2017

The Third-Party Doctrine and the Future of the Cloud

Neil M. Richards
Washington University in St. Louis School of Law, nrichards@wustl.edu

THE THIRD-PARTY DOCTRINE AND THE FUTURE OF THE CLOUD

NEIL RICHARDS*

ABSTRACT

When the government seeks electronic documents held in the cloud, what legal standard should apply? This simple question raises fundamental questions about the future of our civil liberties in the digital world. In a series of cases, government lawyers have argued that information shared with digital intermediaries—including emails and cloud-stored documents—can be seized without a warrant. Their argument rests upon a controversial Fourth Amendment principle known as the "Third-Party Doctrine," which maintains that information shared even with trusted "third parties" loses a reasonable expectation of privacy under the Fourth Amendment, and with it, the protection of the warrant requirement. Criminal defendants and civil libertarians have argued the opposite, and as the issue has not reached the Supreme Court, the two sides have fought to a messy standstill. This article puts the debate over the Third-Party Doctrine in historical, jurisprudential, and technological context, and offers a normative and civil-liberties-protective way forward for Fourth Amendment law in the age of the cloud. My claim is not only that we must reconsider the way we think about the Third-Party Doctrine, but that this shift in thinking will have important ramifications for the ways in which we think about technology and law (particularly constitutional law) more generally.

This argument proceeds in three steps. Part One develops a concept I call the "the lag problem" of the Fourth Amendment. Offering a bird's-eye historical view of the Fourth Amendment's relationship with new technologies, I show how the Fourth Amendment has been a bulwark of civil liberties against ever-encroaching state surveillance, but that our legal understandings of Fourth Amendment privacy have always lagged

* Thomas & Karole Green Professor of Law, Washington University School of Law; Affiliate Scholar, The Center for Internet and Society at Stanford Law School; Affiliate Fellow, the Information Society Project at Yale Law School; Fellow, Center for Democracy and Technology. For helpful discussions and comments on prior drafts, I am grateful to Steve Bellovin, Nate Cardozo, Danielle Citron, Nate Jones, Peter Joy, Orin Kerr, Sue Glueck, Jennifer Granick, David Gray, Woody Hartzog, Pauline Kim, Ed McNicholas, Marcia Hofmann, Paul Ohm, Bob Pollack, Dan Solove, Nancy Staudt, Brian Tamanaha, and Simon Waxman. This paper was supported by a grant from the Future of Privacy Forum underwritten by Microsoft Corporation, though all arguments and conclusions in it are my own.

somewhat behind our advancing technologies. Part Two focuses on the Third-Party Doctrine in particular, and makes two claims. The descriptive claim is that when its origins and assumptions are looked at more closely, the Third-Party Doctrine is really much smaller and more limited than most observers have assumed. The second normative claim is that the best way to understand the Third-Party Doctrine in the context of new technologies is in the limited, exceptional way in which it was adopted, rather than as a general rule that would swallow the essential principle that the Fourth Amendment guarantees a general protection of privacy for people against their government. Part Three argues that when we put the Third-Party Doctrine in its proper place as a limited exception rather than one that would swallow the rule of privacy, we need a new set of legal principles to govern Fourth Amendment privacy in the cloud.

I offer four such principles. First, I argue that the broad view of the Third-Party Doctrine is manifestly unsuited to the protection of our digital civil liberties. Second, I compare my approach to Orin Kerr's "Equilibrium-Adjustment Theory" of the Fourth Amendment, and contend that in contrast to Kerr's approach, when it comes to the question of closing lags in the civil liberties context, we should focus on those questions of civil liberties rather than on questions of state access to data. Third, I explain that the process of interpretation of the Fourth Amendment is inescapably normative, and I argue that principles of intellectual privacy offer a useful guide to the normative project of translating Fourth Amendment values in a way that closes the technological lag. Fourth, I explain that no matter how we interpret the Fourth Amendment, any approach to the protection of digital civil liberties will need to account for the important role that intermediaries play in the practices of data processing and protection. In a digital world, trusted intermediaries are very different from merely being "third parties," and whichever path our law takes, it must take this fact into account.

There are, of course, multiple paths that Fourth Amendment law could take in the future to grapple with these problems. My purpose is not so much to call for a particular solution as to highlight the considerations I believe should apply as we translate the Fourth Amendment's text into workable doctrine for the cloud age in a way that is practical but also protects the traditions and normative commitments of our hard-won civil liberties.

TABLE OF CONTENTS

INTRODUCTION

When the government seeks electronic documents held in the cloud,[1] what legal standard should apply? This simple question masks a surprising complexity. It also raises fundamental questions about the future of our civil liberties in the digital world. In a series of cases, government lawyers have argued that information shared with digital intermediaries—including emails and cloud-stored documents—can be seized without a warrant. Their argument rests upon a controversial Fourth Amendment principle known as the "Third-Party Doctrine," which maintains that information shared even with trusted "third parties" loses a reasonable expectation of privacy under the Fourth Amendment, and with it, the protection of the warrant requirement. Criminal defendants and civil libertarians have argued the opposite, and as the issue has not reached the Supreme Court, the two sides have fought to a messy standstill.

Yet issues of digital civil liberties and intermediaries refuse to stop coming. Beyond the high-profile case of smartphone security that pitted Apple Computer against the FBI over the contents of the San Bernardino Shooter's iPhone,[2] Microsoft is engaged in two separate lawsuits with the U.S. government over whether warrants issued by United States courts apply to electronic communications stored in other countries,[3] and the First and Fourth Amendment standards that should govern government orders that seek to secretly obtain the contents of its customers' emails stored in the cloud.[4]

At stake in these and other disputes is not only the privacy of users of electronic platforms, but the future of the cloud itself. As more of our lives are lived with the assistance and mediation of digital platforms, litigation testing the privacy of stored documents will in a very real sense determine

1. Paul Schwartz helpfully defines the "cloud" as "the locating of computing resources on the Internet in a fashion that makes them highly dynamic and scalable." Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. PA. L. REV. 1623, 1624 (2013). These resources can include cloud storage—like those stored in Dropbox, iCloud, or OneDrive—or it can include remote processing, such as the remote servers that power mobile phone applications like Apple's Siri or Internet of Things appliances like the Amazon Echo. In this Article, when I refer to the "cloud," I typically refer to the more colloquial usage of "cloud" as meaning remote storage rather than also remote processing.

2. *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. ED 15-0451M, 2016 WL 618401 (C.D. Cal. Feb. 16, 2016).

3. Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197 (2d Cir. 2016). *See generally* Microsoft Corp., DIGITAL CONSTITUTION, www.digitalconstitution.com.

4. Complaint for Declaratory Judgment, Microsoft Corp. v. U.S. Dep't of Justice, No. 2:16-cv-00538 (W.D. Wash. Apr. 14, 2016), 2016 WL 1464273; *see also* Neil M. Richards, *Secret Searches and Digital Civil Liberties* (forthcoming 2017).

the privacy of our digital society as a whole, and the extent to which we can trust the intermediaries that enable our participation in that society.[5] Cloud privacy thus implicates not only our newest technologies, but some of our most ancient and cherished civil liberties. Given the enormity of this question, courts resolving questions of cloud privacy must consider both the technological and constitutional contexts in which cloud providers are operating. While scholars have almost universally condemned the Third-Party Doctrine in the digital context,[6] courts remain confused about what legal regime should replace it. In this respect, the issue presents a thorny problem of line-drawing: a broad view of the Third-Party Doctrine might woefully underprotect civil liberties, but at least it has the perceived virtues of clarity and allowing law enforcement to obtain incriminating evidence.

This article puts the debate over the Third-Party Doctrine in historical, jurisprudential, and technological context, and offers a normative and civil-liberties-protective way forward for Fourth Amendment law in the age of the cloud. My claim is not only that we must reconsider the way we think about the Third-Party Doctrine, but that this shift in thinking will have important ramifications for the ways in which we think about technology and law (particularly constitutional law) more generally. This argument proceeds in three steps. Part One develops a concept I call the "the lag problem" of the Fourth Amendment. I offer a bird's-eye view of the Fourth Amendment's relationship with new technologies from its inception, and show not only that the Fourth Amendment has been a bulwark of civil liberties against ever-encroaching state surveillance, but that our legal understandings of Fourth Amendment privacy have always lagged somewhat behind our advancing technologies, from postal mail to the telegraph, and from telephones to the Internet. I argue not only that this is a

5. Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap*, 126 YALE L.J. 1180 (2017).

6. *E.g.*, Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 ¶ 49, https://journals.law.standford.edu/sites/default/files/stanford-technology-law-review-stlr/online/freiwald-first-principles.pdf; Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239, 1241 (2009); CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 66 (2007); DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 110 (2011); JAY STANLEY, AM. CONST. SOC'Y FOR LAW & POLICY, THE CRISIS IN FOURTH AMENDMENT JURISPRUDENCE 4 (2010), https://www.acslaw.org/publications/issue-briefs/teh-crisis-in-fourth-amendment-jurisprudence-0; Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 618–19 (2011). *But see* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004); Orin Kerr & Greg Nojeim, *The Data Question: Should the Third-Party Records Doctrine Be Revisited?*, A.B.A. J. (Aug. 1, 2012, 9:20 AM), http://www.abajournal.com/magazine/article/the_data_qeustion_should_the_third-party_records_ doctrine_be_revisited/.

common pattern from which we can learn, but that a certain kind of moderation in the development of legal doctrine can sometimes be a good thing, at least as long as the law catches up eventually rather than remaining ossified by the technological and social assumptions of the past. I conclude by suggesting that we are in the midst of another lag with respect to the constitutional protection afforded cloud data, and note that the development of the law is at an important crossroads, with broad readings of the Third-Party Doctrine threatening to substantially diminish the Fourth Amendment.

Part Two focuses on the Third-Party Doctrine in particular, and makes two claims. The first is a descriptive observation: when its origins and assumptions are looked at more closely, the Third-Party Doctrine is really much smaller and more limited than most observers have assumed. The second claim is normative. Applying the insights of the lag problem to the Third-Party Doctrine, I argue that the best way to understand the Third-Party Doctrine in the context of new technologies is in the limited, exceptional way in which it was adopted, rather than as a general rule that would swallow the essential principle that the Fourth Amendment guarantees a general protection of privacy for people against their government.

Part Three argues that when we put the Third-Party Doctrine in its proper place as a limited exception rather than one that would swallow the rule of privacy, we need a new set of legal principles to govern Fourth Amendment privacy in the cloud. The development of these principles will be difficult because the "cloud" is a complex and ever-changing set of technological, business, and legal relationships that implicate a wide variety of technological contexts, applications, and values on a global scale. Nevertheless, the lessons of the lag problem counsel a path forward. I argue that the future of Fourth Amendment law should be guided by four observations. First, I argue that the broad view of the Third-Party Doctrine is manifestly unsuited to the protection of our digital civil liberties. Second, I suggest that an appreciation of the lag problem offers a number of subtle but critical differences to (and, I argue, improvements upon) another leading theory of Fourth Amendment and technological development, Orin Kerr's "Equilibrium-Adjustment Theory."[7] Third, any interpretations of the Fourth Amendment and technology must be not only attentive to the lag problem, but will inevitably and inescapably be normative. In resolving this problem, I argue, the theory of intellectual privacy that I have developed in other work

7. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011).

must be an essential part of the normative calculus that must guide the development of a digital Fourth Amendment. This theory argues that privacy protections for intellectual activities—thinking, reading, and discussing with confidantes—are essential to meaningful civil liberties. Fourth, the project of civil liberties in the cloud (especially in the Fourth and First Amendment contexts) will require both the participation of intermediaries and the recognition by our law that intermediaries will often be best placed to advance civil liberties on behalf of their human clients. Legal doctrine in this area that ignores intermediaries is likely to be unrealistic and under-protective of the fundamental values at stake.

While our law has understandably lagged in this area, now is the critical time to translate our hard-won civil liberties from the physical world into the digital one. At a minimum, the best reading of the history, theory, and doctrine of Fourth Amendment law is to treat cloud data as fully protected by the Fourth Amendment, even when that data is held by trusted third parties such as cloud service or email providers. Fourth Amendment law must embrace the invitation offered by the Supreme Court's recent *Jones*[8] and *Riley*[9] decisions, and bring the Fourth Amendment into the cloud.

I. THE FOURTH AMENDMENT LAG PROBLEM

Lag is a perennial problem in law; in fact, it may be its defining problem. Laws and legal rules are intended to endure across the years, yet they are embodied in words that reflect the language and assumptions of their own time. These assumptions are inevitably a function of existing technologies, but technologies change and disrupt these assumptions and the legal rules they have produced. As Brian Tamanaha puts it well, "The challenge for modern legal systems . . . is that social mores change more swiftly than law, constantly generating a gap between them."[10]

An important illustration of this phenomenon is the story of how Fourth

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

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

10. Brian Z. Tamanaha, *The Third Pillar of Jurisprudence: Social Legal Theory*, 56 WM. & MARY L. REV. 2235, 2248 (2015). This concept has a long pedigree in American legal thought. *See, e.g.*, HENRY SUMNER MAINE, ANCIENT LAW: ITS CONNECTION WITH THE EARLY HISTORY OF SOCIETY, AND ITS RELATION TO MODERN IDEAS 24 (London, John Murray 1861) ("Law is stable; the societies we are speaking of are progressive. The greater or less happiness of a people depends on the degree of promptitude with which the gulf is narrowed."); BENJAMIN N. CARDOZO, THE PARADOXES OF LEGAL SCIENCE 6, 10–11 (1928) (noting that the law's perpetual task is to manage "permanence with flux, stability with progress," and that "[w]e live in a world of change. If a body of law were in existence adequate for the civilization of today, it could not meet the demands of the civilization of tomorrow. Society is inconstant. So long as it is inconstant, and to the extent of such inconstancy, there can be no constancy in law. The kinetic forces are too strong for us").

Amendment constitutional rules have grappled with evolving communications technologies and the social expectations and practices surrounding those technologies. From the nineteenth century to the twenty-first, key Supreme Court cases interpreting the Fourth Amendment have illustrated not only that new technologies and practices have taken a while to be recognized by law, but that both Fourth Amendment law and technology have been changing at the same time. Even though the Fourth Amendment has often fallen behind developing technologies, it has invariably caught up as social norms have wrapped important technologies with expectations of privacy.

In this Part, I explain what I call the "Fourth Amendment lag problem." Beginning with the origins of the Fourth Amendment and the ratification of the Bill of Rights, I trace the development of Fourth Amendment law in the context of technological change. Four technologies in particular are central to this account—the postal system, the telegraph, the telephone, and the digital technologies that are currently transforming our society. Woven throughout this account is the idea that the Fourth Amendment was intended to be and has served as a protection for political liberty, and that nowhere is this protection more important than in the privacy protection of social practices in which political ideas are tested—thinking, reading, and communicating with confidantes.

A. Origins & Methods

From a twenty-first-century perspective, we typically think of the Fourth Amendment as reconciling the competing demands of police investigation of crime with the civil liberties of those being investigated. But the Fourth Amendment was not originally designed as such. Scholars working at the intersection of law and history over the past several decades have deepened our understanding about the circumstances prompting the drafting and ratification of the Amendment, as well as some of the implications of that history. Of course, any invocation of history in the context of constitutional interpretation raises the methodological issues of originalism, and the appropriateness (and limits) of the use of history as an interpretive device. My purpose in this section is modest, drawing from this literature in order to set the context for the reading of the cases that follows. Methodologically, my approach is history-informed but not originalist, as I have written about the practical and normative limitations of strict originalism elsewhere.[11] The

11. Neil M. Richards, *Clio and the Court: A Reassessment of the Supreme Court's Uses of History*, 13 J.L. & POL. 809 (1997).

method I employ, as Justice Kennedy put it similarly in his recent opinion of the Court in *Obergefell v. Hodges*, is one that "respects our history and learns from it without allowing the past alone to rule the present."[12]

The Fourth Amendment guarantees in full that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[13] While the implications of the Fourth Amendment's history remain a topic of scholarly debate,[14] the literature allows us to make a number of conclusions about the Fourth Amendment's right against unreasonable searches and seizures that was ratified in 1789. First, the right was a response to perceived abuses of the Crown in the late colonial and Revolutionary periods of American history. One government practice that particularly rankled the colonists who would become revolutionaries was the use of so-called "general warrants," search authorizations that were not limited in scope and were not required to identify the target of the search with specificity.[15] General warrants were problematic because they greatly increased the power of the state in a relatively unchecked way. As Leonard Levy explains, "[p]romiscuously broad warrants allowed officers to search wherever they wanted and to seize whatever they wanted, with few exceptions."[16]

Second, it is important to appreciate how the Fourth Amendment's rejection of general warrants operates to provide a structural limitation on the power of the state. Fourth Amendment rights are not just a civil liberty, but a substantive check on the power of the state to intrude into and interfere with the privacies of life. As Raymond Ku has argued, the Fourth Amendment "is best understood as a means of preserving the people's authority over government—the people's sovereign right to determine how and when government may intrude into the lives and influence the behavior of its citizens."[17] Ku's review of the history of the origins of the Fourth

12. Obergefell v. Hodges, 135 S. Ct. 2584, 2598 (2015).

13. U.S. CONST. amend. IV.

14. *See generally* WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 602–1791 (2009).

15. *See* Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1190 (2016) [hereinafter Donohue, *The Original Fourth Amendment*]; *see also* LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE 75, 81–84 (2016) [hereinafter DONOHUE, FOREIGN INTELLIGENCE].

16. LEONARD W. LEVY, ORIGINS OF THE BILL OF RIGHTS 153 (1999).

17. Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1326 (2002).

Amendment provides strong evidence that its purpose was to guarantee limits on the power of the executive to surveil and interfere with its citizens.[18] David Gray has also offered an insightful reading of the warrant requirement's history as promoting a collective principle of security against an aggressive state.[19] Similarly, William Stuntz has shown how the original purpose of the Fourth Amendment was not so much privacy as it was to place substantive limitations on the scope of the government's power,[20] while there is also substantial evidence that the guarantee of these promises in the Bill of Rights was central to the ultimate ratification of the Constitution.[21]

Third, the nature of that substantive limitation on government power was, among other things, a limitation on its ability to use its power to investigate, peer into, and thereby chill minority political and religious beliefs held by its citizens. In this respect, it is notable that the right against unreasonable searches and seizures was understood at the time of its recognition to be related to other protections of the Bill of Rights, most notably the First Amendment protections for free speech and press, the Third Amendment protection against the quartering of soldiers in private homes, and the Fifth Amendment right against self-incrimination.[22]

Most important of these for our purposes is the linkage between the Fourth and First Amendments. Robust libertarian protection for speaking and writing is a relatively recent phenomenon in American law, and only really began to develop from the middle of the twentieth century onwards.[23] However, it is impossible to understand the scope of protection for political liberty envisioned by the Constitution and the Bill of Rights without an appreciation of the important role that the Fourth Amendment played in this scheme. We see this textually in the Amendment's protection of the "right

18. *Id.* at 1332–43.

19. David Gray, *Fourth Amendment Remedies as Rights: The Warrant Requirement*, 96 B.U. L. REV. 425 (2016).

20. William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 447 (1995).

21. Donohue, *The Original Fourth Amendment*, *supra* note 15, at 1283–98; DONOHUE, FOREIGN INTELLIGENCE, *supra* note 15, at 92.

22. LEONARD W. LEVY, ORIGINS OF THE FIFTH AMENDMENT: THE RIGHT AGAINST SELF-INCRIMINATION 390 (1968).

23. *See* MARK A. GRABER, TRANSFORMING FREE SPEECH: THE AMBIGUOUS LEGACY OF CIVIL LIBERTARIANISM 106–08 (1992) (discussing early-twentieth-century free speech jurisprudence); G. Edward White, *The First Amendment Comes of Age: The Emergence of Free Speech in Twentieth-Century America*, 95 MICH. L. REV. 299, 318 (1996) (same); DAVID M. RABBAN, FREE SPEECH IN ITS FORGOTTEN YEARS 282 (1997) (same); *see also* RICHARDS, *supra* note 68, at 33–40 (discussing the evolution of modern First Amendment principles from the opinions of Justice Brandeis in the 1920s to the late twentieth-century).

of the people to be secure in their . . . papers, and effects" which would have included diaries and private letters, many of which may have been dissenting, subversive, scandalous, blasphemous, and possibly even all four at once.[24] Agents of the Crown regularly used general warrants to seize papers of this sort, in a way that undermined the practical ability of citizens to engage in private, collective political activity.[25] William Cuddihy notes that "[b]y 1763, general warrants to censor the British press were so common that their champions published an anthology of them dating back a century."[26] The Fourth Amendment can only be seen as a direct rejection of these colonial practices of issuing general warrants, such as writs of assistance, and of unwarranted and unconstrained searches and seizures more generally.[27] The cases from the 1760s that prompted the Fourth Amendment—the prosecutions of John Entick[28] and John Wilkes[29] in England and the *Writs of Assistance* case[30] in Boston—were thus not really "criminal procedure" cases as we understand the term today, but rather substantive cases about the protection of political dissent from an aggressive and inquisitive state.[31]

So, too, were the pre-revolutionary practices that spurred the Fifth Amendment's right against self-incrimination.[32] As William Stuntz observed over twenty years ago, the events and precedents that stimulated the recognition of Fourth and Fifth Amendment rights were "classic First Amendment cases in a system with no First Amendment, no vehicle for direct substantive judicial review,"[33] and no police forces. The recognition of express protection for "papers" should thus best be understood as an attempt to place a substantive limit on government power primarily in the context of communications and dissent.

---

24. U.S. CONST. amend. IV.
25. CUDDIHY, *supra* note 14, at 343, 373–74; LEVY, *supra* note 16, at 172; Stuntz, *supra* note 20, at 394.
26. CUDDIHY, *supra* note 14, at 774.
27. LEVY, *supra* note 16, at 150, 153–54.
28. Entick v. Carrington (1765) 95 Eng. Rep. 807; 19 Howell's State Trials 1029.
29. Wilkes v. Wood (1763) 98 Eng. Rep. 489; 19 Howell's State Trials 1153.
30. The Boston *Writs of Assistance* case took place in 1761. Stuntz, *supra* note 20, at 396 n.9 (citing M.H. SMITH, THE WRITS OF ASSISTANCE CASE (1978)).
31. *Id.* at 403, 408.
32. *Id.* at 413; LEVY, *supra* note 22, at 338–39.
33. Stuntz, *supra* note 20, at 403.

B. The Mails

During the nineteenth century, the Fourth Amendment, like other protections of the Bill of Rights, did not apply to the states.[34] In the absence of a federal police force, Fourth Amendment issues arose far less frequently than they do today. The Supreme Court was finally called upon to interpret the Fourth Amendment in the 1878 case of *Ex parte Jackson*, involving the confidentiality of private mail carried by the Post Office.[35] In retrospect, it should be no surprise that the case involved the federal mails. The Post Office was not merely one of the first departments of the federal government, but arguably the most important. Article I Section 8 of the Constitution granted Congress the power "to establish Post Offices and post Roads,"[36] a power that Congress wasted no time in executing. One of the First Congress's initial acts of business was to create the Post Office; in fact, the Post Office shared equal billing with the Bill of Rights and a fisheries bill in a notification sent by Secretary of State Thomas Jefferson to the States in 1789.[37] The Post Office was a communications network that tied the newly united states into a single nation, and its importance to the project of national unity under the new Constitution is difficult to overstate.[38]

There was no guarantee, however, that the new Post Office would provide confidential mails, either by mandate of the Fourth Amendment or from some other source. At the time of the ratification of the Fourth Amendment and the creation of the Post Office, postal confidentiality was definitely seen as desirable, but it was not considered to be mandated by constitutional law or tradition.[39] This fact is illustrated by correspondence from none other than George Washington, who feared for the confidentiality of the ideas he expressed in letters about the Constitution. Washington was legitimately concerned about his correspondence and its ideas, that "by passing through the post-office . . . they should become known to all the world."[40] Washington's fears dated back to the colonial experience, in

34. Barron v. Mayor of Baltimore, 32 U.S. (7 Pet.) 243 (1833) (holding that the Bill of Rights does not apply to actions by state governments).

35. *Ex parte* Jackson, 96 U.S. 727 (1878).

36. U.S. CONST. art. I, § 8, cl. 7.

37. LEVY, *supra* note 16, at 12.

38. *See generally* RICHARD R. JOHN, SPREADING THE NEWS: THE AMERICAN POSTAL SYSTEM FROM FRANKLIN TO MORSE (1995).

39. Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L. J. 123, 141 (2007).

40. DAVID J. SEIPP, THE RIGHT TO PRIVACY IN AMERICAN HISTORY 11 (1978) (quoting Letter from George Washington to Marquis de Lafayette (Feb. 7, 1788), *in* 11 THE WRITINGS OF GEORGE WASHINGTON 218 (Worthington C. Ford ed., New York, G.P. Putnam's Sons 1891)), http://pirp.harvard.

which the British Post Office had been part of the intelligence network of the Crown, a practice that, if anything, had been stepped up during the Revolution.[41] Yet Washington phrased his concern in terms of the desirability of confidentiality rather than in terms that the law mandated such arrangements.

By contrast, by the middle of the nineteenth century, as David Seipp explains, public opinion had come to regard "the 'sanctity of the mails' as absolute in the same way it esteemed the inviolability of the home."[42] This belief treated postal confidentiality as nothing less than sacred; an elementary building block of the American national compact.[43] Thus, what had been little more than a hope of postal privacy in 1789 had evolved within a century into a broad social consensus that postal privacy was an essential element of the rights of Americans against their government. Anuj Desai has powerfully demonstrated how the experience of the Revolution led Benjamin Franklin and other early leaders of the Post Office to build protections for postal confidentiality into the administrative fabric and culture of the new agency.[44] A combination of statutes enacted by the Continental Congress, internal rules of practice, and the federal Post Office Act of 1792 established a baseline rule of postal privacy from sources other than the First and Fourth Amendments.[45] This principle of privacy was extended formally to third parties with the passage of the Postal Act of 1825.[46] During the next hundred years, these administrative norms developed into broader social expectations about the inviolability of the confidentiality of letters entrusted to postal carriers.[47]

Ex parte Jackson put these expectations to the test. Jackson had been convicted of using the mails to distribute an advertisement for lottery prizes, in violation of an 1868 Act of Congress.[48] The case presented a relatively

---

edu/pubs_pdf/seipp/seipp-p78-3.pdf.

41. KENNETH ELLIS, THE POST OFFICE IN THE EIGHTEENTH CENTURY: A STUDY IN ADMINISTRATIVE HISTORY viii (1958); Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 STAN. L. REV. 553, 559–63 (2007); JOHN, *supra* note 38, at 43.

42. Note, *The Right to Privacy in Nineteenth Century America*, 94 HARV. L. REV. 1892, 1899 (1981).

43. *Id.*

44. Desai, *supra* note 41, at 568.

45. *Id.*

46. Act of March 3, 1825, ch. 64, 4 Stat. 102, 107.

47. Desai, *supra* note 41, at 568, 577.

48. *Ex parte* Jackson, 96 U.S. 727, 728, 730 (1878). In addition to his Fourth and First Amendment arguments, Jackson made several other wide-ranging challenges to his conviction, including Congress's power to pass the statute under the Postal Clause in the first place, a challenge which the Court dismissed. *Id.* at 729–30.

simple question under the Fourth Amendment—was a warrant required before the Post Office opened a letter in its possession? Textually, at least, there was a very good argument that the answer should have been "no." The Fourth Amendment mentions a person's "papers," which would presumably include letters, but letters sent in the mail are given to a government official (a postal carrier) and usually protected by little more than paper and seal of some sort, whether of wax or glue. Under such circumstances, where a paper letter is literally in the hands of the government, it was not clear as a textual matter that a warrant would be constitutionally required. The argument that a letter-writer had waived any Fourth Amendment protection by handing the letter to the state for delivery would seem to have been a strong one.

But Jackson and his lawyers (one of whom was fittingly named "Mr. Post") rejected this argument. They argued that because Congress had vested a monopoly over the mails in the Post Office and given it the power to exclude certain categories of letters from delivery, this power, if left unchecked, contained the potential for abuse whereby the government could "cut off all means of epistolary communication upon any subject which is objectionable to a majority of its members."[49] In other words, they asserted that Congress lacked the power to inspect and thereby chill minority expression. This was of course no less than an implicit First Amendment argument, a type of claim that, as explained above,[50] was consistent with several centuries of argumentative practice in British, colonial, and American search and seizure cases.

The Supreme Court accepted both Jackson's First and Fourth Amendment concerns, and held that a warrant was required before a postal inspector opened a letter or sealed package. The Court reasoned that these sorts of materials:

> 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. The 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. . . . No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and all regulations adopted as to mail matter of

49. *Id.* at 730–31.
50. *See supra* notes 23–33 and accompanying text.

> this kind must be in subordination to the great principle embodied in the fourth amendment of the Constitution.[51]

Importantly, the *Jackson* Court understood its Fourth Amendment holding to be motivated by First Amendment considerations as well. Immediately following its holding that the Fourth Amendment required a warrant before a letter held by the Post Office could be opened by it, the Court explained the close relationship between the privacy of letters and the freedom of expression. It reasoned:

> Nor can any regulations be enforced against the transportation of printed matter in the mail, which is open to examination, so as to interfere in any manner with the freedom of the press. Liberty of circulating is as essential to that freedom as liberty of publishing; indeed, without the circulation, the publication would be of little value. If, therefore, printed matter be excluded from the mails, its transportation in any other way cannot be forbidden by Congress.[52]

The Court's linkage of the First and Fourth Amendments in this way in assessing the constitutional protection given to letters or other papers is particularly significant since there was essentially no First Amendment law when *Jackson* was decided in 1878.[53] Although it has never been appreciated as such, *Ex parte Jackson* can thus be considered to be the first important freedom of expression case decided by the Supreme Court. And it is significant that the issue that first caused the Court to interpret the First Amendment in a protective way was the issue of privacy of letters carried in the mails.

Underlying the Supreme Court's decision in *Jackson* was the robust tradition of postal privacy that had developed in the ninety-eight years that the Fourth Amendment had also largely lain dormant. Whereas it was perhaps unlikely in 1789 that a court would have held that warrants were required before the government could open letters in the post, in the intervening century a combination of government policies and evolving social expectations resulted in the mails being imbued with a culturally shared understanding of constitutional protection.[54] The rule in *Jackson* did not result from either Fourth Amendment originalism or existing judicial

---

51. *Jackson*, 96 U.S. at 733.

52. *Id.*

53. MICHAEL KENT CURTIS, FREE SPEECH, "THE PEOPLE'S DARLING PRIVILEGE": STRUGGLES FOR FREEDOM OF EXPRESSION IN AMERICAN HISTORY 13–14 (2000).

54. For more on the development of privacy expectations surrounding letters in the nineteenth century, see Richards & Solove, *supra* note 39, at 140–44.

precedent, but rather from the policy changes in the early Post Office that gave an administrative guarantee of postal confidentiality in order to encourage the development of trust in the new federal postal system.[55]

From this broader perspective, *Jackson* can be seen as closing a lag between law on the books and changed social expectations. The expansion of the federal postal network alongside the expansion of the new United States in the nineteenth century was a new techno-social practice that pushed beyond existing legal rules (in this case, the constitutional rules respecting postal confidentiality). While the Fourth Amendment lagged behind, users and administrators of the new Post Office network developed norms of postal confidentiality starting in the 1780s. By the time the Supreme Court addressed the issue of whether the Fourth Amendment protected postal confidentiality almost a century later, the social norms surrounding the mails had evolved so as to treat postal privacy as sacred. As a result, the evolution of social norms made it easy for the Court to end the lag in Fourth Amendment doctrine, and it was made even easier by the close nexus between the Fourth Amendment issue (postal confidentiality) and the First Amendment interests in dissemination of information and ideas about public matters.

C. The Telegraph

The mails were not the only Fourth Amendment context in which the lag problem occurred in the nineteenth century. The lag problem was also present in the development of the other great nineteenth-century communications network—the telegraph, which was invented in 1844.[56] Like the mails, the telegraph involved an intermediary (in this case the telegraph company) who was entrusted with the contents of a message; but unlike the mails, telegraph companies were not government agents, but rather private enterprises such as Western Union. As Thomas Cooley put it in 1879, "There are . . . to every telegraphic despatch three parties—the sender, the receiver and the telegraph company."[57] In order to build customer trust, telegraph companies imposed rules guaranteeing telegraphic confidentiality, and pushed for a federal law that would guarantee telegrams the privacy of the U.S. Mail.[58] However, telegraph companies were

55. Desai, *supra* note 41, at 557.

56. ITHIEL DE SOLA POOL, TECHNOLOGIES OF FREEDOM 25 (1983).

57. Thomas M. Cooley, *Inviolability of Telegraphic Correspondence*, 27 AM. L. REG. 65, 66 (1879).

58. WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 146–47 (updated and expanded ed. 2007).

unsuccessful in their efforts, in significant part due to the fact that the public issue of telegraphic confidentiality became bound up in the controversy surrounding the disputed Hayes-Tilden presidential election of 1876.[59] The Supreme Court did not rule on the issue, but the Missouri Supreme Court did in the context of allegations that both the St. Louis police commissioner and the state governor had been involved in an illegal gambling ring. That court reached a compromise, allowing access to the telegrams without a warrant, but requiring that any request for the contents of telegraphic communications specify both the date and subject of the message, a kind of specificity but not quite a warrant.[60] Other states took action on the issue as well; a majority of states had passed telegram confidentiality statutes by 1885,[61] while many states had also restricted access by government agents and private parties.[62]

Unlike the case of the mails (and as we will see, the telephone), the privacy of telegrams was not directly settled by the Supreme Court's prompt extension of Fourth Amendment protection. Nevertheless, the hallmarks of the lag problem were certainly present in the case of telegrams. Telegraphy was a new technology that enabled for the first time the rapid transmission of short text messages over long distances. This new capacity created a challenge for existing legal structures that had not contemplated the technology and especially the fact that reading telegrams could happen either by tapping the live wires or by examining copies held by the privately-owned telegraph companies.[63] The technology thus jumped out ahead of the law, which lagged behind. But as the technology developed, and as patterns of use and social expectations built up around it, the lag between law and social expectations began to close, first by business practices guaranteeing confidentiality to customers by contract, and then by state statutory law. What is important to take from this example is the dynamism of the legal system, and its capacity to bring new and disruptive technologies within its protection over time, whether by constitutional law or other means

One reason that the telegraph may not have received the same level of protection as the mails is that for much of the nineteenth century it remained an expensive technology, more suited to terse business and government communications than to extended discussions of politics (for example) by

59. SEIPP, *supra* note 40, at 30–40.

60. *Ex parte* Brown, 72 Mo. 83, 93–95 (1880); *see also* SEIPP, *supra* note 40, at 41–42.

61. MORRIS GRAY, A TREATISE ON COMMUNICATION BY TELEGRAPH § 120, at 212 & n.1, 213 & nn.1–3 (Boston, Little, Brown & Co.1885) (collecting statutes).

62. *Cf*. Note, *supra* note 42, at 1901 (noting that it was "much debated" whether nineteenth century state statutes prevented government investigators from accessing telegrams).

63. DIFFIE & LANDAU, *supra* note 58, at 146.

ordinary people.[64] That void would ultimately be filled in the twentieth century by the telephone, to which we now turn.

D. Telephones

Unlike the mails and the telegraph, however, the Fourth Amendment status of telephones prompted sustained judicial attention over almost a century. The telephone represents the third major communications network in which we can observe the pattern of the lag problem, and it is one that is a more familiar story to discussions of privacy and the Fourth Amendment.

Telephone technology was developed in the 1870s after pioneering scientific work by Alexander Bell and others. The telephone network developed quickly, and shared similarities with both the mails and the telegraph. Like the mails, the telephone connected households and permitted extensive communications beyond the technical limitations of telegraphy. Like telegraphs, telephones were privately developed, and required trust in both the recipient of a call and the private telephone company to ensure confidentiality. Early telephones were rudimentary compared to the mature technology with which we are familiar today; making a call required a caller to dictate the number to a human operator who would manually make the connection.[65] Moreover, some early telephones were communal "party lines," in which one line was shared by a community. It was some time before the technology of electronic dialing and the norm of private, residential telephones took root, a reminder that individual technologies themselves change over time.[66]

It was in the context of these early telephones that the Supreme Court decided the 1928 case of *Olmstead v. United States*.[67] Olmstead was one of the most ambitious bootleggers in American history, a former Seattle police officer whose criminal business during Prohibition made him the largest employer in the Puget Sound area.[68] A lengthy police investigation into his organized criminal enterprise resulted in Olmstead's arrest and conviction for violations of the National Prohibition Act.[69] Much of the key evidence against Olmstead was provided by warrantless wiretaps of the telephone line

64. *See* POOL, *supra* note 56, at 91.

65. RICHARD R. JOHN, NETWORK NATION: INVENTING AMERICAN TELECOMMUNICATIONS 383–85 (2010).

66. *Id.*

67. 277 U.S. 438 (1928).

68. NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 139–40 (2015).

69. *Olmstead*, 277 U.S. at 455–57.

he had installed between his home and his enterprise's headquarters in Seattle, and which he had used to direct his criminal empire.[70] On appeal, the Supreme Court rejected Olmstead's argument that the Fourth Amendment required a warrant before the police could wiretap a telephone call. Chief Justice Taft looked at the text of the Fourth Amendment and saw that it protected tangible, physical things—persons, houses, papers, and effects. He then looked at the telephone, which involved electrical impulses being sent along a phone line that ran, like a road, between buildings, and concluded that a warrant was not necessary because telephone calls did not involve "tangible material effects."[71]

Olmstead is best known today for the famous dissent of Justice Brandeis, who argued that warrantless wiretaps violated the Fourth Amendment.[72] Two basic principles motivated Brandeis's dissent—the importance of civil liberties against the government and the need for the law to keep up with changing technologies. He explained that changing technologies threatened an "invasion of 'the sanctities of a man's home and the privacies of life'"[73] by enabling "[s]ubtler and more far-reaching means of invading privacy . . . . Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet."[74]

In a passage that seems to have uncannily foreseen the development of cloud computing, Brandeis predicted that:

> [w]ays may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions.[75]

Brandeis argued that the Court's view of existing law was cramped and unimaginative, and that its insistence that the Fourth Amendment only protected tangible property would eviscerate the important civil liberties at issue. He suggested that, on the contrary, the Fourth Amendment needed to evolve in the face of changing technology to protect its core values,

70. *Id.* at 456–57.
71. *Id.* at 466.
72. *Id.* at 471–85 (Brandeis, J., dissenting).
73. *Id.* at 473 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).
74. *Id.*
75. *Id.* at 474.

including "the significance of man's spiritual nature, of his feelings and of his intellect."[76] I have argued at length elsewhere that when Brandeis's dissent is read in connection with his First Amendment opinions, it becomes clear that he saw the critical linkages between the protection of communications privacy and the importance of free expression, a value I have termed "intellectual privacy."[77]

Chief Justice Taft did not rule in *Olmstead* that users of telephones desiring privacy against the government were completely out of luck. He noted that although the Fourth Amendment did not protect the confidentiality of telephone conversations, Congress was certainly able to pass a law protecting them.[78] Several years later, Congress did exactly that with the Communications Act of 1934, section 605 of which made wiretapping by private parties a federal crime, and barred the government from introducing in court evidence it had obtained from warrantless wiretapping.[79] However, as an evidentiary rule rather than a prohibition, section 605 did little in practice to restrain government officials from widespread eavesdropping.[80]

One important difference between the Court's examination of telephones and the mails was that it decided its first telephone case well before the social importance of telephones had been established. Despite the lack of a social consensus in favor of the confidentiality of telephone calls, however, the rule in the *Olmstead* case was unpopular. As the twentieth century advanced and as telephone technology became more accessible to the general public, the social norm respecting the confidentiality of telephone conversations took root, just as it had in the context of the mails and the telegraph. But even as telephone technology became more private, the absence of meaningful restriction of government wiretapping led to widespread and well-documented abuses. These included warrantless wiretapping by the FBI of political subversives and dissidents such as Martin Luther King, Jr.[81]

Whether in spite of or because of these abuses, a line of Warren Court

76. *Id.* at 478.

77. RICHARDS, *supra* note 68, at 5, 95, 143–45.

78. *Olmstead*, 277 U.S. at 465–66.

79. DANIEL J. SOLOVE & PAUL SCHWARTZ, INFORMATION PRIVACY LAW 273–74 (5th ed. 2015); Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1273 (2004).

80. Solove, *supra* note 79, at 1273–74.

81. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1953 (2013); FREDERICK A.O. SCHWARZ JR. & AZIZ Z. HUQ, UNCHECKED AND UNBALANCED: PRESIDENTIAL POWER IN A TIME OF TERROR 22–23 (2007); DAVID J. GARROW, THE FBI AND MARTIN LUTHER KING, JR. 117–18, 148–50 (Penguin Books 1984) (1981).

Fourth Amendment cases gradually chipped away at the refusal of the Court in *Olmstead* to extend the Fourth Amendment to electronic technologies. In *Lopez v. United States*,[82] the Court upheld a bribery conviction based upon a recorded conversation made with the warrantless use of a pocket wire recorder, but only over a blistering dissent from Justices Brennan, Douglas, and Goldberg championing the right to privacy, and with the Chief Justice wavering in a concurrence that shared their concerns. Four years later, in the *Katz* case, the Court held that warrantless government wiretapping violated the Fourth Amendment, even when it occurred in the context of a public phone booth.[83] In so doing, the Court reversed its decision in *Olmstead* decided thirty-nine years before.

Katz, of course, is best known for Justice Harlan's famous concurrence, in which he articulated the notion of a "reasonable expectation of privacy," which has since become one of the touchstones of Fourth Amendment law.[84] *Katz* is a famous case, and as such has had a substantial mythology built up around it. Like most "great cases," the mythology has tended to obscure important nuance. One of these nuances is Justice Harlan's rationale for grounding the Fourth Amendment in privacy. Harlan advanced the idea that for the warrant requirement to apply, a defendant must have had both an actual, subjective expectation of privacy, and also "one that society is prepared to recognize as 'reasonable.'"[85] What is particularly interesting is the frequently overlooked rationale on which Harlan's articulation of the rule rested. He noted that:

> a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected" because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.[86]

In other words, the key for Fourth Amendment protection was not whether something was physical or intangible, or in or out of a house (or a phone booth). The key was instead the normative social expectations surrounding the activity—the very kind of normative social expectations that had built

82. 373 U.S. 427 (1963).
83. Katz v. United States, 389 U.S. 347 (1967).
84. *Id.* at 361 (Harlan, J., concurring).
85. *Id.*
86. *Id.*

up over time in the past to surround the mails, and to a lesser extent the telegraph. As Harlan noted further:

> The critical fact in this case is that "[o]ne who occupies it, [a telephone booth] shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume" that his conversation is not being intercepted. The point is not that the booth is "accessible to the public" at other times, but that it is a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable.[87]

For better or worse, then, a Fourth Amendment built on objectively reasonable expectations of privacy is inescapably one that must be built on normative, contextual (and thus complicated) foundations. I will return to this theme in Part III.

A second often-overlooked dimension of *Katz* is the relationship between the *Olmstead-Katz* line of cases and the First Amendment. I have argued elsewhere that Justice Brandeis's opinion in *Olmstead* fits neatly with his contemporaneous dissents in early First Amendment cases to sketch out the broad outlines of a theory of intellectual privacy.[88] There are other important privacy linkages from the *Katz* period as well, linkages that echo earlier understandings of rights against government searches as protections for political, religious, and cultural dissent. In *Mapp v. Ohio*,[89] which had a few years earlier established that the exclusionary rule for Fourth Amendment violations applies to the States, police searching for evidence of racketeering prosecuted the defendant for possession of pornographic books and pictures instead.[90] A subsequent case with strikingly similar facts, *Stanley v. Georgia*, ended the practice of police snooping through personal libraries once and for all under the direct auspices of the First Amendment, declaring:

> If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional

87. *Id.* (alterations in original) (citations omitted).

88. Neil M. Richards, *The Puzzle of Brandeis, Privacy, and Speech*, 63 VAND. L. REV. 1295 (2010); RICHARDS, *supra* note 68, at 5, 143–145.

89. 367 U.S. 643 (1961).

90. *Id.* at 644–45.The Exclusionary Rule forbids the admission of incriminating evidence obtained in violation of the Fourth Amendment. *Id*. at 648.

> heritage rebels at the thought of giving government the power to control men's minds.[91]

Another example of this phenomenon is the Court's decision three year later in the so-called "*Keith*" case, which held that the Fourth Amendment applies to investigations of domestic terrorists.[92] As Justice Powell explained in his opinion for the Court:

> History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect "domestic security." Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent.[93]

Though modern lawyers tend to separate out the doctrines of free speech and search and seizure (perhaps in large part due to the sheer size of each body of law), the intermingling of these issues was as common in the age of the telephone as it was in the age of paper. With the *Katz* reversal of *Olmstead* and the return of the implicit linkages between the First and Fourth Amendments, the doctrinal lag surrounding telephones (and early electronic communications more generally) was closed.

Congress had been waiting for *Katz* to come down. The following year it enacted the Omnibus Crime Control and Safe Streets Act of 1968,[94] which included the Wiretap Act.[95] Using *Katz* as a constitutional floor, the Wiretap Act specified detailed procedures for warrants to obtain the contents of telephone calls, and, among many other provisions, made unauthorized wiretapping by private or public actors a federal felony.[96]

---

91. Stanley v. Georgia, 394 U.S. 557, 565 (1969).
92. United States v. U.S. Dist. Court, 407 U.S. 297 (1972).
93. *Id.* at 314.
94. Pub. L. No. 90-351, 82 Stat. 197 (1968) (codified as amended in scattered sections of 18 U.S.C.).
95. *Id.* tit. 3, 82 Stat. at 211 (codified as amended at 18 U.S.C. §§ 2510–2522).
96. *Id.*

E. Data

Technology, however, did not stop moving, nor did it stop creating lags between the law on the books and the social and technical practices in action. Digital technologies powered by "Moore's Law"[97] have roughly doubled in power every two years for decades, with a corresponding drop in cost for computing power.[98] The rise of business and personal computers, the Internet, smartphones, and big data analytic tools over the past half-century has created unprecedented virtual mountains of personal data, as well as an inevitable lag as legal rules have struggled to keep pace with the information revolution.[99] Congress passed the Electronic Communications Privacy Act in 1986 to bring the nascent technology of email within the Wiretap Act's statutory framework,[100] but at the federal level at least, the law has largely ossified since then.

In recent years, federal and state courts have been bombarded with a bewildering series of cases that have forced them to grapple with the Fourth Amendment protection afforded to a wide array of different types of personal data sought by law enforcement. These cases have included text messages,[101] email contents,[102] the files and other data contained on smartphone hard drives,[103] IP addresses,[104] cell phone "metadata,"[105] and data obtained by cell-site simulators, colloquially known as "stingrays,"

97. Moore's Law refers to the phenomenon that processing power/transistor density has doubled roughly every 18–24 months since the 1960s, permitting geometric expansion in computing power for a fixed price. It was first announced in 1965 as an industry aspiration by Gordon Moore, an engineer and later co-founder of Intel. *See* Gordon E. Moore, *Cramming More Components onto Integrated Circuits*, ELECTRONICS, Apr. 19, 1965, at 114–17.

98. *See* Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393, 398 (2014).

99. *See* Neil M. Richards, *Digital Laws Evolve*, *in* THE WIRED WORLD IN 2015, at 83–84 (David Baker ed. 2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2523748.

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

101. City of Ontario v. Quon, 560 U.S. 746, 759–60 (2010).

102. United States v. Warshak, 631 F.3d 266, 282–88 (6th Cir. 2010) (holding that a subscriber has a reasonable expectation of privacy in the contents of emails stored with, or sent or received through, a commercial Internet service provider).

103. Riley v. California, 134 S. Ct. 2473 (2014). *Riley* is discussed *infra* at notes 172–184.

104. United States v. Stanley, 753 F.3d 114, 124 (3d Cir. 2014) (holding that the defendant had no reasonable expectation of privacy in the fact that he was making unauthorized use of a neighbor's wireless network).

105. United States v. Graham, 824 F.3d 421, 424 (4th Cir. 2016) (en banc) (holding that the government did not violate the Fourth Amendment by obtaining historical cell-site location information from the defendants' cell phones without a warrant). Cell-site location information "indicate[s] which cell tower—usually the one closest to the cell phone—transmitted a signal [when people use] their cellphones to make and receive calls and texts." *Id.* Thus, cell-site location information can be used to place the owner of a cell phone near the scene of a crime.

government devices deceptively posing as cell towers to trick mobile phones into connecting and transmitting data.[106] Consider just the question of location data, a question that should be relatively easy because the Supreme Court held unanimously in 2012 that a Fourth Amendment search occurred when a physical GPS tracker was placed on a suspected drug dealer's car pursuant to a warrant whose time and place scope was exceeded.[107] Yet, beyond physical GPS trackers, there are many other sources of location data that have or will produce Fourth Amendment issues, including cell-site location data,[108] phone GPS chip location data,[109] automated license plate readers,[110] photographic geotags, smartphone apps, and even personal fitness trackers embedded in watches or shoes. Even these forms of data raise relatively simple questions compared to issues of data encryption, cell phone security, the use of warrants to obtain globally stored cloud data, or whether cloud providers can tell their customers that their data has been seized pursuant to a warrant.[111]

We are in the midst of yet another lag that implicates communications privacy, a lag made all the more bewildering by the fact that the technologies carrying our communications data are the same ones carrying other kinds of data. As the courts wade into this technical and contextual mess, one particular Fourth Amendment rule promises to offer an easy answer to these questions in favor of government access and doctrinal clarity. It is to this rule that we now turn.

---

106. *See* United States v. Patrick, 842 F.3d 540, 542–44 (7th Cir. 2016) (discussing cell-site simulators but ultimately declining to address the question of whether their use constitutes a "search" because the government conceded that it did for purposes of this case); State v. Andrews, 134 A.3d 324, 339–52 (Md. Ct. Spec. App. 2016) (holding that the government's use of use of cell-site simulators invaded the defendant's reasonable expectation of privacy and was not governed by the Third-Party Doctrine). *See generally* Cyrus Farivar, *Warrantless Stingray Case Finally Arrives Before Federal Appellate Judges*, ARS TECHNICA (Jan. 29, 2016, 6:00 AM), http://arstechnica.com/tech-policy/2016/01/warrantless-stingray-case-finally-arrives-before-federal-appellate-judges/ (discussing the *Patrick* appeal); Cyrus Farivar, *Appeals Court: No Stingrays Without a Warrant, Explanation to Judge*, ARS TECHNICA, (Mar. 31, 2016, 8:29 AM), http://arstechnica.com/tech-policy/2016/03/appeals-court-no-stingrays-without-a-warrant-explanation-to-judge/ (discussing the *Andrews* decision).

107. United States v. Jones, 132 S. Ct. 945 (2012). *Jones* is discussed *infra* at notes 157–171.

108. Ford v. State, 477 S.W.3d 321, 330–35 (Tex. Crim. App. 2015). For an explanation of cell-site location data, see *supra* note 105.

109. United States v. Myles, No. 5:15-CR-172-F-2, 2016 WL 1695076, at *6–7 (E.D.N.C. Apr. 26, 2016). Whereas cell-site location data shows a record of where the cell phone has been in the past, GPS chip location data "shows where the phone is presently located." *Id.* at *6.

110. *See* ACLU Found. of S. Cal. v. Superior Court, 186 Cal. Rptr. 3d 746 (Cal. Ct. App. 2015) (seeking records generated by Los Angeles's automatic license plate readers under the California Public Records Act), *review granted*, 352 P.3d 882 (Cal.).

111. Complaint for Declaratory Judgment, Microsoft Corp. v. U.S. Dep't of Justice, No. 2:16-cv-00538 (W.D. Wash. Apr. 14, 2016), 2016 WL 1464273.

II. OUR TINY THIRD-PARTY DOCTRINE

No discussion of the Fourth Amendment status of data in our information society can occur without an invocation of the Third-Party Doctrine, the notion that information shared with third parties loses its Fourth Amendment protection. The Third-Party Doctrine has been much criticized, but it stubbornly refuses to go away. The question of the viability of the Third-Party Doctrine is one of the most important questions of civil liberties of our time. At stake is not merely what level of Fourth Amendment protection applies to metadata, or even to privacy, but in a very real sense, what the power relationship will be between Americans and their government in the digital age. We are living in an information society, and information has been and will continue to be power. We should therefore tread carefully when presented with the government's argument that data held by third parties lacks constitutional protection, lest we repeat the mistakes of *Olmstead* on a far greater scale.

This Part takes a critical look at the Third-Party Doctrine, and looks closely at its origins and its interpretations. Although there is already a literature on the Third-Party Doctrine, I intend to make three contributions to the scholarly and policy debate. First, as the preceding Part has set up, the importance of the Third-Party Doctrine means that it is essential to look at the Doctrine in the broadest historical context. Second, I offer a close examination of the development of the doctrine at the Supreme Court in the 1970s, and show that the Doctrine was not and should not be anything like as broad as its government proponents have suggested. When we look at the origins of the Third-Party Doctrine, we can see that it is much narrower than the blunt idea that "what is shared is unprotected." It turns out that our Third-Party Doctrine can be viewed instead as a fairly limited doctrine, much narrower than its proponents and many of its critics have assumed. I thus offer a reading of the cases that presents what I call our "Tiny Third-Party Doctrine." Third, I offer a path forward for the law in this bewilderingly complex area of technology and constitutional civil liberties. In recent cases, the Supreme Court has offered some indications that it is taking the project of the translation of the Fourth Amendment into the digital environment seriously. I hope to offer a path forward along lines consistent with those indications.

A. Origins of the Doctrine

In a recent briefing to Members of Congress, the Congressional Research Service described the Third-Party Doctrine as follows:

> In these cases, the Court held that people are not entitled to an expectation of privacy in information they voluntarily provide to third parties. This legal proposition, known as the third-party doctrine, permits the government access to, as a matter of Fourth Amendment law, a vast amount of information about individuals, such as the websites they visit; who they have emailed; the phone numbers they dial; and their utility, banking, and education records, just to name a few.[112]

Consider, for a moment, the breadth of the suggestion that "information you voluntarily provide to third parties" is not protected by the Fourth Amendment. In a digital age in which technology companies hold vast repositories of personal data on behalf of their customers, that is close to all the personal information that exists. Next, consider that this reading of the law is the one being provided to Congress, which has been stalling on a long-overdue reform of the Wiretap/Electronic Communications Act for years, even as states like California have amended their surveillance statutes to require warrants before emails and cloud documents may be searched or seized by the government.[113] Because the constitutional rule is a baseline from which statutory rules may only depart in a more rights-protective direction, understanding what the Fourth Amendment requires is essential even were Congress to attempt meaningful surveillance law reform.

The Third-Party Doctrine rests upon a simple two-part intuition— (1) the Fourth Amendment only requires the government to get warrants for things that are private, and (2) information I share with others is no longer private, so it does not require a warrant. The Third-Party Doctrine has its origins in this idea in the context of person-to-person conversations. Before *Katz*, a line of cases established the principle that people who confide their crimes to the wrong people have assumed the risk of betrayal, whether their false confidant is a police informant,[114] a "jailhouse snitch," or an undercover law enforcement officer.[115]

For example, in *Hoffa v. United States*,[116] the Court upheld the

112. RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE (2014).

113. *See* California Electronic Communications Privacy Act, CAL. PENAL CODE §§ 1546–1546.4 (West 2017). *See generally* Press Release, ACLU of Northern California, In Landmark Victory for Digital Privacy, Gov. Brown Signs California Electronic Communications Privacy Act into Law (Oct. 8, 2015), https://www.aclunc.org/news/landmark-victory-digital-privacy-gov-brown-signs-california-electronic-communications-privacy. *See also infra* notes 213–214 and accompanying text.

114. On Lee v. United States, 343 U.S. 747 (1952); Hoffa v. United States, 385 U.S. 293 (1966).

115. Lewis v. United States, 385 U.S. 206 (1966).

116. 385 U.S. 293.

conviction of a man who confided in an informant his plans to bribe jurors in another criminal case in which he was a defendant. The Court reasoned that the informant, who was in the hotel suite by invitation, had every right to listen to the incriminating conversation he had with the defendant, Jimmy Hoffa. Hoffa's error, according to the Court, was that he "was not relying on the security of the hotel room; he was relying upon his misplaced confidence that [the informant] would not reveal his wrongdoing."[117]

Similarly, in *United States v. White*,[118] decided after *Katz*, the Court upheld the conviction of a man who was convicted based upon statements made to a government informant who was wearing a radio transmitter or "wire." The Court found it relevant that a warrant would not have been necessary if the conversation had not been recorded, and it did not change the result when the wire produced a "more accurate" version of the conversation than the recollections of the informant.[119] These cases, many of which involved organized crime, stand for the proposition that criminals have no reasonable expectation of privacy that their associates will not betray them, whether or not the associates are secretly recording the criminals. In other words, if a person chooses poorly in her third party confidantes, the Fourth Amendment does not protect her.

B. Miller and Smith

Reasonable people (and societies) can disagree about the merits of the misplaced trust rule in the informant cases.[120] However, any disagreement on that score is tangential to the real stakes in the Third-Party Doctrine context. The controversial application of the Third-Party Doctrine is not its application to occasional in-person conversations, but to large-scale systems of records held by trusted businesses, agents, and intermediaries. This extension of the doctrine beyond person-to-person communications was enabled by two Supreme Court cases from the 1970s. In *United States v. Miller*[121] and *Smith v. Maryland*,[122] the Court extended the rationale of *Hoffa* and *White* to customer records held by banks and telephone

117. *Id.* at 302.
118. 401 U.S. 745 (1971).
119. *Id.* at 752–53.
120. In fact many do. Given its history of secret police terror under the Gestapo and the Stasi, modern German constitutional law sharply restricts the use of undercover policing and secret surveillance. *See* Jacqueline E. Ross, *The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany*, 55 AM. J. COMP. L. 493 (2007).
121. 425 U.S. 435 (1976).
122. 442 U.S. 735 (1979).

companies. Many courts and commentators have understood *Miller* and *Smith* to have extended the misplaced trust rule to all paper or digital documents held by third parties.[123] As one commentator explains the issue, "The third-party doctrine holds that if a citizen shares information with a third party, then she has no Fourth Amendment complaint if that third party subsequently shares that information with the government."[124] But as we will see, a close examination of the cases reveals that they were actually much more carefully limited than that, and that this broad theory of the Third-Party Doctrine rests on a narrower and shakier foundation than many have assumed.

Like *Olmstead* many years before, *Miller* involved an investigation into an illegal liquor business, in this case a Georgia moonshine conspiracy.[125] Mitch Miller was convicted based upon copies of checks, deposit slips, and other financial records that the police had subpoenaed from his local bank. The Supreme Court rejected Miller's argument that the police violated his Fourth Amendment rights when they used only a subpoena based upon relevance rather than a warrant based upon probable cause. Several factors contributed to this determination. First, most of the seized materials were not Miller's "private papers" within the meaning of the Fourth Amendment, but rather belonged to the bank.[126] Second, although the original checks and deposit slips had belonged to Miller in the past, the Court concluded that he lacked a reasonable expectation of privacy in them because they were not "confidential communications" but rather negotiable instruments that were part of commercial transactions. Relevant to this conclusion was the existence of the Federal Bank Secrecy Act, which despite its name required banks to keep records of that sort in order to assist in criminal, tax, and other investigations.[127] Also relevant was the Court's interpretation of *Katz* that the reasonableness inquiry required it to "examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents."[128] Third, the court concluded, relying on the misplaced trust cases, that

123. *See, e.g.*, Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SECURITY L. & POL'Y 247 (2016); Brief of *Amici Curiae* Brennan Ctr. for Justice et al., in Support of Defendant-Appellant and Reversal at 8, United States v. Moalin, No. 13-50572 (9th Cir. Nov. 5, 2015), 2015 WL 6966514, at *8, https://epic.org/amicus/fisa/215/moalin/BJC-EPIC-et-al-Amicus-Brief.pdf.

124. Gray, *supra* note 19, at 431 n.26.

125. *Miller*, 425 U.S. at 437.

126. *Id.* at 440–41.

127. *Id.* at 442–43 (citing 12 U.S.C. § 1829b(a)(1)).

128. *Id.* at 442.

> [t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[129]

This last statement, broader perhaps than was necessary to decide the case, has been the most controversial, and provides the strongest support for the broad view of the Third-Party Doctrine. Indeed, as William Stuntz has explained, "In terms of privacy protection, *Miller* seems ridiculous," but bank records are also necessary to the process of financial investigations in the modern regulatory state.[130]

Miller may well be "ridiculous," but even on its own terms, to understand *Miller* we must also understand its limitations. The documents seized in that case were mostly not Miller's, but were the bank's, and even his slips and checks had been turned over to the bank for its commercial purposes. The Court was careful to note that the case did not involve any "confidential communications,"[131] thereby sidestepping any linkage with free expression or any broad conflict with privacy expectations. Indeed, the existence of a federal statutory scheme requiring the retention of this kind of commercial data also seemed to be an important factor in the Court's analysis. Finally, unlike a telephone company or an internet service provider, banks are not intermediaries.[132] Banks use their own bank records for their own, highly regulated purposes. (In the 1970s in particular, what banks held in trust was not so much their customers' information but their money.) From these perspectives, the invocation of the misplaced trust cases at the end of the *Miller* analysis seems unnecessary, almost gratuitous, and was perhaps a rhetorical flourish to stave off the two dissenting opinions of Justices Brennan and Marshall.[133] After all, the contents of telephone calls and of locked desks in homes are also highly useful to criminal investigations, but there was no suggestion whatsoever in *Miller* that their constitutional protections were up for reexamination, as the Court was

129. *Id.* at 443 (citation omitted).
130. Stuntz, *supra* note 20, at 444–45.
131. *Miller*, 425 U.S. at 442.
132. This is a point made by Judge Boggs in *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). *Warshak* is also briefly discussed below in the text accompanying note 155.
133. *See Miller*, 425 U.S. at 447 (Brennan, J., dissenting); *id.* at 455 (Marshall, J., dissenting).

operating solidly within the *Katz* regime rather than at odds with it.

Miller may have been readily distinguishable from *Katz*'s special protection for confidential communications, but the Court's next case came a little closer to the contents of phone calls. *Smith v. Maryland*[134] asked whether a warrant was required before the police could seize the phone numbers dialed by the customer of a telephone company. The Court again held that a warrant was not required, but as in *Miller*, it was careful to distance itself from confidential communications.[135] *Smith* is a curious case on which to base a broad theory of the Third-Party Doctrine, since it arose from a single purse-snatching and harassment by a petty criminal.[136] Michael Lee Smith had stolen Patricia McDonough's purse on the streets of Baltimore one day in 1976, and then driven off in his 1975 Monte Carlo.[137] McDonough began receiving obscene harassing phone calls from a man who claimed to be the robber. During one of the calls, he told her to step onto her front porch, and when she did so, she saw the Monte Carlo driving slowly past her house.[138] McDonough noted the license plate, which the police traced to Smith. The police then installed (without first getting a warrant) an analog device called a "pen register" at the phone company switchboard to record the numbers Smith dialed from his home phone. One of those numbers turned out to be McDonough's, and on the basis of this and other evidence, Smith was arrested and convicted of robbery.[139]

The Supreme Court upheld Smith's conviction over his Fourth Amendment challenge to the warrantless installation of the pen register. The Court took painful care to distinguish pen registers (which record only the numbers dialed) from wiretaps (which obtain the contents of a telephone call), and ruled that telephone users lack a reasonable expectation of privacy in the telephone numbers they dial.[140] This was the case, the Court believed, because "we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone user realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed."[141] Moreover, most people were aware that the phone company knew the phone numbers they dialed because the phone company frequently recorded them

134. 442 U.S. 735 (1979).
135. *See id.* at 741.
136. *Id.* at 737.
137. *Id.*
138. *Id.*
139. *Id.*
140. *Id.* at 741–42.
141. *Id.* at 742.

for a variety of legitimate purposes, including long-distance billing and fraud and harassment detection.[142] Moreover, even if Smith had held a contrary belief, the Court held that this belief was unreasonable because of *Miller* and the misplaced trust cases.[143]

In reaching this conclusion, the Court accepted a brilliant piece of argumentative framing by Stephen Sachs, the young Maryland attorney general who argued the State's case. In his briefs and at oral argument, Sachs built his case around two essential elements in order to secure what he believed to be a narrow victory for the state. The first of these was the hard distinction between contents and phone numbers; what current usage would term "metadata." Sachs opened his oral argument by offering an explanation of the limited incursion into privacy that a pen register was capable of:

> [T]he point I'd like to make, Your Honors, is that it hears no sound. It captures no words uttered into the mouth piece, as this Court phrased it in *Katz*. It captures no content. It achieves no communication, other than the limited communication between the user and the phone company itself. It has been defined by Congress, indeed, by its exclusion from the requirements of Title 3 as not to be a communication. It doesn't disclose if the call is completed. It doesn't reveal who the caller is. It doesn't say if the number was busy. It doesn't say who the parties are and it doesn't tell the duration of the call.[144]

Sachs' second framing point was even more effective. He reminded the Justices of their own usage of older-model telephones before automated dialing, in which every caller spoke with an operator who connected their line to the phone which they wished to call. Sachs explained that

> [t]here is no reasonable expectation of privacy and I would go so far as to say that, in a great many cases, although it's improvable, inherently, there is frequently not a subjective expectation of privacy. The user of a telephone knows to go back to the days, however long ago they may be, to go back to the days when this was not done mechanically but done by human communication. One said to the operator Millie, "Millie, get me George" or "get me Sam, down at the

142. *Id.* at 742–43.

143. *Id.* at 743–45.

144. Transcript of Oral Argument at 27:02, Smith v. Maryland, 442 U.S. 735 (1979) (No. 78-5374), https://apps.oyez.org/player/#/burger6/oral_argument_audio/16917.

> grocery store." All that's done now, Your Honor, is that we communicate and impart that information, the number we wish to achieve, to a phone company who has—who is not statutory [sic] barred from disclosing that information to third parties, unlike communication between the party calling and the party called.[145]

Sachs' argument was so persuasive that the Court expressly accepted this argument in its opinion, referring to the relevant portions of the transcript of oral argument in which Smith's lawyer had conceded Sachs' claim that "if [Smith] had placed the calls through an operator, he could claim no reasonable expectation of privacy. We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate."[146]

The relevance of this point for the Third-Party Doctrine is the incredible narrowness of the holding in *Smith*. Sachs did not need the Court to rule broadly about the Fourth Amendment status of records or documents held by third parties, nor was the Court so inclined. As attorney general, his interest was solely in upholding the conviction of a robber who had terrorized his victim using the telephone, which he accomplished. Accordingly, he reduced his argument to the narrow claims that the government had merely obtained a phone number, and that phone numbers used to be told orally to the phone company's operator. Sachs explained this point in an interview some thirty-six years later, noting:

> It was a routine robbery case. The circumstances are radically different today. There wasn't anything remotely [like] a massive surveillance of citizens' phone calls or communications . . . . To extend it to what we now know as massive surveillance, in my personal view, is a bridge too far. It certainly wasn't contemplated by those involved in *Smith*.[147]

From this perspective, it becomes clear that as a justification for the broad view of the Third-Party Doctrine, *Miller* and *Smith* are woefully deficient. Each dealt with very narrow contexts, and each was in its way something of an exceptional case. Even together, they do not justify a broad view of the Third-Party Doctrine. The most that they can support on their own terms is something of a "Tiny Third-Party Doctrine."

---

145. *Id.* at 27:55.

146. *Smith*, 442 U.S. at 744–45 (citation omitted).

147. David Kravets, *How a Purse Snatching Led to the Legal Justification for NSA Domestic Spying*, WIRED (Oct. 2, 2013, 6:30 AM) (brackets in original) (internal quotation marks omitted), https://www.wired.com/2013/10/nsa-smith-purse-snatching/.

The strongest argument that *Miller* and *Smith* could support something other than a Tiny Third-Party Doctrine is their invocation of the misplaced trust cases such as *Hoffa* and *White*. But the misplaced trust cases are not necessary to resolve either case. *Miller* involved bank records that either belonged to the bank or had been turned over to the bank for transactional purposes, and the entire banking industry was in any event subject to the comprehensive federal record-keeping requirements of the somewhat misleadingly named Bank Secrecy Act.[148] *Smith*, similarly, involved a single piece of non-content information—a telephone number—that Sachs was keen to distinguish from the contents of a phone call that were so strongly protected in *Katz* and its progeny.[149] In so doing, he was resting his argument on a very old distinction between the contents of a communication and information necessary only to get those contents to the correct address. The distinction between contents and address information in the constitutional law of communications privacy goes all the way back to *Ex parte Jackson*, in which the Court drew a distinction between the inside of a sealed package (which receives the full protection of the Fourth Amendment) and its exterior (which does not).[150] This distinction survives today, which is why the government needs a warrant to read mail in a paper letter, but does not need one to read a postcard, which has its contents on the outside of its "envelope," right next to the address information.[151]

Moreover, neither *Miller* nor *Smith* implicated the linkages to free expression that have existed in the law of searches and seizures since the colonial period. Particularly in the 1970s, when even commercial advertising was held to be outside the protection of the First Amendment, banking was seen as merely "commercial" and thus entitled to lower Fourth Amendment protection as well.[152] The Supreme Court has continued to hold that commercial activities receive lower Fourth Amendment protection,[153]

148. *See supra* notes 126–127 and accompanying text.

149. *See supra* note 144 and accompanying text.

150. *Ex parte* Jackson, 96 U.S. 727, 733 (1878) ("[A] distinction is to be made between different kinds of mail matter,—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. Letters and sealed packages of this kind 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. The 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.").

151. *See, e.g.*, United States v. Van Leeuwen, 397 U.S. 249, 251 (1970).

152. *See* Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1217–19 (2005).

153. *See* Minnesota v. Carter, 525 U.S. 83, 90 (1998) ("Property used for commercial purposes is treated differently for Fourth Amendment purposes from residential property. 'An expectation of privacy

especially in highly regulated industries.[154]

Nevertheless, the Tiny Third-Party Doctrine that resulted from *Miller* and *Smith* has not stopped enterprising government lawyers from inflating it into something much bigger. The Justice Department, for example, has never conceded that email is not subject to the Third-Party Doctrine, even though that argument was defeated in the Sixth Circuit case of *United States v. Warshak*,[155] which essentially brought email within the warrant protection of *Ex parte Jackson*. Nevertheless, because the government did not seek Supreme Court review of that decision, it remains open to argue that email contents are not protected by the Fourth Amendment outside the Sixth Circuit states of Kentucky, Michigan, Ohio, and Tennessee. Most importantly, however, the fact remains that when looked at closely and in context, *Miller* and *Smith* support at best only a Tiny Third-Party Doctrine.

C. The Roberts Court's Third-Party Doctrine

While the lower federal courts are struggling with whether and how to close the Fourth Amendment lag with respect to data, the Roberts Court has begun to send a strong message that it intends to ensure that the valuable protections for communications and other forms of privacy in the physical world will be extended to digital technologies. In two recent cases, solid majorities of the Court have hinted that they are interested in closing the digital lag. At the same time, the Justices have acknowledged that the task of protecting essential civil liberties in a digital society will be a challenging one.[156]

In the first of these cases, *United States v. Jones*,[157] the Court unanimously rejected the idea that the government could deploy a GPS tracker without a valid warrant. All nine Justices agreed that a physical GPS tracker placed on a suspected drug dealer's car for a month without a valid warrant violated his Fourth Amendment rights, but in a series of opinions disagreeing about the rationale for this conclusion, they debated what a digital Fourth Amendment might look like. Writing for a majority of five Justices, Justice Scalia ruled narrowly that because the physical placement

---

in commercial premises, however, is different from, and indeed less than, a similar expectation in an individual's home.'" (quoting New York v. Burger, 482 U.S. 691, 700 (1987))).

154. Dow Chem. Co. v. United States, 476 U.S. 227, 236 (1986) ("The intimate activities associated with family privacy and the home and its curtilage simply do not reach the outdoor areas or spaces between structures and buildings of a manufacturing plant.").

155. 631 F.3d 266, 287–88 (6th Cir. 2010).

156. City of Ontario v. Quon, 560 U.S. 746, 759–60 (2010).

157. 132 S. Ct. 945 (2012).

of a tracker on a car would have constituted a trespass under eighteenth-century law, the result should be no different in the twenty-first, and a valid warrant should have been procured.[158] Because this would have been an easy case under eighteenth-century law, he concluded, there was no need to get into the *Katz* analysis of whether Jones had an expectation of privacy, reasonable or otherwise.[159]

Concurring on behalf of the other four Justices, Justice Alito rejected the idea that the technicalities of eighteenth-century law are the appropriate way to think about location privacy in a digital age.[160] The Court's fixation on the placement of the physical tracker on Jones's car, he argued, fixated on a "trivial" trespass, while leaving lower courts with no guidance on the much more important problem of privacy rights against GPS location tracking by electronic means (including by using location data held by phone or app companies about their customers).[161] Justice Alito first noted a serious problem with *Katz*—not only is it circular because expectations are based on law that is based upon expectations, but the very idea of an expectation of privacy becomes problematic at times in which information technology is in flux.[162] Second, he suggested that the proper solution to problems like these may ultimately be specific legislative rules operating above a constitutional floor (as had happened in the wiretapping context).[163] Turning to the question of whether Jones' expectation of privacy was objectively reasonable, he concluded that while "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable . . . the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[164] This was because of the long-standing societal expectation that the police "would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[165] And though there must be a line between short-term and long-term location monitoring, the government had far exceeded it in this case.[166]

158. *Id.* at 949, 953–54. In the case, the police had obtained a warrant before installing the tracker, but it had permitted the installation of a tracker in the District of Columbia within ten days, whereas the actual installation happened in Maryland on the eleventh day. *Id.* at 948.

159. *Id.* at 953–54.

160. *Id.* at 957–59 (Alito, J., dissenting).

161. *Id.* at 961.

162. *Id.* at 962.

163. *Id.* at 962–63.

164. *Id.* at 964 (citation omitted).

165. *Id.*

166. *Id.*

The most interesting opinion in *Jones* was written by Justice Sotomayor. While she provided the fifth vote for Justice Scalia's opinion of the Court, her analysis was similar to that of Justice Alito, but went much further. At the outset, Justice Sotomayor explained that location surveillance implicates serious Fourth Amendment concerns because location reveals highly sensitive information. As she put it eloquently,

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. The Government can store such records and efficiently mine them for information years into the future. And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility."[167]

Justice Sotomayor went further and made the linkage between the sensitivity of GPS data and intellectual privacy explicit:

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society."[168]

Finally, as if that were not enough of a bold statement about the importance of digital civil liberties, Justice Sotomayor expressly indicated an interest in revisiting the Third-Party Doctrine to bring it back in line with the long-standing Fourth Amendment commitments to civil liberties that are being imperiled by broad government assertions of access to digital records.[169] She argued that it was necessary to revisit the premise that "an individual has no reasonable expectation of privacy in information voluntarily

---

167. *Id.* at 955–56 (Sotomayor, J., concurring) (citations omitted) (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)).

168. *Id.* at 956 (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

169. *Id.* at 957.

disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[170] Noting that this information included books read, emails sent, and phone numbers dialed (the fact pattern of *Smith v. Maryland*), Justice Sotomayor doubted whether, in determining expectations of privacy,

> people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. 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.[171]

The second Roberts Court digital Fourth Amendment case is *Riley v. California*,[172] two consolidated cases in which the government sought to use the occasion of a search incident to a valid arrest to engage in the warrantless search of mobile phones found on the person of the defendants. The consolidated cases included one in which the government seized an old-style "flip phone," and one in which it seized a full-featured modern "smartphone."[173] There is settled Fourth Amendment precedent that police making a valid arrest do not need a warrant to search the person of an arrestee in order to protect themselves and to preserve evidence.[174] In one prior case, the Court had even upheld the search of the contents of a container (a cigarette packet) that was roughly the same physical size as a modern smartphone.[175] Unlike *Jones*, in which the Court did not need to reach the harder issue of electronic searches because the GPS tracker was physical, *Riley* required the Court to consider alleged infringements of the Fourth Amendment that were digital rather than physical.

As in *Jones*, the Court was unanimous, holding that the Fourth Amendment protects the contents of a mobile phone from warrantless search. But unlike *Jones*, the Court's methodology was not based upon ancient precepts of trespass law, but on the capabilities of modern digital

170. *Id.* (citations omitted).
171. *Id.*
172. 134 S. Ct. 2473 (2014).
173. *Id.* at 2480–81.
174. *Id.* at 2482–83.
175. United States v. Robinson, 414 U.S. 218 (1973).

technologies and their relationship to our cherished civil liberties.[176] In this methodological respect, Chief Justice Roberts's opinion for the Court was more like Justice Sotomayor than Justice Scalia in *Jones*, and more like Justice Brandeis than Chief Justice Taft in *Olmstead*. In fact, there were striking methodological and interpretive similarities between the Chief Justice's majority opinion in *Riley* and Justice Sotomayor's concurrence in *Jones*. The Court's opinion in *Riley* began with an overview of the search-incident-to-arrest doctrine, before turning to the issue of smartphones with the observation that smartphones have rapidly become ubiquitous in our society, and that the "digital content" on phones called for a different balance that respects their unique features.[177] These included both qualitative and quantitative differences from the technologies that prior cases had examined. Cell phones, the Court explained, are "minicomputers" with an "immense storage capacity" that happened to also function as telephones, as well as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[178] From this premise, the Chief Justice provided a metaphor for the importance of cell phones that seems destined to remain in Fourth Amendment law for some time:

> Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so. And if they did, they would have to drag behind them a trunk of the sort held to require a search warrant in *Chadwick*, rather than a container the size of the cigarette package in *Robinson*.[179]

Even more interesting, in discussing the storage capacity of modern smart phones at length, the Chief Justice indicated that cloud computing requires constitutional protection. Noting that many phone users (even sophisticated ones) often cannot tell whether data on their phone resides on its local flash memory or in the cloud, the opinion hinted that the distinction between the two kinds of storage "generally makes little difference" for Fourth Amendment purposes.[180] Moreover, in addressing the government's argument (perhaps prompted by Third-Party Doctrine concerns) that to

176. *Riley*, 134 S. Ct. at 2488–91.
177. *Id.* at 2482–85, 2489–91.
178. *Id.* at 2489.
179. *Id.* (citation omitted).
180. *Id.* at 2491.

avoid reaching cloud-stored data, it could develop "'protocols to address' concerns raised by cloud computing," the Court's opinion somewhat colloquially responded:

> Probably a good idea, but the Founders did not fight a revolution to gain the right to government agency protocols. The possibility that a search might extend well beyond papers and effects in the physical proximity of an arrestee is yet another reason that the privacy interests here dwarf those in *Robinson*.[181]

To be clear, *Riley* was not a Third-Party Doctrine case, but its reference to cloud-stored documents begs a very important question for the future of digital Fourth Amendment rights: If the broad view of the Third-Party Doctrine applies to cloud-stored documents, why is the Court so concerned about protecting these documents under the Fourth Amendment? The Court's opinion in *Riley* is not explicit, but its general methodological approach suggests that not merely Justice Sotomayor but also the Chief Justice and other members of the Court do not believe that the Third-Party Doctrine actually reaches documents stored in the cloud by private companies on behalf of their customers. The logical implications of this conclusion would go beyond email to browsing history, synced bookmarks, address books, the location data implicitly at issue in *Jones*, and browsing and other reading histories, at a minimum. It would probably reach other kinds of sensitive data mentioned regularly in these cases like photographs[182] and financial data[183] as well. As the Court concluded, "Privacy comes at a cost," and in the context of personal information in digital form, one of those costs to law enforcement seems to be that it will increasingly be required to obtain a warrant to access it.[184] The Supreme Court's digital Fourth Amendment cases suggest that a strong majority of the Court is interested in closing the technological lag in the Fourth Amendment context.

III. PRIVACY IN THE CLOUD

Closing the lag between Fourth Amendment doctrine and digital technologies in the age of cloud computing and big data will not be easy. It

181. *Id.*

182. *Id.* at 2493 ("But the fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery.").

183. *Id.* ("The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years.").

184. *Id.*

will be particularly challenging, as the Roberts Court has noted in its digital Fourth Amendment cases, to protect civil liberties while our technologies are in a state of rapid development. The great virtue of the Third-Party Doctrine is its clarity, and a digital Fourth Amendment that moves beyond that doctrine's oversimplification must deal with the problem of complexity. For better or for worse, the problem of Fourth Amendment privacy in the age of the cloud will require a more nuanced solution, at least if we wish to preserve an effective balance between state power and civil liberties.

In this Part, I offer four observations about how to resolve this problem, and propose a new way of looking at the privacy problems implicated by data held by others. First, I argue that the broad view of the Third-Party Doctrine is manifestly unsuited to the protection of our digital civil liberties. Second, I compare my approach to Orin Kerr's "Equilibrium-Adjustment Theory" of the Fourth Amendment, and contend that in contrast to Kerr's approach, when it comes to the question of closing lags in the civil liberties context, we should focus on those questions of civil liberties rather than on questions of state access to data. Third, I explain that the process of interpretation of the Fourth Amendment is inescapably normative, and I argue that principles of intellectual privacy offer a useful guide to the normative project of translating Fourth Amendment values in a way that closes the technological lag. Fourth, I explain that no matter how we interpret the Fourth Amendment, any approach to the protection of digital civil liberties will need to account for the important role that intermediaries play in the practices of data processing and protection. In a digital world, trusted intermediaries are very different from merely being "third parties," and whichever path our law takes, it must take this fact into account. There are, of course, multiple paths that Fourth Amendment law could take in the future to grapple with these problems. My purpose is not so much to call for a particular solution as to highlight the considerations I believe should apply as we translate the Fourth Amendment's text into workable doctrine for the cloud age in a way that is practical but also protects the traditions and normative commitments of our hard-won civil liberties.

A. Third-Party Doctrine Balance

At the outset, it is important to acknowledge plainly that the broad reading of the Third-Party Doctrine is manifestly unsuited to the project of translating our enduring values into a digital future. The intuition underlying the broad Third-Party Doctrine is that when we put information "out there," we no longer can treat it as private. Superficially, there is a certain amount of sense in this logic: if you tell someone your secrets, you do not get to

complain when they betray your misplaced trust. This doctrine had obvious application in an analog world in which our documents usually remained in our homes, we read exclusively on paper, and the phone company recorded just the phone numbers we dialed but not the contents of conversations themselves. As we saw, in *Smith* the Supreme Court seems to have been persuaded by Stephen Sachs's argument to the effect that, in the old days, a caller had to tell a human operator the recipient's number.[185] The Court declined to reach a different result just "because the telephone company has decided to automate."[186] In that case, too, the stakes for civil liberties seemed small, while the defendant, a purse-snatcher turned stalker, was clearly guilty.

But in a digital world, the simple intuition of misplaced trust applied universally threatens the end of the Fourth Amendment as we know it. Stripped out of the narrow logic that was persuasive in a pair of peculiar 1970s cases, the doctrine has been used to support, among other things, warrantless dragnet surveillance by the National Security Agency,[187] the warrantless collection of cell-phone GPS and other forms of non-content data,[188] and the warrantless use of "stingrays" or cell-site simulators.

While this analogy is a simple one, it is not one that stands up to close analysis. What was a close case for analog bank records or the telephone numbers dialed by a single criminal suspect leads to a radically different result in a digital society in which the typical social practices of citizens and consumers are inextricably intertwined with personal data held on their behalf by private companies. This is the case whether we are considering browsing habits, location data, emails, or an uncountable number of other data sets.

To claim that these data collection schemes are equivalent to their analog predecessors is unconvincing. Today, because so many technologies work by transmitting and storing our data, the civil-liberties implications of the Third-Party doctrine are vastly greater. If we accept the logic of the Third-Party Doctrine for our current data practices, then it would logically follow that future data sets would also lose Fourth Amendment protection.

If we follow this line of logic, it might have no conceivable stopping point. The broad view of the Third-Party Doctrine would presumably also cover any data captured by the new wave of Internet of Things technologies

185. Smith v. Maryland, 442 U.S. 735, 744–45 (1979); *supra* notes 145–146.

186. *Smith*, 442 U.S. at 745.

187. *E.g.*, Klayman v. Obama, 805 F.3d 1148 (D.C. Cir. 2015) (Kavanaugh, J., concurring in denial of rehearing en banc).

188. United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (en banc).

arriving or on the horizon—Internet-connected televisions, light switches, washing machines, electrical meters, Barbie dolls, self-driving cars, and even toilets.[189] Consider in this regard the rise of Internet of Things appliances with voice interfaces, whether Apple TV, the Amazon Alexa, or Samsung's new line of televisions. These technologies work by listening to our domestic conversations for keywords so that they can immediately respond to our wishes. The most efficient way to perform the voice recognition on which this technology rests is to send the data to be processed in the cloud (which of course means the data centers owned or leased by the company). This is so for the simple reason that a data center holds vastly more computing power than that which can fit into a small home appliance.[190]

One possible solution to this problem would be to take a page from *Ex parte Jackson* and divide the world of data up into "content" and "envelope" data. Recall that in *Jackson*, the contents of a letter were protected, but the words written on the outside of the envelope were not.[191] This is a distinction that has persisted in wiretapping law, embodied in the Electronic Communications Privacy Act's distinction between "contents" (which usually require a warrant to obtain) and transactional data (which requires a lower showing).[192] The government has used this argument in the national security context with the now-famous distinction between "content" and "metadata."[193] This distinction may have made sense at the time of *Jackson*, where the typewriter was cutting-edge technology, but it does not work today.

The content/envelope/metadata distinction is unsatisfying in the digital

189. *See* Andrew Meola, *What is the Internet of Things (IoT)?*, BUS. INSIDER (Dec. 19, 2016, 2:11 PM), http://www.businessinsider.com/what-is-the-internet-of-things-definition-2016-8; Mike Murphy, *Internet of Too Many Things: 18 Things That Have No Business Being Connected to the Internet*, QUARTZ (Dec. 3, 2015), https://qz.com/563952/18-internet-of-things-devices-that-have-no-business-being-connected-to-the-internet/.

190. Tim Moynihan, *Alexa and Google Home Record What You Say. But What Happens to That Data?*, WIRED (Dec. 5, 2016, 9:00 AM), https://www.wired.com/2016/12/alexa-and-google-record-your-voice/.

191. *See supra* notes 150–151 and accompanying text.

192. *Compare* 18 U.S.C. § 2518 (2012) (establishing detailed warrant requirements for intercepting the contents of an electronic communication, including a complete factual statement, the absence of less invasive procedures, probable cause, and automatic termination), *with id.* § 2703(c)–(d) (allowing the government to compel disclosure of transactional data by administrative subpoena or by court order upon a showing of "specific and articulable facts showing . . . reasonable grounds to believe that the . . . information sought [is] relevant and material to an ongoing criminal investigation").

193. *See* ACLU v. Clapper, 785 F.3d 787, 822 (2d Cir. 2015) ("The government argues, and the district court held, that [the Third-Party Doctrine] requires rejection of appellants' claim that the acquisition of telephone metadata (as opposed to the contents of communications) violates the Fourth Amendment, or even implicates its protections at all.").

context for several reasons. First, from a technological perspective, the distinction of "content" and "metadata" breaks down when it encounters the Internet because the complex network architecture of the Internet permits units of data to change their status between "content" and "metadata" while in transit. A team of eminent computer scientists studied this problem and concluded that "[t]he Internet disrupts the content/non-content distinction . . . arguably to the point of collapse, as it ceases to remain a workable rule for courts to apply in the context of an IP-based communications environment."[194] Considering the Third-Party Doctrine, they went on to conclude that the doctrine was simply "unworkable" when applied to the architecture of the Internet,[195] partly for complicated technological reasons and partly because notions of knowing consent to share data with a third party are fanciful given the way data is transferred on the Internet. These technical realities led the scientists to conclude that, as a technological matter, "[s]imply trying to extend the concept of a 'dialed phone number' to the Internet does not work."[196]

Second, the distinction is complicated by another set of technological issues. Even assuming that we could maintain a technical distinction between "content" and "metadata," modern data science techniques allow analysts to learn arguably even more from "metadata" than from the contents of communications. A former general counsel to the NSA explained that "[m]etadata absolutely tells you everything about somebody's life . . . . If you have enough metadata you don't really need content."[197] This is the case because, as Laura Donohue puts it helpfully, "Data is content, but metadata provides the context for everything we do."[198] In practice, the use of data science can be used to infer so much about a person from metadata that if we are concerned about protecting privacy, the content/metadata distinction is wholly unsatisfactory.[199]

There is a third reason the distinction between content and envelope data going back to *Jackson* is unpersuasive, and it does not require a grasp of Internet architecture or data science to grasp. One significant difference

194. Steven M. Bellovin et al., *It's Too Complicated: How the Internet Upends* Katz, Smith, *and Electronic Surveillance Law*, 30 HARV. J.L. & TECH. 1, 100 (2016).

195. *Id.* at 101.

196. *Id.* at 99.

197. Alan Rusbridger, *The Snowden Leaks and the Public*, N.Y. REV. BOOKS (Nov. 21, 2013), http://www.nybooks.com/articles/2013/11/21/snowden-leaks-and-public/.

198. DONOHUE, FOREIGN INTELLIGENCE, *supra* note 15, at 39.

199. *See* Laura K. Donohue, *The Dawn of Social Intelligence (SOCINT)*, 63 DRAKE L. REV. 1061 (2015) (analyzing the growing ability of government agencies to compile detailed and sensitive information about social relationships through metadata analysis).

between the metadata on the outside of a mailed letter and the addressing information on an email is the nature of the carrier. Mr. Jackson's letter was carried by a mail carrier—a federal official who literally held the letter in his hand and read the address with his eyes in order to deliver the letter. By contrast, electronic communications are carried by private carriers who are not agents of the state. Under such circumstances, it is arguably reasonable to expect even greater privacy against government surveillance.

The broad reading of the Third-Party Doctrine puts the Fourth Amendment at risk. For centuries, our criminal justice system has limited the power of the state by presuming not only that one is innocent until proven guilty but also that one has the right to be free of police monitoring and interference unless there is probable cause to suspect that one has committed a crime.[200] The warrant requirement forces police to persuade a judge that an individual is up to no good. It can be inconvenient, which is precisely the point.[201] But if our data—the facts of our lives—are no longer locked up in secure analog technologies and are also unprotected by the warrant requirement, surveillance and interference becomes much easier, and the specter of a police state looms large. It undermines not just our privacy but indeed any claim that we live in a free society.

B. Lags and Equilibria

In a widely cited article, Professor Orin Kerr attempts to explain how courts do (and should) interpret the Fourth Amendment in the face of social and technological shocks. Kerr offers something that he calls an "Equilibrium-Adjustment" Theory of the Fourth Amendment. This theory has two elements. The first of these is descriptive, the idea that

> [w]hen new tools and new practices threaten to expand or contract police power in a significant way, courts adjust the level of Fourth Amendment protection to try to restore the prior equilibrium.
>
> The result is a correction mechanism. When changing technology or social practice makes evidence substantially harder for the government to obtain, the Supreme Court generally adopts lower Fourth Amendment protections for these new circumstances to help restore the status quo ante level of government power. On the other hand, when changing technology or social practice makes evidence substantially easier for the government to obtain, the Supreme Court

200. *See, e.g.*, Johnson v. United States, 333 U.S. 10 (1948).
201. *Id.* at 13–14.

> often embraces higher protections to help restore the prior level of privacy protection.[202]

This account of Fourth Amendment development as maintaining a steady level of government power is something I will call Kerr's "descriptive account of equilibrium." The second part of Kerr's theory is expressly normative; he argues not only that his descriptive account is accurate, but that it is also desirable as a normative theory of how the Fourth Amendment should work in practice.[203]

In my view, the insights that can be gleaned from the lag problem suggest a modest critique of Kerr's descriptive claim and a robust critique of his normative one. First, at a descriptive level, Equilibrium-Adjustment Theory focuses on the power of the state rather than the civil liberties of the people the government is entrusted with serving.[204] This is a curious emphasis for a Fourth Amendment doctrine, because the Fourth Amendment is a civil liberty rather than a grant of state power. Looking at the problem of civil liberties in terms of maintaining state power turns the analysis upside down, minimizing the importance of civil liberties by focusing on the perspective of police and prosecutors rather than that of free citizens. By contrast, I would suggest that the Fourth Amendment, like other civil liberties, should mean more than a measure of incursion on perfectly efficient crime control.

Second, at a normative level, recognizing the lag problem reveals that even in times of technological change, constitutional doctrine remains dynamic like technology rather than static. This emphasizes the development and expansion of constitutional law, rather than its return to a baseline of police power, and it shows that the progress of the law is contingent and complex. The ultimate difference between the two perspectives may be one of framing: the lag problem perspective sees the civil liberties glass as half-full, whereas Equilibrium-Adjustment Theory sees it as half-empty. But in a time of rapid technological change, when both law and technology can seem to have drifted free of their moorings, framing questions may be among the most important questions we have. When legal questions boil down to the interpretation and translation of traditions to new contexts, the power to define the terms of the argument is in a very real sense the power to dictate its resolution. This was, of course, Stephen Sachs's brilliant insight in his argument in *Smith v. Maryland*.[205] Nowhere

202. Kerr, *supra* note 7, at 480.
203. *Id.* at 525–26.
204. *Id.* at 526–29.
205. *See supra* notes 144–146 and accompanying text.

is this observation more powerful than in the context of the Third-Party doctrine, a proxy through which many of the most important battles over the future of our civil liberties are being waged.

C. Fourth Amendment Normativity

If we are to choose a perspective with which to view the lag problem (or the adjustment of our technological equilibrium, if you will), we must inescapably make a normative choice. Our choice of focus—on police power or on civil liberties—is a normative one, fraught with doctrinal consequences for the society it will help to create. This is why, for example, Justice Scalia's attempt in *Jones* to use eighteenth-century trespass law as the touchstone for the Fourth Amendment is likely to be as unsuccessful as was Chief Justice Taft's attempt to use a similar interpretive strategy in *Olmstead*. Interpretation of the Fourth Amendment is an inherently normative inquiry, and we should be honest about that fact.

This observation also helps to explain why the misplaced trust cases cannot resolve the issues raised by the Third-Party Doctrine. Eighteenth-century trespass law is as useful at dealing with wiretapping or GPS technology as jailhouse snitches are at helping us understand the cloud. And the content/envelope distinction produces incoherent results when it is applied to the architecture of the Internet and big data analytics. This is not to say that analogies never work, or that these older bodies of doctrine will never produce insight, but rather that we must evaluate them critically. Fundamentally, though, in the cloud context, they are unsuitable as bright-line rules for navigating complex and evolving technological and social issues. Modern technology asks questions of these rules that lead them to produce absurd results.

In adapting our hard-won civil liberties from physical contexts into digital ones, we face again the classic interpretive problem of constitutional translation—as technology changes, how do we make sure that the law evolves in ways that preserve its enduring (normative) commitments to values like privacy and the rule of law?[206] In translating the Fourth Amendment to the cloud, we should focus on the normative values that we want to protect. In particular, we should look to the Fourth Amendment's long association with the First Amendment as a guide to ensuring that its enduring values survive the translation to digital form. Fourth Amendment protection should be strongest when dealing with social and technological

206. *See generally* Lawrence Lessig, *Fidelity in Translation*, 71 TEX. L. REV. 1165 (1993).

activities that are intertwined with a First Amendment value. In other words, the Fourth Amendment should be interpreted in ways that protect intellectual privacy. Any other conclusion would be contrary not just to the original traditions of the Fourth Amendment, discussed in Part I, but also to its best values. By protecting intellectual privacy, the Fourth Amendment serves to protect political dissent and self-government. Moreover, it would be deeply and unpleasantly ironic if the Fourth Amendment failed to fully protect digital "papers," at a time when the First Amendment is stronger than it has ever been, reaching expenditures of money,[207] corporate advertising,[208] and allegedly data mining[209] and the writing of code.[210]

From this perspective, we can see the importance of expanding the Fourth Amendment to cover data stored by new technologies rather than applying a broad, blunt, and unsatisfying reading of the Third-Party Doctrine of *Smith* and *Miller*. As we have seen, the Supreme Court has in the past expanded the Fourth Amendment to include the contents of letters and telephone calls, even those made from public phone booths. The current Court has indicated some sympathy for this approach in its recent *Jones* and *Riley* cases. But despite these developments, the constitutional status of data subject to the Third-Party Doctrine remains under (if you will) a cloud. The constitutional status of this data, including email, will remain uncertain until the Supreme Court squarely addresses the question.

When the Court does take such a case, it will be faced with a normative choice, just like it faced in *Riley*. In that case, the Court confronted a similarly simple rule—containers of arrestees can be seized and searched without a warrant—applied to the digital context of smartphones that can hold vast amounts and access infinite amounts of information. The simple rule was at odds with the values of the Fourth Amendment, and the Court expanded the warrant requirement to cover phones searched incident to an arrest. In so doing, it recognized the radically different capabilities of digital technologies. The amount of information that can be stored in a pocket diary or cigarette packet is so much larger as to be qualitatively different from that which can be stored on an iPhone, and the new doctrine announced in *Riley* changed the rule in order to maintain fidelity to the constitutional principle of Fourth Amendment privacy in the digital context.

---

207. Citizens United v. FEC, 558 U.S. 310 (2010).

208. Sorrell v. IMS Health Inc., 564 U.S. 552 (2011).

209. *Id. See generally* Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501 (2015).

210. See Neil Richards, *Apple's "Code = Speech" Mistake*, MIT TECH. REV. (March 1, 2016), https://www.technologyreview.com/s/600916/apples-code-speech-mistake/#/set/id/600918/ (considering and rejecting this argument).

Something similar needs to happen with the broad reading of the Third-Party Doctrine, which, taken to its logical conclusion, suggests that all of our digital information that is exposed to a network loses the protection of the Fourth Amendment. One solution to this problem would be to use Fourth Amendment doctrine to restore the balance that physical searches and less advanced technology provided until recently. The way to do this would be for courts to take a page from *Riley* and affirm that warrants are required before the government can obtain electronic letters or papers held by trusted intermediaries.[211] The final source of these rules will ultimately have to be the Supreme Court, and an important first step would be for the Court to take Justice Sotomayor's invitation to curtail the Third-Party Doctrine, particularly in the context of electronic information.

There will of course be difficult cases. Not all kinds of electronic information are as analogous to postal mail and telephone conversations as emails and cloud documents are. Moreover, even while the crude content/envelope distinction makes little technological sense in the context of Internet architecture and big data analytics, reasonable minds can certainly differ about whether all data is constitutionally equivalent from a Fourth Amendment perspective. Location data, for instance, may require its own body of doctrine. We must also recognize the limitations of constitutional doctrine, which can be insufficiently granular to prescribe the detailed procedures that are necessary to regulate something as complex as electronic surveillance. Modern Fourth Amendment regulation of telephone and electronic surveillance has, almost since its creation worked in tandem with the federal Wiretap Act, passed in 1968 in the aftermath of *Katz* to bring order to electronic surveillance.[212] Yet even though the Wiretap Act was updated in 1986 to include email, federal wiretapping law is hopelessly out of date and has failed to deal with the interpretive problems raised by the cloud.

Recognizing this problem, California recently passed the California Electronic Communications Privacy Act, which went into effect on January 1, 2016.[213] This law, better known as "CalECPA," is a broad protection of

211. As I have argued elsewhere, courts should go further and declare that even when such warrants are obtained, indefinitely delayed notice (particularly enforced by injunction) is constitutionally unreasonable. *See* NEIL M. RICHARDS, NCC GRP., SECRET GOVERNMENT SEARCHES AND THE FUTURE OF CIVIL LIBERTIES (forthcoming 2017).

212. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. 3, 82 Stat. 197, 211 (1968) (codified as amended at 18 U.S.C. §§ 2510–2520).

213. California Electronic Communications Privacy Act, CAL. PENAL CODE §§ 1546–1546.4 (West 2017). (In full disclosure, I signed a letter written to California Governor Edmund G. Brown, Jr. on behalf of a number of legal scholars that asked the Governor to sign rather than veto the bill. *See* Letter

electronic information that requires California police to obtain a warrant before they access "electronic information"—either digitally or from a physical device—such as emails, stored documents, or the "metadata" associated with electronic information.[214] Although CalECPA only applies in California, it is a well-drafted statute that could serve as a model for the reform of federal wiretapping law.

D. Intermediaries and the Future of Civil Liberties

In addition to a normatively sensitive Fourth Amendment supplemented by updated surveillance statutes, the project of civil liberties in the cloud (especially in the Fourth and First Amendment contexts) will require both the participation of intermediaries and the recognition by our law that intermediaries will often be best placed to advance civil liberties on behalf of the humans who are their clients.

This perspective reveals the importance of Apple's and Microsoft's stands on behalf of the privacy and security of their customers against the government.[215] In these cases and others like them, we are witnessing an emerging truth about civil liberties today: when our lives rely upon digital technologies, we often have little choice but to rely in turn on those technologies' providers to protect our interests. When the government comes to them seeking our data, they, not we, are in the best position to protect that data, and by extension, our civil liberties. In essence, we are forced to trust them.[216]

This is a controversial proposition. After all, technology companies are usually profit-maximizing organizations for which quarterly returns and shareholder value are more important than something as ethereal as civil liberties. And while every other major democracy has a national privacy law regulating the corporate sector, American privacy law is piecemeal, highly constrained, and often gives companies the practical ability to do what they want with our data, as long as they do not lie about it or cause unwarranted harm.[217] These concerns are not trivial. It is important for customers of these

---

from Legal Scholars to Edmund G. Brown, Governor of California (Sept. 12, 2015), https://www.aclunc.org/sites/default/files/SB178ScholarsSupport.pdf).

214. CAL. PENAL CODE §§ 1546–1546.1.

215. *See supra* notes 2–4.

216. *See* Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016) (explaining the importance of trust as a framework for thinking about digital privacy issues); Richards & Hartzog, *supra* note 5 (same).

217. *See* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES (forthcoming 2018).

companies (which is to say, essentially everyone in a digital economy) to be careful in their interactions with them. Not all technology companies treat privacy with equal seriousness, and it is worth noting that the companies taking the strongest stands for privacy seem to be the ones that sell software and devices in exchange for customers' money, rather than the "free" services that "monetize" their users by targeting them with data-based advertisements. Sometimes we will need government to regulate companies, too. An important dimension of a digital society subject to the rule of law will be to demand checks and balances among humans, governments, and technology firms, and law can be used to promote trust. In other work, Woodrow Hartzog and I have argued that trustworthy companies must meet four criteria—they must be *honest* with their customers, *protect* those customers' data, treat it in a manner that is *discreet*, and most importantly be *loyal* to those customers with their data rather than betraying them for profit.[218] Although there are many market incentives for companies to act this way, not all companies will. To ensure that they do, we should recognize them as our information fiduciaries, and the law should recognize them as the same.[219]

But we need not always be cynical. Yes, businesses benefit when we trust them: many of the leading intermediaries want our confidence, and their privacy positions reflect this. But when corporate and civil-liberties interests coincide, the human beings that are their users should embrace the alignment. For better or for worse, the nature of modern technologies is such that the companies creating, designing, and controlling those technologies must play a role in maintaining our vital liberties. We can therefore be cautiously optimistic about the San Bernardino iPhone and Irish email cases.[220] These are important moves from companies that we, as citizens of digital democracies, need on our side.

CONCLUSION

The Third-Party Doctrine is in many respects a classic example of a recurring problem in law—what happens to a rule that made sense in one context when that context radically changes? In resolving the problems created by the Third-Party Doctrine in the digital context, courts interpreting

218. Richards & Hartzog, *supra* note 216.

219. For promising proposals along these lines, see Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016); and Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611 (2015).

220. *See supra* notes 2–3.

the Fourth Amendment will have to choose between the simple rule and the underlying values behind that rule. I have argued in this paper that the core values that underpin Fourth Amendment law—notably the important linkages between the protection against warrantless searches and political dissent—risk being undermined by the simple but broad version of the doctrine. I have attempted to make the case that Fourth Amendment jurisprudence is inevitably a normative one, and that the Third-Party Doctrine is deeply normatively unsatisfying, particularly when judged against traditional Fourth Amendment values. Yet abandoning the broad reading of the Third-Party Doctrine requires us to replace it with something, and that replacement is likely to be more complicated or at least more nuanced than what came before. It will most likely require not only new constitutional doctrine, but changes in statutory law and corporate business practices as well. But we should not shirk this challenge. The constitutional protection against unreasonable searches and seizures is one of our most important civil liberties, and it is essential that its protections be translated faithfully into the digital context. The digital transition is a dangerous time for our civil liberties, but recent developments in constitutional law and corporate strategy provide hope that a robust digital Fourth Amendment is possible.