generally require a warrant for government access to Fourth Amendment "papers," including electronically stored data. If one of the established exceptions to the warrant requirement applies, courts should construe it narrowly and exercise great vigilance given the First Amendment interests at stake. One way to achieve this goal would be a judicial presumption in favor of a warrant, where the government claims an exception and the search or seizure involves expressive or associational data. Such a presumption would require courts to treat warrantless intrusions into our digital data with a healthy dose of skepticism right off the bat, no matter how "benevolent and benign" the government's motives or how "special" its needs.[238] It is also consistent with Supreme Court precedent requiring "scrupulous exactitude" when applying the Fourth Amendment to situations where significant First Amendment rights are at stake.[239] And most importantly, it will ensure that neither advances in technology nor lags in law will subvert the essential guarantees of free speech and association that fuel democratic government.

IV. ELECTRONIC COMMUNICATIONS & CLOUD DATA

With these principles in mind, I return to the third-party records doctrine and examine two basic types of digital data that exemplify Fourth Amendment "papers": electronic communications records and personal files stored in the cloud. Applying the test articulated in Section III, I conclude that both types of data, as well as their associated metadata, should be protected under the Fourth Amendment and thus require a warrant to search or seize.

A. Communications Data and Metadata

As the Supreme Court has recognized, the history and purpose of the Fourth Amendment reveal an original intent to guarantee the privacy of sealed letters.[240] By specifying that "papers" should receive Fourth Amendment protection, the Framers meant to protect written communications as much as a diary in

236. *Id.*

237. United States v. U.S. Dist. Court, 407 U.S. 297, 313 (1972).

238. *Id.* at 314.

239. Zurcher v. Stanford Daily, 436 U.S. 547, 564 (1978) (citations omitted) (internal quotation marks omitted).

240. United States v. Jacobsen, 466 U.S. 109, 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable."); *Ex parte* Jackson, 96 U.S. 727, 733 (1877).

a desk drawer.[241] The Court should ensure that the third-party doctrine does not erode this democratic guarantee. Email, for example, should enjoy at least as much constitutional protection as a letter in the mail. The same should also hold true for other kinds of electronic communications, such as text messages, private Facebook messages, and Snapchats.[242] These too are the equivalent of "papers" under the Fourth Amendment.

The Sixth Circuit endorsed this analogy in *United States v. Warshak*, reasoning that email "is the technological scion of tangible mail" and that it would "defy common sense to afford emails lesser Fourth Amendment protection."[243] The Court explicitly rejected the argument that a service provider's ability or right to access the content of email should somehow defeat the communicant's Fourth Amendment privacy interest.[244] Instead, *Warshak* likened service providers to "the functional equivalent of a post office or a telephone company," which the police may not simply storm to read a letter.[245]

Indeed, the content of communications, whether spoken, typed, or beamed over the Internet, are the kind of expressive and associational materials that the Framers intended to shield from arbitrary search and seizure through the Fourth Amendment. Communications content, whatever its form, should be treated as "papers" for Fourth Amendment purposes. It does not matter that some emails may have little obvious First Amendment value. An inbox may be littered with spam, porn, or hateful speech. On the other hand, it may belong to a political activist, replete with messages about strategy, talking points, and organizing. The fact of the matter is that there is no way to tell before looking, and it is critical to afford truly expressive and associational data the constitutional protection it is entitled.[246] Once the data has been searched or seized, the

241. *See* Entick v. Carrington, (1765) 19 How. St. Tr. 1029 (K.B.) 1065 ("Has a Secretary of State a right to see all a man's private letters of correspondence, family concerns, trade and business? This would be monstrous indeed! And if it were lawful, no man could endure to live in this country."); *cf.* Aldridge v. Tuscumbia, Courtland & Decatur R.R. Co., 2 Stew. & P. 199, 209 (Ala. 1832) (finding that the "sole design and object" of Section 9 of Alabama's 1819 Bill of Rights, which closely mirrored the Fourth Amendment, was "to protect the citizen, in person, and his private correspondence, from wanton and vexatious seizures and searches, made on slight and frivolous charges of criminal offences [*sic*]").

242. *See* Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 326 (2010) ("Substantial questions would arise if courts were to begin saying what means of speech should be preferred or disfavored. And in all events, those differentiations might soon prove to be irrelevant or outdated by technologies that are in rapid flux."). Snapchat is a social messaging service that allows users to send pictures that automatically delete ten seconds after being viewed by the recipient. *See* Snapchat Support, *Snaps*, SNAPCHAT, https://support.snapchat.com/ca/snaps.

243. United States v. Warshak, 631 F.3d 266, 285–86 (6th Cir. 2010). In *Warshak*, the Sixth Circuit relied on the Supreme Court's decision in *City of Ontario v. Quon*, and the Ninth Circuit's decision in *United States v. Forrester*. *See* City of Ontario v. Quon, 560 U.S. 746, 762 (2010) (implying that "a search of [an individual's] personal e-mail account" would be just as intrusive as "a wiretap on his home phone line"); United States v. Forrester, 512 F.3d 500, 511 (2008) ("The privacy interests in [mail and email] are identical.").

244. *Warshak*, 631 F.3d at 286-87.

245. *Id.* at 286.

246. *See* Marcus v. Search Warrants of Prop. at 104 East Tenth St., 367 U.S. 717, 731 (1961).

damage to privacy and the Fourth Amendment has been done. As a result, the Court should read the Fourth Amendment to categorically protect the content of electronic communications.

The more difficult question is whether the metadata associated with private electronic communications should be treated as "papers" as well. Unfortunately, analogies to tangible mail are not particularly helpful here. In *Ex parte Jackson*, the Supreme Court held that letters in the mail are "as fully guarded from examination and inspection, *except as to their outward form and weight*, as if they were retained by the parties forwarding them in their own domiciles."[247] Since that time, several circuit courts have found that the warrantless use of "mail covers" (inspecting and recording the outside of envelopes sent through the mail) does not violate the Fourth Amendment.[248] Notably, the Supreme Court has never weighed in on the constitutionality of this practice. Instead, the Court's later decisions in *Smith* and *Miller* have come to stand for the general proposition that communications metadata, regardless of its nature, is not protected by the Fourth Amendment.[249]

The text of the Fourth Amendment, however, makes no such distinction, and I submit that none is justified if the metadata is likely to reveal expressive or associational activities protected by the First Amendment.[250] The Framers

---

247. *Ex parte* Jackson 96 U.S. 727, 733 (1877) (emphasis added). It is important to note, however, that the *Jackson* Court did not consider the First Amendment implications of warrantless mail covers. Had it done so, it might have recognized the potential for a First Amendment violation, as some lower courts have done. *See* Paton v. LaPrade, 524 F.2d 862, 865, 870 (3d Cir. 1975) (finding that a warrantless mail cover to record names and addresses on sent letters may violate an individual's First Amendment rights); ACLU v. Nat'l Sec. Agency, 493 F.3d 644, 664 (6th Cir. 2007) (recognizing *Paton*, but holding that plaintiffs lacked standing); Patterson v. FBI, 705 F. Supp. 1033, 1045–46 (D.N.J. 1989) (recognizing *Paton*, but finding that that the government's responsibility for conducting foreign policy and national security affairs outweighed the First Amendment implications).

248. United States v. Huie, 593 F.2d 14 (5th Cir. 1979); United States v. Choate, 576 F.2d 165, 181–82 (9th Cir.), *cert. denied*, 439 U.S. 953 (1978); United States v. Costello, 255 F.2d 876, 881–82 (2d Cir.), *cert. denied*, 357 U.S. 937 (1958).

249. *See, e.g.*, ACLU v. Clapper, 959 F. Supp. 2d 724, 751 (S.D.N.Y. 2013) (discussing lack of individual privacy rights in telephone records); *In re* FBI for an Order Requiring Prod. of Tangible Things from [redacted], No. BR 13-109, 2013 WL 5741573 at *2 (FISA Ct. Aug. 29, 2013) (applying *Smith* to the collection of metadata because call detail records belonging to a telephone company are not protected by the Fourth Amendment); [redacted], No. PR/TT (FISA Ct. [redacted]) (Kollar-Kotelly, J.) (explaining legal rationale for initial bulk collection of telephonic metadata). *But see* Klayman v. Obama, 957 F. Supp. 2d 1, 31–32 (D.D.C. 2013) (distinguishing metadata collection from *Smith v. Maryland*, 442 U.S. 735 (1979), in the length of time, the formalization of the process, and the breadth of the collection).

250. Of course, even the "outward form and weight" of snail mail may reveal information about its content and import that has important expressive or associational value. Consider a postcard or political flyer, for example, which might be seen (and quickly forgotten) by a mail carrier. Until recently, it was not widely known that the U.S. Postal Service now photographs the outside of every piece of mail sent in America. Ron Nixon, *U.S. Postal Service Logging All Mail for Law Enforcement*, N.Y. TIMES (July 3, 2013), http://www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html; Lauren Walker, *Postal Service Photographs Every Piece of Mail in the U.S., Shares With Agencies That Request It*, NEWSWEEK (Oct. 28, 2014), http://www.newsweek.com/postal-service-photographs-every-piece-mail-us-shares-agencies-request-it-280614; *see also* OFFICE OF INSPECTOR GEN., U.S. POSTAL SERV., Report No. HR-AR-

would have recoiled at the thought of unfettered government access to a list of everyone who read a copy of John Wilkes' *North Briton*, No. 45. Yet the metadata generated by browsing the web, sending email, and downloading files from the Internet could easily produce such a list. Indeed, Internet service providers, including mobile phone carriers, log user activity on the Internet, such as the websites visited. A web address, or URL, may be analogous at some level to the address on a letter or the numbers dialed on a telephone, but it can also be far more revealing. Some URLs may simply point to a homepage or domain (e.g., www.brennancenter.org), but they are usually more specific, identifying individual articles, pictures, or videos that a user views online (e.g., https://www.brennancenter.org/analysis/rethinking-privacy . . .). Each click on a website leads to a unique URL with easily identifiable content. Likewise, every Google search directs the user to a unique web page, the URL for which contains the terms of the query itself (e.g., www.google.com/search?q=rethinking+privacy . . .).[251]

Visiting a website or conducting a Google search also generates metadata about the user, including information about the time and location of the activity, once again raising First Amendment concerns. Websites often place small packets of data, known as "cookies," on a user's computer that enable the sites to track online activity. These cookies provide a more complete profile of a user's preferences based on information about previous web browsing habits.[252] Indeed, computer forensic examiners often use them to confirm past Web activity and determine where and when a particular device accessed a particular website.[253] A user can takes steps to block or erase cookies,[254] but in order for a web browser to display websites correctly, it is still necessary to convey some basic information about the computer or smartphone to the website, like the size

---

14-001, POSTAL INSPECTION SERVICE MAIL COVERS PROGRAM AUDIT REPORT (May 28, 2014), https://www.uspsoig.gov/sites/default/files/document-library-files/2014/hr-ar-14-001.pdf. If digitally processed and analyzed, such a large cache of images could reveal a wealth of protected expressive and associational information. Should the Supreme Court have an opportunity to revisit its position in *Ex parte Jackson*, 96 U.S. 727, 733 (1877) with respect to so-called mail covers, it should take this practice and technology into account, which was surely unimaginable in 1877.

251. *See in re* U.S. for an Order Authorizing the Use of a Pen Register & Trap on [xxx] Internet Serv. Account/User Name [xxxxxxx@xxx.com], 396 F. Supp. 2d 45, 49 (D. Mass. 2005) ("A user may visit the Google site . . . . [I]f the user then enters a search phrase, that search phrase would appear in the URL after the first forward slash. This would reveal content . . . The substance and meaning of the communication is that the user is conducting a search for information on a particular topic." (internal quotation marks omitted)).

252. *How Companies Collect Your Private Information When You Browse Online*, REPUTATION.COM, http://www.reputation.com/reputationwatch/articles/how-companies-collect-manage-and-use-your-private-information-when-you-browse-online.

253. *See, e.g.*, Jon S. Nelson, *Google Analytics Cookies and the Forensic Implications*, DIGITAL FORENSIC INVESTIGATOR NEWS (Feb. 1, 2012), http://www.dfinews.com/articles/2012/02/google-analytics-cookies-and-forensic-implications; *Web Browser Cookie Forensics*, GIBSON RES. CORP., https://www.grc.com/cookies/forensics.htm?tnb0rvf5pho2c; *Forensic Computer Examinations*, CYBERLAB COMPUTER FORENSICS, LLC (June 27, 2005), http://www.ccforensic.com/pages/2cforensics.html.

254. *See, e.g.*, *How It Works*, GHOSTERY, https://www.ghostery.com/en/how-it-works.

of the screen and any browser plugins installed.[255] It turns out, however, that the precise combination of hardware and software running on a computer is often distinctive enough to make it individually identifiable from millions of others. The result is a kind of device fingerprint or "supercookie" that cannot be hidden or deleted.[256]

Supercookies are a long way away from inspecting the "outward form and weight" of postal mail. Even if courts are inclined to believe that the First Amendment implications of a mail cover are negligible,[257] there ought to be outright alarm at the First Amendment implications of Internet communications metadata. Web browsing records may be considered metadata, but they are at least as revealing as content, if not more so. There is no such thing as a brown paper envelope on the Internet. Thus, even if it were logical to distinguish between content and metadata, it would make little practical difference in the long run. Courts should instead analyze the First Amendment implications of the metadata itself, which in the case of online communications are hugely significant.

One objection to this line of reasoning is that metadata should not be treated as a person's "private papers," but instead as "business records" belonging to a third party. In fact, the *Miller* Court relied on this distinction to conclude that bank records are not "private papers" because individuals "assert neither ownership nor possession" of them."[258] But whatever analytic value this distinction once held, it has been eclipsed by the realities of modern technology. The question of ownership and possession for communications metadata is not nearly as obvious or clean-cut as the financial instruments at issue in *Miller*, and as a result, these factors no longer provide a workable constitutional rule.

First, the ownership of metadata may be difficult to determine. Consider email, for example. Some of the most revealing metadata, such as the "to/from" information or the IP address (location) of the sender, is not created by a third party, but by the author and the device responsible for sending the message. The service provider is not an author or intended recipient; it is performing a ministerial task when it collects this information. The service provider has no ownership or property interest in email metadata outside of the contractual agreement detailed in the company's terms of service. In order to perform that service, the company may be licensed to record some forms of metadata generated by its users, but it does not generally contribute original information or assert an independent claim of ownership.

---

255. Peter Eckersley, *How Unique Is Your Web Browser?*, ELEC. FRONTIER FOUND. 5 tbl. 1 (2009), https://panopticlick.eff.org/browser-uniqueness.pdf.

256. *Id.* at 3.

257. United States v. Choate, 576 F.2d 165, 176 (9th Cir. 1978).

258. United States v. Miller, 425 U.S. 435, 440 (1976); *see also* United States v. Davis, 785 F.3d 498, 511 (11th Cir. 2015) (en banc) ("For starters, like the bank customer in Miller and the phone customer in Smith, Davis can assert neither ownership nor possession of the third-party's business records he sought to suppress.").

Second, with respect to possession, third parties may retain a copy of some metadata in the course of transmitting it, but so do the sender and recipient. Although it is usually hidden from view, every email contains a "header" full of metadata that is stored alongside the message, and it is available to any user who knows where to look. Similar information may also be stored locally on a personal hard drive or mobile device. Moreover, users may retain some degree of control over their metadata, even in the hands of a third party.[259] In some circumstances, a user can even delete information and cause the company to purge it from its records, as when closing an account or permanently deleting an email.[260] Thus, the possession and ownership of metadata is not in any way exclusive to third parties. Instead, it will vary from one type of metadata to another, and depend in large part on a company's own policies.[261] There is no longer a clean analytical line to draw, if there ever was one at all.[262] In short, it

259. Some mainstream email providers like Gmail and Hotmail do not allow users to disable metadata collection, but some smaller start-ups are now enabling customers to prevent collection of metadata from email headers. For example, companies like ShazzleMail permit users to eliminate metadata collection by delivering messages directly to recipients without creating server copies. *See* Adam Tanner, *How to Send Email Without Leaving Any Metadata Traces*, FORBES (July 21, 2014), http://www.forbes.com/sites/adamtanner/2014/07/21/how-to-send-email-without-leaving-any-metadata-traces/. A similar service is being developed by the heads of secure communications system Silent Circle and Lavabit, best remembered as the email service used by Edward Snowden. Known as the Dark Mail Alliance, the technology will automatically deploy peer-to-peer encryption to both content and metadata of email messages and attachments, allowing users to communicate securely. *See* Ryan Gallagher, *Meet the "Dark Mail Alliance" Planning to Keep the NSA Out of Your Inbox*, SLATE (Oct. 30, 2013), http://www.slate.com/blogs/future_tense/2013/10/30/dark_mail_alliance_lavabit_silent_circle_team_up_to_create_surveillance.html. Tech companies like Google and Twitter also provide users with opt-out options for some metadata-gathering services. *See, e.g.*, *Opt out*, GOOGLE, https://support.google.com/ads/answer/2662922?hl=en (describing how to opt out of interest-based ads derived from metadata collection); *Know your Google security and privacy tools*, GOOGLE, https://www.google.com/goodtoknow/online-safety/security-tools/ (Advising users on how to browse websites without Google collecting data about their activity or sharing it with other parties.); *Twitter Supports Do Not Track*, TWITTER, https://support.twitter.com/articles/20169453-twitter-supports-do-not-track (describing Twitter's Do Not Track privacy preference, which allows users to enable a browser feature which prevents Twitter from providing tailored suggestions or ads to them); *How to Opt out of Add-On Metadata Updates,* MOZILLA FIREFOX, https://blog.mozilla.org/addons/how-to-opt-out-of-add-on-metadata-updates/ (describing process for users to opt-out of metadata tracking from Mozilla's Add-Ons Gallery).

260. *See Deleted Cloud Data: A Provider-by-Provider Survey,* ASS'N OF CERTIFIED E-DISCOVERY SPECIALISTS (June 2014), http://www.aceds.org/wp-content/uploads/2014/06/Download-Provider-by-Provider-Survey-of-Deleted-Cloud-Data.pdf.

261. Yahoo, for example, purports to purge from its servers any emails deleted from the trash folder. *See How Long Does Mail Remain in My Trash Folder Before It's Deleted?*, YAHOO!, http://help.yahoo.com/l/us/att/smallbusiness/bizmail/manage/manage-55.html. By contrast, Google allows Gmail users to "delete information from [their] services," but notes that it "may not immediately delete residual copies from [its] active servers and may not remove information from [its] backup systems." *Privacy Policy*, GOOGLE (Feb. 2015), https://static.googleusercontent.com/media/www.google.com/en/us/intl/en/policies/privacy/google_privacy_policy_en.pdf.

262. Even the *Smith* Court seemed to recognize the folly of this argument in the context of electronic communications. *Smith* relied on *Miller*, but the driving force in *Smith* was voluntariness, not property law or the "business records" doctrine. The Court specifically rejected the idea that privacy hinges on a phone company's individual billing practices, which would "make a crazy quilt of the Fourth Amendment." Smith v. Maryland, 442 U.S. 735, 745 (1979).

is misguided to attempt to distinguish "business records" metadata from the communications themselves. What should matter is whether the communicants have a significant First Amendment interest in the metadata generated by their communications.

Cell phone call records are perhaps the most obvious form of metadata laden with First Amendment interests. Even without access to the content of telephone calls, detailed logs showing calls placed and received can reveal a wealth of deeply personal expressive and associational activities. Consider, for example, the import of a single call to a substance abuse hotline, phone sex operator, or political campaign headquarters. Indeed, the record of that call may provide as much or more information than the actual conversation.[263] And as the amount of data grows, it only becomes more revealing.[264] Analyzed in the aggregate, call metadata can identify the membership, structure, and participants in an organization or political movement. It can identify the congregants at a particular church, mosque, or synagogue. And it can map political, professional, and journalistic networks by creating "social graphs" that include donors, political supporters, and confidential sources.[265] Such information is "a far cry" from the day-long pen register the Court found permissible in *Smith*.[266] Given the significant First Amendment interests at stake, such call logs should be considered one's private "papers" under the Fourth Amendment.

This approach is also consistent with the way a growing number of courts have treated the privacy of cell phone location metadata.[267] In addition to the

---

263. *See* Declaration of Professor Edward W. Felten at 14-16, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 13-CV-3994).

264. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 36 ("Records that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic – a vibrant and constantly updating picture of the person's life," including "'familial, professional, religious, and sexual associations.'" (quoting United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring))); ACLU v. Clapper, 785 F.3d 787, 823 (2d Cir. 2015) ("Metadata today, as applied to individual telephone subscribers, particularly with relation to mobile phone services and when collected on an ongoing basis with respect to all of an individual's calls (and not merely, as in traditional criminal investigations, for a limited period connected to the investigation of a particular crime), permit something akin to the 24–hour surveillance that worried some of the Court in *Jones*."). *But see* Smith v. Obama, 24 F. Supp. 3d 1005, 1007-09 (finding *Jones* inapplicable and relying instead on the third-party doctrine); United States v. Moalin, No. 10-cr-4246 JM, 2013 WL 6079518, at *7 (S.D. Cal. Nov. 18, 2013).

265. Declaration of Professor Edward W. Felten at 17, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 13-CV-3994).

266. *Klayman*, 957 F. Supp. 2d at 31.

267. *See*, *e.g.*, United States v. Cooper, No. 13-cr-00693-SI-1, 2015 WL 881578, at *6-7 (N.D. Cal. Mar. 2, 2015) (likening cell site location data to GPS monitoring, which "'generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations'" (quoting *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring))); *In re* U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 125 (E.D.N.Y. 2011) (finding that "there is no meaningful Fourth Amendment distinction between content and other forms of information, the disclosure of which to the Government would be equally intrusive and reveal information society values as private" and concluding that an exception to the third-party doctrine applies to cell-site-location records); Tracey v. State, 152 So. 3d

metadata created by electronic communications generally, the use of mobile devices for that activity generates a constant stream of location data through wireless pings to nearby cellular towers and GPS signals.[268]

This type of location information has the capacity to generate a detailed record of First Amendment activities, raising many of the same privacy concerns that motivated the Supreme Court in *United States v. Jones*.[269] *Jones* held that a Fourth Amendment search occurred when the police attached a GPS tracker to a car and monitored it for 28 days.[270] The opinion of the Court focused on the physical trespass involved in affixing the GPS device to a private vehicle, but five Justices also concluded that the location tracking itself violated the defendant's reasonable expectations of privacy.[271] For Justice Alito, it was critical that such cost-efficient, comprehensive, and covert surveillance had no late 18th-century analog.[272] Justice Sotomayor pointed to the "wealth of detail" about "familial, political, professional, religious, and sexual associations" created by GPS monitoring.[273]

It was not lost on the *Jones* Court that similar information could be obtained through access to cell phone location records,[274] but the majority chose not to

---

504, 522 (Fla. 2014) (finding an expectation of privacy in real-time cell-site information notwithstanding the fact the records are disclosed to the phone company or "to a business or other entity for personal purposes"); Commonwealth v. Augustine, 4 N.E. 3d 846, 863 (Mass. 2014) (finding that even though historical cell-site information is "business information" privacy interests require police to obtain a search warrant to obtain them); State v. Earls, 70 A.3d 630, 632 (N.J. 2013) (recognizing an expectation of privacy in historical cell-site information because "cell phones can now trace our daily movements and disclose not only where individuals are located at a point in time but also which shops, doctors, religious services, and political events they go to, and with whom they choose to associate"); *see also* United States v. Powell, 943 F. Supp. 2d 759, 776 (E.D. Mich. 2013) (finding an expectation of privacy in real-time, cell-site tracking records "not just because of the potential for tracking into protected areas, because the information obtained through such means is, in the aggregate, so comprehensive").

268. *See In re* U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d at 115 (describing cell phone location technology); *Augustine*, 4 N.E. 3d at 853; *Earls*, 70 A.3d at 636-38. *See generally*, *The Electronic Communications Privacy Act (ECPA), Part 2: Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec. & Investigations of the H. Comm. on the Judiciary*, 113th Cong. 6 (2013) (statement of Matt Blaze, Associate Professor, University of Pennsylvania), http://fas.org/irp/congress/2013_hr/ecpa2.pdf. Modern smartphones produce even more types of metadata, stemming from features like voicemail, instant messaging, and full-blown Internet access. *See* Riley v. California, 134 S. Ct. 2473, 2490 (2014). Every software application, or "app," installed a smartphone also produces metadata, which can include current and historic location information, user contacts, age, gender, and a unique device identification number. Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You*, WALL ST. J. (Dec. 17, 2010), http://www.wsj.com/articles/SB10001424052748704368004576027751867039730.

269. United States v. Jones, 132 S. Ct. 945 (2012).

270. *Id.* at 949.

271. *Id.* at 958, 964 (Alito, J., joined by Ginsburg, Breyer, and Kagan, JJ., concurring); *id.* at 955 (Sotomayor, J. concurring).

272. *Id.* at 958 (Alito, J., concurring).

273. *Id.* at 955 (Sotomayor, J., concurring) (citing People v. Weaver, 909 N.E.2d 1195, 1999 (N.Y. 2009)); *see also* David J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 143–151 (discussing the First Amendment implications of surveillance).

274. *Jones*, 132 S. Ct. at 963 (Alito, J. concurring) ("Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users – and as of June

address that issue and ruled on trespass grounds alone.[275] As a result, the Court left open the door to some predictably incongruous lower court opinions on the privacy of mobile phone metadata. Some courts have found no right to privacy in such location information, including the Fifth and Eleventh Circuits.[276] In *United States v. Davis*, for example, the Eleventh Circuit dismissed the significance of the *Jones* concurrences and found the lack of a physical trespass to be determinative.[277] The court opted to double down on the third-party doctrine,[278] mistaking ownership as a prerequisite for privacy.[279]

By contrast, other courts – including the highest courts of three states – have found a right to privacy in cell phone location information and rejected a rote application of the third-party doctrine.[280] These opinions focus on the same kind of First Amendment activities that moved Justice Sotomayor in *Jones*.[281] In *Tracey v. State*, for example, the Florida Supreme Court shared the concern that location tracking can reveal protected expressive and associational activities such as trips to "the psychiatrist, the plastic surgeon, the abortion clinic, the

---

2011, it has been reported, there were more than 322 million wireless devices in use in the United States.").

275. *Id.* at 954 ("It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.").

276. *See, e.g.,* United States v. Davis, 785 F.3d 498, 518 (11th Cir. 2015) (en banc); *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 608-09 (5th Cir. 2013).

277. *Davis*, 785 F.3d at 514 ("Jones is wholly inapplicable to this case.").

278. *Id.* at 512 ("The longstanding third-party doctrine plainly controls the disposition of this case.").

279. *See* Elizabeth Goitein, *United States v. Davis – Wrestling With the Third Party Doctrine*, JUST SECURITY (May 13, 2015), http://justsecurity.org/22989/united-states-v-davis-wrestling-party-doctrine/ ("The government may not freely search a rented apartment or tap a telephone wire the caller does not own. Judge Hull's characterization of the cell site data as company-generated information that merely 'concerns' Davis misses the mark. The information contained in the phone records is entirely a byproduct of Davis's communications. Davis generated the information; the phone company merely recorded it.").

280. United States v. Cooper, No. 13-cr-00693-SI-1, 2015 WL 881578, at *7-8 (N.D. Cal. Mar. 2, 2015); *In re* U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 122-26 (E.D.N.Y. 2011); Tracey v. State, 152 So. 3d 504, 522-23 (Fla. 2014); Commonwealth v. Augustine, 4 N.E. 3d 846, 863 (Mass. 2014); State v. Earls, 70 A.3d 630, 641-42.

281. *See Cooper*, 2015 WL 881578, at *7-8 (citing United States v. Jones, 132 S. Ct. 945 (2012) and Riley v. California, 134 S. Ct. 2473 (2014); *In re U.S.* for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d at 118 ("Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts." (citing United States v. Maynard, 615 F.3d 544, 561-62 (D.C. Cir. 2010), *aff'd on other grounds sub nom.* United States v. Jones, 132 S. Ct. 945 (2012))); *Tracey*, 152 So. 3d at 524-25 (citing *Jones*, 132 S. Ct. 945 (2012)); *Augustine*, 4 N.E.3d at 861 (citing *Jones*, 132 S. Ct. 945 (2012), and Commonwealth v. Rousseau, 990 N.E.2d 543, 553 (Mass. 2013); *Earls*, 70 A.3d at 640-41 (citing *Jones*, 132 S. Ct. 945 (2012)).

AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue, or church, the gay bar and on and on."[282] Likewise, the Massachusetts Supreme Judicial Court found in *Commonwealth v. Augustine* that cell phone location information "implicates the same nature of privacy concerns as a GPS tracking device,"[283] a form of surveillance which the court previously determined "'chills associational and expressive freedom' and allows the government 'to assemble data that reveal private aspects of identity,' potentially 'alter[ing] the relationship between citizen and government in a way that is inimical to democratic society.'"[284] The New Jersey Supreme Court has long rejected the third-party doctrine and declined to apply it in this context, also citing Justice Sotomayor's concurrence in *Jones* in its most recent case on point, *State v. Earls*.[285]

These decisions find further support in the Supreme Court's 2014 opinion on cell phone privacy, *Riley v. California*.[286] In *Riley*, the Court required police to obtain a warrant to search a cell phone incident to arrest, citing the volume and sensitivity of the data it contains.[287] The Court specifically pointed to "[h]istoric location information," which is "a standard feature on many smart phones and can reconstruct someone's movements down to the minute" and is capable of revealing detailed information about protected First Amendment activities.[288]

Indeed, the same First Amendment interests are at stake whether the data is generated directly by a GPS device placed under the bumper or pulled from cell towers.[289] If a warrant would be required to obtain the information directly, as

---

282. *Tracey*, 152 So. 3d at 519 (citing *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) (quoting People v. Weaver, 909 N.E.2d 1195, 1999 (N.Y. 2009)).

283. *Augustine*, 4 N.E.3d at 861.

284. *Rousseau*, 990 N.E.2d at 552.

285. *Earls*, 70 A.3d at 641.

286. *Riley*, 134 S. Ct. 2473.

287. *Id.* at 2489-90, 2493.

288. *Id.* at 2490 (citing United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring)).

289. Cell phone location metadata can burden First Amendment expressive and associational interests in at least three ways. *See* Andrew Crocker, *Trackers That Make Phone Calls: Considering First Amendment Protection for Location Data*, 26 HARV. J.L. & TECH. 619, 641 (2013). First, it can be used to identify anonymous speakers, which, as Daniel Solove observes, would infringe on the right to anonymous speech recognized by the Supreme Court in *Talley v. California*. *See* David J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 145 (citing Talley v. California, 362 U.S. 60 (1960)). A search of historical cell-site information, for example, could enable law enforcement to match a mobile device with the cell phone tower used to send a message. Second, location metadata can be used to burden associational freedom by identifying individuals present at an event such as a protest, lecture, or political meeting. The Supreme Court has held that such "expressive" association is protected by the First Amendment. *See* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958). Third, location metadata can be used to determine *all* of one's associations, including the strength of those relationships by correlating location data from different individuals. Such data can reveal whose phones were side-by-side on the train, at the office, or in the middle of the night, allowing algorithms to identify colleagues, couples, and confidants – even otherwise obscure associates – by tracking which movements intersect. *See* Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, WASH. POST (Dec. 4, 2013), http://www.washingtonpost.com/

the Supreme Court found in *Jones*, then the same standard should apply to similar third-party records. Otherwise, courts risk creating an end run around the Fourth Amendment.

In short, warrantless access to electronic communications data and metadata poses an existential threat to First Amendment values that was not present in 1877 when the Court decided *Ex parte Jackson*. Today, communications metadata has such significant First Amendment implications that it should be treated like "papers" under the Fourth Amendment.

Assuming that the Fourth Amendment generally protects communications content and metadata, the remaining issues are (1) determining when a search or seizure occurs and (2) whether a probable cause warrant should be required.

Determining when a Fourth Amendment search and seizure has occurred is more complicated than it seems. After all, some "papers" may be truly public information, in which case searching or seizing them would not be a Fourth Amendment event. To wit, in *Ex parte Jackson*, Justice Field distinguished between sealed letters and newspaper circulars, "between what is intended to be kept free from inspection, such as letters, and sealed packages subject to letter postage; and what is open to inspection, such as newspapers, magazines, pamphlets, and other printed matter, purposely left in a condition to be examined."[290]

But in the digital world, life is not so binary.[291] The text of a tweet, for example, is generally public and intended to be shared as widely as possible.[292] At the same time, users retain the option of sending "protected tweets," which require approving "each and every person" who may view the content.[293] Likewise, content posted on Facebook can be completely private, completely public, or somewhere in between. Facebook users have a range of options: they can block everyone else from accessing specific information, they can share a message with a friend or an entire group of friends, and they can also make certain content completely public and open to anyone who cares to go looking.[294]

Following the Fourth Amendment framework outlined in this article, a search would occur when accessing content that is not available to the general public

---

world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.

290. *Ex parte* Jackson, 96 U.S. 727, 733 (1877).

291. The Eighth Circuit was prescient in cautioning that *Ex parte Jackson* should not be "viewed as indicating or implying any such legal absoluteness." Oliver v. United States, 239 F.2d 818, 821 (8th Cir. 1957) ("[T]o read *Jackson* [in that fashion] would require the assumption that the Court had considered [*sic*] engaged in a survey and contemplation of all the possible forms of mail which might then or at any future time exist, under legislative or administrative authority, and was presuming to speak upon the question in relation to such a total horizon.").

292. *See Library of Congress Is Archiving All of America's Tweets*, BUSINESS INSIDER (Jan. 22, 2013), http://www.businessinsider.com/library-of-congress-is-archiving-all-of-americas-tweets-2013-1.

293. *About Public and Protected Tweets,* TWITTER, https://support.twitter.com/articles/14016-about-public-and-protected-tweets.

294. Facebook Help Center, *What audiences can I choose from when I share?*, FACEBOOK, https://www.facebook.com/help/211513702214269.

and without the active consent of the user. This is an objective inquiry, but one that nonetheless accounts for an individual's personal decisions about privacy. Thus, it would be a search to access protected tweets, Facebook content that is not marked public, and email of any kind (unless law enforcement was a recipient).

Unlike the text of a public tweet or Facebook post, however, not all of the metadata associated with it will be accessible to the public. Some information, such as the number of "retweets" on Twitter or the number of "likes" on Facebook may be as public as the message itself. Likewise, users may opt to publicize their location information, as when using Foursquare, Grindr, or Tinder.[295] But in most cases, communications metadata will not be publicly available. The phone company may know where a subscriber makes a call or visits a website, but the metadata generated by that activity is not publicly available. The key is to make an objective assessment of what data users have actually exposed to public scrutiny and not simply presume they have "assumed the risk" that all third-party records will be public information available to the police.

Consider metadata produced by cell phone communications. Cell phone users do not publicize their location information by revealing it to service providers.[296] They do not even "voluntarily" share it with the providers in any meaningful way.[297] It is just the way cell phones work, not consent to scrutiny.[298] As the Supreme Court of New Jersey reminds us, people buy cell phones to call friends, send text messages, and use the Internet, "[b]ut no one buys a cell phone to share detailed information about their whereabouts with the police." Similarly, the identity of the people with whom one communicates is generally private, not public data. It is only because of a legal artifact – the third-party doctrine – that there is any confusion about this reality. Moreover, it is unreasonable to counsel against using cell phones if individuals wish to retain their privacy, as some courts have done.[299] This presents an unacceptable

295. Foursquare is a location-based social network service that provides personalized recommendations of places to go and things to do based on information provided by the user. *See* Foursquare, *About Us*, FOURSQUARE, https://foursquare.com/about. Tinder is a location-based social networking application that allows mutually interested users to connect and communicate. *See* iTunes Preview, *Tinder Description*, ITUNES, https://itunes.apple.com/us/app/tinder/id547702041?mt=8. Grindr is an all-male social networking platform that connects users based on proximity. *See* Grindr, *Learn More*, GRINDR, http://grindr.com/learn-more.

296. *See Earls*, 70 A.3d at 641 ("When people make disclosures to phone companies and other providers to user their services, they are not promoting the release of personal information to others.").

297. *In re* U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 317 (3d Cir. 2010).

298. *In re* U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 127 (E.D.N.Y. 2011) ("The fiction that the vast majority of the American population consents to warrantless government access to the records of a significant share of their movements by "choosing" to carry a cell phone must be rejected.").

299. *See, e.g.,* United States v. Davis, 785 F.3d 498, 520 (11th Cir. 2015) (en banc) (Pryor, J., concurring) ("If a cell phone user does not want to reveal his location to a cellular carrier, he also has

dilemma in an age when cell phones are "ubiquitous, and for many, an indispensible [sic] gizmo to navigate the social, economic, cultural, and professional realms of modern society."[300] Indeed the United States Supreme Court has repeatedly recognized that these communications devices are not only pervasive, but also essential to the exercise of First Amendment activity.[301]

Finally, a lawful search or seizure of communications data should require a probable cause warrant, "as is required when papers are subjected to search in one's own household."[302] Indeed, the warrant requirement is paramount when searches and seizures of expressive material are concerned. Any other approach risks sanctioning the sort of general warrant that the Framers sought to forbid.[303] Thus, as the Supreme Court found in *Roaden v. Kentucky*, a hub of First Amendment activity such as "the bookstore or the commercial theater, each presumptively under the protection of the First Amendment, invokes such Fourth Amendment warrant requirements because we examine what is 'unreasonable' in light of the values of freedom of expression."[304] The Court should recognize that the Internet has assumed this role in modern society; it is the global hub of First Amendment activity, the greatest bookstore, theater, and forum for debate that the world has ever known. The Court should not penalize information privacy because of advances in technology, but instead should extend First and Fourth Amendment guarantees into cyberspace.

B. Papers in the Cloud

In June 2014, the *New York Times* ran a feature proclaiming "The Era of the Cloud" to describe a fundamental shift in how people and companies store and

---

another option: turn off the phone."). *But see* Tracey v. State, 152 So. 3d 504, 523 (Fla. 2014) ("Requiring a cell phone user to turn off the cell phone just to assure privacy from governmental intrusion that can reveal a detailed and intimate picture of the user's life places an unreasonable burden on the user to forego necessary use of his cell phone, a device now considered essential by much of the populace.").

300. United States v. Cooper, No. 13-cr-00693-SI-1, 2015 WL 881578, at *8 (N.D. Cal. Mar. 2, 2015).

301. City of Ontario v. Quon, 560 U.S. 746, 760 (2010) ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification."); Riley v. California, 134 S. Ct. 2437, 2484 (2014) ("[M]odern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.").

302. *Ex parte* Jackson, 96 U.S. 727, 733 (1877); United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) ("It only stands to reason that, if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception.").

303. *See* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (per curiam) (observing that "broad authorization to examine electronic records . . . creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant"); *accord* United States v. Galpin, 720 F.3d 436, 447 (2d Cir. 2013).

304. Roaden v. Kentucky, 413 U.S. 496, 504 (1973).

access digital information.[305] Rather than keeping and processing large amounts of data in-house, which is costly and inefficient, engineers have developed a way to distribute that job efficiently among a global network of millions of computers, pooling and renting huge amounts of computing power for collective use.[306] "You already work in the cloud, too," the *Times* explained, "if you use a smartphone, tablet, or web browser. And you're using the cloud if you're tapping online services like Dropbox or Apple's iCloud or watching *House of Cards* on Netflix."[307]

Consider Dropbox, for example, a service that enables people to store documents on remote servers they do not own but can access securely. Users may keep their files entirely private or choose to selectively share them with friends and colleagues. Dropbox operates on a common "freemium" business model, permitting users to get the basic service for free and pay for more space or greater access.[308] In the physical world, it is roughly analogous to renting space in a warehouse to store boxes of files, but with the benefit of instantaneous and remote access to any page on demand for any authorized user.[309] Similar services, such as Google Drive, are known for enabling multiple authorized users to edit the same file at the same time from different computers, thus eliminating many obstacles to collaborative work.

Under an unchecked interpretation of the third-party doctrine, users of Dropbox and Google Docs would not have a reasonable expectation of privacy in any of the files they upload, regardless of whether other people have permission to access or edit them. By virtue of "sharing" files with the company, they would have forfeited any expectation of the privacy of that information. Thus, if they wish their data to remain private and free from unreasonable search and seizure, they should not store it in the cloud, or so the logic goes.

This scenario, however, is quite a long way from the facts in *Smith* and *Miller* and presents a far greater threat to First Amendment freedoms than the Supreme Court imagined in the 1970s. The Court clearly did not see the cloud on the horizon, much less anticipate that it would become the modern replacement for desktops and warehouses. Indeed, for most of American history, the sanctity of the home has been a reliable proxy for protecting the privacy of personal papers. Private records could be locked in file cabinets and desk drawers. Love letters could be kept inside a hatbox in the closet or stashed inside a shoebox under the bed. Because the Supreme Court has closely guarded the privacy of

---

305. Quentin Hardy, *The Era of the Cloud*, N.Y. TIMES (June 12, 2004), http://bits.blogs.nytimes.com/2014/06/11/the-era-of-cloud-computing/.

306. *Id.*

307. *Id.*

308. Uzi Shmilovici, *The Complete Guide to Freemium Business Models*, TECHCRUNCH.COM (Sept. 4, 2011), http://techcrunch.com/2011/09/04/complete-guide-freemium/.

309. *See* United States v. Cotterman, 709 F.3d 952, 965 (9th Cir.) (en banc) ("With the ubiquity of cloud computing, the government's reach into private data becomes even more problematic. In the 'cloud,' a user's data, including the same kind of highly sensitive data one would have in "papers" at home, is held on remote servers rather than on the device itself.").

the home and other "constitutionally protected areas," one could be confident that such papers would not be subject to warrantless searches or seizures.[310]

It took the rise of the Pony Express, founded in 1860, for the Court to establish a Fourth Amendment privacy right in "papers" that are not physically inside the home. *Ex parte Jackson* held that "[t]he constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be," such as "in the mail."[311]

We are now in the midst of an information migration, away from the home or office and into the cloud. Personal letters, business files, photo albums, and music collections are flocking to secure corporate data servers outside of the home. But it is critical to recognize that people are not actually "sharing" these private files with companies like Dropbox or Google in any meaningful sense of the word. The users retain control of the information: They may dictate who has access to it and who does not, and they may delete it or move it elsewhere as they please. Cloud service providers do not claim ownership of the information or assert any rights to it, except as authorized by the user.[312]

The metadata associated with cloud computing is similar to the metadata associated with electronic communications generally. It contains information about who uploaded a file, who accessed it, from where, and when. It is also likely to contain data about the author or authors of collaborative works, as well as detailed logs of who contributed what and when. Such data touches at the heart of First Amendment expressive and associational activity. After all, the Wilkes affair began with the Crown's search for the author of *North Briton*, No. 45. If the same information were stored locally – on a local hard drive or in a desk drawer – there would be little debate as to whether it would rise to the level of Fourth Amendment "papers." The fact that it resides online should not change the result.[313]

As with electronic communications, not every file or bit of metadata will have significant First Amendment expressive and associational value. Some data may be unprotected speech, such as obscenity or child pornography. On the other end of the spectrum, some data may be quintessential First Amendment speech or associational activity involving the exercise of political or religious

310. "Constitutionally protected areas" include locations beyond the walls of a private home, including garages, boarding houses, rented houses, hotel rooms, park cabins, factories, private offices, and mobile homes. *See supra* notes 90–97 and accompanying text.

311. *Ex parte* Jackson, 96 U.S. 727, 733 (1877).

312. *See, e.g.*, *Dropbox Terms of Service*, DROPBOX (Jan. 22, 2015), https://www.dropbox.com/terms ("When you use our Services, you provide us with things like your files, content, email messages, contacts and so on ('Your Stuff'). Your Stuff is yours. These Terms don't give us any rights to Your Stuff except for the limited rights that enable us to offer the Services.").

313. *See* Riley v. California, 134 S. Ct. 2473, 2491 (2014) ("Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference . . . . Moreover, the same type of data may be stored locally on the device for one user and in the cloud for another.").

beliefs.[314] Libraries of photos, videos, and music may be a form of self-expression or they may be full of illegally downloaded media. The problem is that there is no way to tell the virtuous from the vile without first conducting a search.[315] As a result, courts should address the privacy of cloud data as a category, independent of whether a particular file or piece of metadata has First Amendment value. The imperative to protect truly expressive and associational data counsels in favor of Fourth Amendment protection for these electronic "papers" in the cloud.

Were the Court to treat personal cloud data and metadata like private papers, it would be relatively straightforward to determine when a search or seizure occurs. If the user has not made the information public, then accessing it without his or her consent is a search. Likewise, copying, altering, or removing it would be a seizure.

Determining whether information is or is not public would usually involve little more than looking at the user's access settings ("private," "friends only," "public," etc.), which the user controls. A service provider with no independent right to the information could not consent to a search or seizure, just as a landlord could not give consent to police to enter a tenant's home and search it.[316] By contrast, the use of "peer-to-peer" file sharing software like LimeWire or BitTorrent is designed to make files on a personal computer available for download by the general public, which includes the police.[317] The decision to freely share such information means that accessing or downloading it would not be a search or seizure, even if there were some subjective expectation that the files remain private.[318]

If the Fourth Amendment is to remain relevant in the digital world, then the Supreme Court must begin to treat cloud data more like "papers" in the home. It must not penalize privacy for advances in technology, but work to catch up and protect this First Amendment space through the Fourth Amendment.

C. Potential Limitations

It is important to recognize that this approach has some potential limitations, depending on how broadly the Supreme Court draws the First Amendment. By focusing on expressive and associational activity, some kinds of data will inevitably fall outside the scope of Fourth Amendment "papers."[319] That data

---

314. *See* Roberts v. United States Jaycees, 468 U.S. 609, 617–618 (1984).

315. Marcus v. Search Warrants of Prop. at 104 E. Tenth St., 367 U.S. 717, 731 (1961).

316. Chapman v. United States, 365 U.S. 610, 616–17 (1961) (allowing a landlord to consent to a search and seizure on behalf of a tenant would "reduce the Fourth Amendment to nullity and leave tenants' homes secure only in the discretion of landlords") (internal quotation marks, alterations, and citation omitted); *see also* Stoner v. California, 376 U.S. 483, 490 (1964) (holding that a hotel employee cannot give consent to search a room while a guest is occupying it).

317. United States v. Conner, 521 F. App'x 493, 497 (6th Cir. 2013).

318. United States v. Borowy, 595 F.3d 1045, 1048 (9th Cir. 2010).

319. *See* Solove, *supra* note 161, at 1123–24 ("The Fourth Amendment does not categorically prohibit the government from compelling certain disclosures by individuals or institutions. If it did,

may include medical or financial records, which as a general category do not have obvious significant First Amendment value. This is not to imply, however, that such records are not highly private or that they should not enjoy constitutional protection. To the extent this information may be contained on an individual's hard drive or cell phone, on a personal cloud server, or memorialized in electronic communications, it would be protected under the theory described in this article.

Consider, for example, the privacy of medical records generated and maintained solely by health care providers. It is difficult to find a significant First Amendment expressive or associational interest in such data even though many people would consider it highly private information. However, should those medical records be emailed to patients or stored among their other private "papers" on a cloud server, the analysis proposed in this article would apply. Thus, an email between doctor and patient would be protected in the same way as any other email. X-rays, test results, or fitness logs stored by the patient would also receive Fourth Amendment protection.

Moreover, it is important to recognize that third-party medical records may well be protected under a Fourteenth Amendment theory of information privacy. The Supreme Court opened this door in *Whalen v. Roe*[320] and *Ferguson v. City of Charleston*.[321] In *Ferguson*, the Court found a reasonable expectation of privacy in the results of diagnostic tests performed at a hospital, despite the fact that a range of medical personnel may have access to them.[322] Most recently, a district court in Oregon applied *Whalen* and *Ferguson* to invalidate the government's warrantless seizure of prescription drug records.[323] The court reasoned that the scope of Fourth Amendment protections for medical records should be informed by the Fourteenth Amendment right to information privacy recognized in *Whalen*.[324] I believe this is a sound practice for future courts to follow.

Like medical records, financial records are not traditionally associated with the exercise of First Amendment speech and associational freedoms. Although some transactions will undoubtedly reveal political or ideological associations, financial records do not fit neatly into this test – with two potentially significant exceptions. First, to the extent that information is the subject of online communications or personal data stored in the cloud, it should receive the same Fourth Amendment protections afforded to cloud and communications data generally. Thus, the third-party records generated by shopping on Amazon.com, for

---

then a significant amount of corporate regulation and the tax system would be nearly impossible to carry out. But the fact that the government can compel certain disclosures does not mean that it can compel people to disclose the details of their sexual lives or require them to send in their diaries and personal papers along with their tax forms.").

320. Whalen v. Roe, 429 U.S. 589, 599–600 (1977) (recognizing a Fourteenth Amendment right to information privacy for patients receiving medical care).

321. Ferguson v. City of Charleston, 532 U.S. 67, 79 n.14.

322. *Id.* at 78.

323. Or. Prescription Drug Monitoring Program v. DEA, 998 F. Supp.2d 957, 964-65 (D. Or. 2014).

324. *Id.*

example, would be protected communications data just like other Web browsing activity. Second, even though the *Miller* Court found no reasonable expectation of privacy in bank records, it was also careful to describe deposit slips and personal checks as "negotiable instruments to be used in commercial transactions," distinguishing them from "confidential communications."[325] It is not obvious that this distinction is still valid,[326] and if the Court continues to equate spending money with speech, then the rationale in *Miller* loses much of its force.[327]

CONCLUSION

The Supreme Court took a wrong turn when it created the third-party doctrine in *Smith* and *Miller*, but the magnitude of that mistake is just now coming into view. The Court must therefore make a choice. It can either reinforce the doctrine to the detriment of First Amendment values, or it can right the course. The analytical framework proposed in this article provides one possible solution that is guided by the history and purpose of the Fourth Amendment. At a minimum, however, the Court should recognize that the third-party doctrine has no place in the digital world and should limit or overrule *Smith* and *Miller*.

325. United States v. Miller, 425 U.S. 435, 442 (1976).

326. The information contained in bank records today carries tremendous First Amendment implications that did not exist in 1976. The Internet, after all, does not accept cash. Credit card purchases are ubiquitous, even for small items, and often generate multiple types of metadata, including location information. The data can easily paint a portrait of daily life in addition to providing data about individual purchases, investments, or political donations. Mobile payment platforms generate even more sensitive metadata. *See Mobile BIS Introduces Next Generation of Bill Paying Technology*, BIS COMPUTER SOLUTIONS (Sept. 23, 2009), http://www.biscomputer.com/press/mobile-bis-introduces-next-generation-of-bill-paying-technology.

327. The Court's recent decisions in *Citizens United* and *McCutcheon* clearly equate spending money with First Amendment–protected speech. Citizens United v. Fed. Election Commc'n, 558 U.S. 310, 339–340 (2010) (citing Buckley v. Valeo, 421 U.S. 1, 19 (1976) (per curium)); McCutcheon v. Fed. Election Commc'n, 134 S. Ct. 1434, 1448 (2014). Thus, if a financial transaction is more of a communication and not merely a "negotiable instrument," then it is not clear how *Miller* would be decided today.

***