THE CASE FOR THE THIRD-PARTY DOCTRINE

Orin S. Kerr[*]

This Article offers a defense of the Fourth Amendment's third-party doctrine, the controversial rule that information loses Fourth Amendment protection when it is knowingly revealed to a third party. Fourth Amendment scholars have repeatedly attacked the rule on the ground that it is unpersuasive on its face and gives the government too much power. This Article responds that critics have overlooked the benefits of the rule and have overstated its weaknesses.

The third-party doctrine serves two critical functions. First, the doctrine ensures the technological neutrality of the Fourth Amendment. It corrects for the substitution effect of third parties that would otherwise allow savvy criminals to substitute a hidden third-party exchange for a previously public act. Second, the doctrine helps ensure the clarity of Fourth Amendment rules. It matches the Fourth Amendment rules for information to the rules for location, creating clarity without the need for a complex framework of sui generis rules.

Finally, the two primary criticisms of the third-party doctrine are significantly weaker than critics have claimed. The third-party doctrine is awkward for reasons of form rather than function; it is a consent rule disguised as an application of Katz*'s "reasonable expectation of privacy" test. Claims that the doctrine gives the government too much power overlook the substitutes for Fourth Amendment protection in the use of the third parties. Those substitutes include entrapment law, common law privileges, the* Massiah *doctrine, the First Amendment, internal agency regulations, and the rights of the third parties themselves.*

---

* Professor, George Washington University Law School. This Article benefited greatly from thoughtful comments during workshops at Seton Hall, Widener-Wilmington, and the GW/Berkeley Privacy Law Scholars Conference. Thanks in particular to Daniel Solove, Christopher Slobogin, David Feige, Stephen Henderson, and Christine Jolls.

TABLE OF CONTENTS

INTRODUCTION

Human beings are social animals. We like to share. We like to gossip. We ask for help from others, and we give help in return. Sometimes we share by speaking in person. Sometimes we write a letter or send a message by computer. In all of these cases, the human impulse to share creates an important opportunity for criminal investigators. When wrongdoers share with others, they often expose evidence of their crimes. A corrupt

businessman might disclose records to his accountant. A mob boss might tell his brother about an assault. A drug dealer might reveal his plans to a confidential informant. In all of these cases, someone other than the criminal or the police—some third party—comes to possess evidence of crime. Investigators often want to collect evidence from these third parties, as they are more likely to cooperate and less likely to tip off the suspect that an investigation is afoot.

The "third-party doctrine" is the Fourth Amendment rule that governs collection of evidence from third parties in criminal investigations.[1] The rule is simple: By disclosing to a third party, the subject gives up all of his Fourth Amendment rights in the information revealed. According to the Supreme Court:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[2]

In other words, a person cannot have a reasonable expectation of privacy in information disclosed to a third party.[3] The Fourth Amendment simply does not apply.

The third-party doctrine is the Fourth Amendment rule scholars love to hate. It is the *Lochner*[4] of search and seizure law, widely criticized as profoundly misguided.[5] Decisions applying the doctrine "top[] the chart of [the]

---

1. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 528–29 (2006) (describing the third-party doctrine).

2. United States v. Miller, 425 U.S. 435, 443 (1976).

3. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

4. Lochner v. New York, 198 U.S. 45 (1905).

5. A list of every article or book that has criticized the doctrine would make this the world's longest law review footnote. However, some of the major criticisms include Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy"*, 34 VAND. L. REV. 1289, 1315 (1981); Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-first Century*, 65 IND. L.J. 549, 564–66 (1990); Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229 (1983) (arguing that the third-party doctrine cases are incorrect because they focus on the rights of the guilty rather than the rights of the innocent); Scott E. Sundby, "*Everyman" 's Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1757–58 (1994).

Recent criticisms of the doctrine include CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 151–64 (2007); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211 (2006) (arguing that the major third-party doctrine cases were wrongly decided on several grounds); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3; Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975 (2007); Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 2007 UCLA J.L. & TECH. 1, 3–4 (advocating a "retooling" of the third-party doctrine for internet searches); Andrew J. DeFilippis, Note, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1092 (2006) (arguing that the Supreme Court should overrule the third-party doctrine).

most-criticized fourth amendment cases."[6] Wayne LaFave asserts in his influential treatise that the Court's decisions applying it are "dead wrong"[7] and "make[] a mockery of the Fourth Amendment."[8] The verdict among commentators has been frequent and apparently unanimous: The third-party doctrine is not only wrong,[9] but horribly wrong.[10] Even many state court judges have agreed. Over a dozen state Supreme Courts have rejected the doctrine under parallel provisions of their state constitutions.[11]

Remarkably, even the U.S. Supreme Court has never offered a clear argument in its favor. Many Supreme Court opinions have applied the doctrine; few have defended it. The closest the Court has come to justifying the doctrine has been its occasional assertion that people who disclose communications to a third party "assume the risk" that their information will end up in the hands of the police.[12] But assumption of risk is a result rather than a rationale: A person must assume a risk only when the Constitution does not protect it. Exactly *why* the Constitution does not protect information disclosed to third parties has been left unexplained.

This Article offers a defense of the third-party doctrine, and especially its most controversial applications. It argues that the doctrine serves two roles that critics have missed. The first and most important purpose is to maintain the technological neutrality of Fourth Amendment rules. Use of third parties has a substitution effect: It takes open and public portions of crimes and hides them from public observation. Without the third-party doctrine, savvy wrongdoers could use third-party services in a tactical way to enshroud the entirety of their crimes in zones of Fourth Amendment protection. The result would allow technology to upset the Fourth Amendment's traditional balance between privacy and security, weakening the deterrent and retributive goals of criminal punishment. The third-party doctrine blocks this end-run around the traditional Fourth Amendment balance. It

---

6. Clark D. Cunningham, *A Linguistic Analysis of the Meanings of 'Search' in the Fourth Amendment: A Search for Common Sense*, 73 IOWA L. REV. 541, 580 (1988).

7. 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.7(c), at 747 (4th ed. 2004).

8. *Id.* § 2.7(b), at 736 ("Such a crabbed interpretation of the *Katz* test makes a mockery of the Fourth Amendment.").

9. *See* sources cited *supra* note 5.

10. *See, e.g.*, 1 LAFAVE, *supra* note 7, § 2.7(c), at 747 ("The result reached in *Miller* is dead wrong, and the Court's woefully inadequate reasoning does great violence to the theory of Fourth Amendment protection which the Court had developed in *Katz*."); Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 753 (2005) ("The third party doctrine presents one of the most serious threats to privacy in the digital age.").

11. For a list of states that have rejected the doctrine, in whole or in part, see Stephen E. Henderson, *Learning from All Fifty States: How To Apply the Fourth Amendment and Its State Analogs To Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373 (2006).

12. Smith v. Maryland, 442 U.S. 735, 744 (1979) ("Because the depositor [in *Miller*] 'assumed the risk' of disclosure, the Court held that it would be unreasonable for him to expect his financial records to remain private.").

helps ensure that the Fourth Amendment rules that apply to crimes committed using third parties are roughly equivalent to the rules that apply to crimes committed without them.

The doctrine's second role is to provide ex ante clarity. Under the third-party doctrine, Fourth Amendment protection for information matches the Fourth Amendment protection for the environment in which it is stored. As a result, Fourth Amendment rules are determined by information's knowable location rather than its unknowable history. Absent the third-party doctrine, courts would face the difficult challenge of creating a clear regime of Fourth Amendment protection for third-party information. Although such challenges are not insurmountable, the clarity of the third-party doctrine provides an important argument in its favor.

The third-party doctrine is no panacea, of course. Critics have made two important arguments against it, one doctrinal and the other functional.[13] The doctrinal argument is that the Justices do not understand the privacy interests at stake in third-party information. To these critics, the Justices' assertion that disclosure automatically renders an expectation of privacy "unreasonable" is simply incorrect.[14] The second argument is functional: It contends that the doctrine is misguided because it grants governments the authority to take more invasive steps without constitutional oversight than are consistent with a free and open society. In particular, the third-party doctrine gives government officials too much power to harass individuals in bad faith.[15]

This Article explains that while both criticisms have some appeal, both considerably overstate the case and ignore important counterarguments. Assertions that the Justices do not understand privacy are objections more about form than substance. Although the third-party doctrine has been framed in terms of the "reasonable expectation of privacy" test, it is better understood as a consent doctrine. Disclosure to third parties eliminates protection because it implies consent. When understood as a subset of consent law rather than an application of the reasonable expectation of privacy test, the third-party doctrine fits naturally within the rest of Fourth Amendment law.

Finally, functional arguments about government power overlook the legal system's substitutes for Fourth Amendment protection. The Fourth Amendment is not the only game in town. Common law privileges, entrapment law, the *Massiah* doctrine, First Amendment doctrine, and statutory privacy protections have been designed specifically to address concerns of police harassment in their use of third parties.[16] These mostly nonconstitutional legal principles each regulate specific aspects of third-party practices to deter police abuses, generally forcing the police to use third parties in good faith or

---

13. *See infra* Section I.B.

14. *See infra* Section I.B.1.

15. *See infra* Section I.B.2.

16. All of these doctrines are discussed *infra* Section IV.B.

in a reasonable way. Critics have overlooked these substitutes, and as a result have tended to see the choice as between Fourth Amendment protection or no protection at all. Understanding how other doctrines substitute for Fourth Amendment protection reveals that this understanding is incorrect.

The goal of this Article is to replace the partial view of the third-party doctrine found in existing scholarship with a richer and more balanced account of its costs and benefits. The topic is a timely one: Technological progress places more and more communications in the hands of third parties,[17] and the growing importance of new technologies such as the internet has led to a renewal of the attacks on the third-party doctrine.[18] Given the latest wave of criticisms, a more complete understanding is needed to better appreciate how the Fourth Amendment should apply both in the case of old technologies and new ones. I do not expect that the arguments offered in this Article will persuade every critic to change positions; reasonable people can disagree on whether the doctrine is appropriate in particular cases. At the same time, I hope the Article will demonstrate a strong affirmative argument for the doctrine in many cases and at least a plausible argument in others.

This Article proceeds in four parts. Part I briefly introduces the law of the third-party doctrine and the harsh criticisms of it. Part II argues that the third-party doctrine ensures technological neutrality of the Fourth Amendment by blocking the opportunistic use of third parties to circumvent the basic balance of Fourth Amendment rules. Part III contends that the doctrine is needed to provide ex ante clarity. The Fourth Amendment's suppression remedy requires clear rules governing when a Fourth Amendment search occurs, and the third-party doctrine creates that needed certainty. Part IV responds to the two primary criticisms of the third-party doctrine, that the doctrine is doctrinally unpersuasive and that it gives too much power to the police. It argues that the first claim is largely a matter of form and that the latter is addressed by legal rules beyond the Fourth Amendment.

I. Introduction to the Third-Party Doctrine

This Part explains the third-party doctrine and summarizes the two basic types of cases: those involving secret agents such as undercover informants, and those involving third-party account records. This Part also introduces the two primary criticisms of the third-party doctrine. The first criticism is doctrinal in nature; it asserts that it is simply incorrect to say that third-party exposure renders an expectation of privacy "unreasonable."[19] The second criticism is functional; it claims that the third-party doctrine gives the government too much power over individuals.[20]

---

17. *See* Solove, *supra* note 1, at 528–29.

18. *See, e.g.*, sources cited *supra* note 5.

19. *See infra* Section II.B.1.

20. *See infra* Section II.B.2.

A. *The Cases*

1. *Secret Agents, 1952–1971*

Although several of the Supreme Court's earliest cases in the law of criminal procedure involved the use of undercover agents and confidential informants[21]—so-called "secret agents"[22]—a Fourth Amendment challenge to such secret agents did not reach the Court until *On Lee v. United States*.[23] Lee sold opium from his laundry store and one day made incriminating statements to his friend Poy. It turned out that Poy was an undercover informant wearing a wire, and the recording of Lee's statements was used against Lee at trial. Lee argued that the government's conduct violated the Fourth Amendment because it was the equivalent of secretly placing a bug inside the store.

The Supreme Court disagreed. According to Justice Jackson, Lee simply "was talking confidentially and indiscreetly with one he trusted."[24] The fact that Poy was wearing a wire was irrelevant, because the recording was "with the connivance of one of the parties"[25] to the conversation (that is, Poy). Justice Jackson suggested that the very idea of seeing these facts as problematic under the Fourth Amendment was quite silly: "It would be a dubious service to the genuine liberties protected by the Fourth Amendment to make them bedfellows with spurious liberties improvised by farfetched analogies . . . ."[26]

The Court reached the same result a decade later in *Lopez v. United States*.[27] Lopez tried to bribe an IRS agent who was wearing a wire, and both the recording and the agent's testimony were admitted against Lopez at trial. Citing *On Lee*, Justice Harlan readily rejected Lopez's claim that his Fourth Amendment rights were violated: "Lopez knew full well [his statements] could be used against him by [the IRS agent] if he wished,"[28] and the wire recording "device was used only to obtain the most reliable evidence possible of a conversation in which the Government's own agent was a participant and which that agent was fully entitled to disclose."[29]

---

21. For example, in *Gouled v. United States*, 255 U.S. 298 (1921), a business acquaintance of a criminal suspect pretended to pay a social visit at the suspect's office when he in fact was intending to search the office for evidence. Eleven years later, in *Sorrells v. United States*, 287 U.S. 435 (1932), an undercover prohibition agent looking for alcohol gained entrance to a suspect's home by posing as a tourist. Although these cases involved secret agents, they did not specifically raise Fourth Amendment challenges to secret agents' use.

22. *See, e.g.*, YALE KAMISAR ET AL., MODERN CRIMINAL PROCEDURE 465 (12th ed. 2008).

23. 343 U.S. 747 (1952).

24. *Id.* at 753.

25. *Id.* at 754.

26. *Id.*

27. 373 U.S. 427 (1963).

28. *Id.* at 438.

29. *Id.* at 439.

Lopez was followed quickly by *Lewis v. United States*[30] and *Hoffa v. United States*,[31] handed down the same day in 1966. In *Lewis*, the defendant invited an undercover agent into his home to sell him marijuana. In *Hoffa*, Teamsters President Jimmy Hoffa confided in his colleague Partin, who turned out to be working secretly for the police. In both cases, the secret agents later testified about what they had seen and heard. Relying on *Lopez* and *On Lee*, the Court concluded that neither use of secret agents had violated the Fourth Amendment. While Hoffa "was relying upon his misplaced confidence that Partin would not reveal his wrongdoing," the Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."[32] And use of an undercover officer in *Lewis* could not be unconstitutional because such a rule would severely hamper undercover investigations:

> Were we to hold the deceptions of the agent in this case constitutionally prohibited, we would come near to a rule that the use of undercover agents in any manner is virtually unconstitutional *per se*. Such a rule would, for example, severely hamper the Government in ferreting out those organized criminal activities that are characterized by covert dealings with victims who either cannot or do not protest.[33]

The last of the secret agent cases, *United States v. White*,[34] affirmed that the third-party doctrine survived the formal switch to the reasonable expectation of privacy test first articulated in Justice Harlan's concurrence in *Katz v. United States*.[35] The facts of *White* were almost identical to those of *Lopez*: White spoke about his crimes to an undercover informant who was wearing a wire, and the recordings of the conversations were used against him at trial.[36] The plurality opinion by Justice White concluded that *Hoffa*, *Lopez*, and *On Lee* had survived *Katz*.[37] *Katz* did not disturb that line of cases because it "involved no revelation to the Government by a party to conversations with the defendant."[38] In the language of *White*, an expectation that a person would not share private information with the police was not constitutionally justifiable:

> Inescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police. If he sufficiently doubts their trustworthiness, the association will very probably end or never

30. 385 U.S. 206 (1966).

31. 385 U.S. 293 (1966).

32. *Id.* at 302.

33. *Lewis*, 385 U.S. at 210.

34. 401 U.S. 745 (1971).

35. 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

36. *White*, 401 U.S. at 746–47.

37. *Id.* at 749–50.

38. *Id.* at 749. Because Justice Black's concurring opinion adopted a far broader rationale, Justice White's plurality opinion expresses the holding of the Court.

> materialize. But if he has no doubts, or allays them, or risks what doubt he has, the risk is his.[39]

Exactly *why* this conclusion was "inescapable"—and why "the risk is his"—was left unexplained.

2. *Business Records, 1973–1980*

The second round of third-party doctrine cases occurred from 1973 to 1980, and they all involved various types of business records. In all of the cases, the Court held that transferring business records to third parties relinquished Fourth Amendment protection. In *Couch v. United States*,[40] Couch had given tax documents to his accountant, and the government issued an IRS summons ordering the accountant to hand over documents that related to Couch's tax returns.[41] In *United States v. Miller*,[42] the government served subpoenas on banks used by the defendant Miller seeking all records relating to his accounts. In *United States v. Payner*,[43] investigators stole a briefcase owned by the vice president of a bank in the Bahamas and then copied the briefcase's contents before returning it. The contents revealed that Payner maintained an account at the bank, and this helped the government show that Payner had falsified his tax returns.[44]

In all three cases, the defendant moved to suppress the financial records under the Fourth Amendment. In all three cases, the Court rejected the claims under the third-party doctrine in opinions by Justice Powell. In *Couch*, Justice Powell concluded that "there can be little expectation of privacy where records are handed to an accountant."[45] By handing information to his accountant, Couch had given his accountant the power to decide what information would be further disclosed in Couch's income tax returns.[46] In *Miller*, Justice Powell used two different arguments. First, the bank records were not the defendant's private or personal letters, but rather were financial documents that would be used in the ordinary course of business.[47] Second, the defendant had voluntarily conveyed the information to a third party just like White, Hoffa, and Lopez. "[I]n revealing his affairs to another," the defendant had assumed the risk "that the information [would] be conveyed by

---

39. *Id.* at 752.

40. 409 U.S. 322 (1973).

41. *Id.* at 324–25.

42. 425 U.S. 435 (1976).

43. 447 U.S. 727 (1980).

44. *Id.* at 728–30.

45. *Couch*, 409 U.S. at 335.

46. *See id.* ("What information is not disclosed is largely in the accountant's discretion . . . . Indeed, the accountant himself risks criminal prosecution if he willfully assists in the preparation of a false return. His own need for self-protection would often require the right to disclose the information given him." (citation omitted)).

47. *Miller*, 425 U.S. at 442.

that person to the Government."[48] In *Payner*, Justice Powell found the case indistinguishable from *Miller*.[49]

Finally, the Court applied the third-party doctrine in *Smith v. Maryland*,[50] a case involving pen registers. A pen register was a device installed at the phone company to record the numbers dialed from a specific telephone. In *Smith*, investigators had asked the phone company to install a pen register on the home phone of a man suspected of robbing and then harassing a woman by making anonymous phone calls. The pen register confirmed that the calls were originating from the man's home, and that information was used to help get a warrant to search his home.[51] The Supreme Court held that use of the pen register was not a "search" because it was covered by the third-party doctrine: "When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed."[52] According to Justice Blackmun, writing for the majority, "[t]he switching equipment that processed those numbers [was] merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber."[53] The third-party doctrine applied even though "the telephone company ha[d] decided to automate."[54]

B. *Common Criticisms of the Third-Party Doctrine*

The criticisms of the third-party doctrine derive from two basic arguments, one doctrinal and the other functional. Both arguments were first developed in dissents from the important third-party doctrine cases, most notably Justice Harlan's dissent in *White*[55] and Justice Marshall's dissent in *Smith*.[56] In the decades since these opinions, a large body of scholarship has echoed and expanded on their two basic claims.

1. *The Doctrinal Critique*

The first important criticism of the third-party doctrine is that it does not accurately apply the reasonable expectation of privacy test. According to

---

48. *Id.* at 443.

49. *Payner*, 447 U.S. at 732 ("*United States v. Miller* established that a depositor has no expectation of privacy and thus no protectable Fourth Amendment interest in copies of checks and deposit slips retained by his bank. Nothing in the record supports a contrary conclusion in this case." (citations omitted) (internal quotation marks omitted)).

50. 442 U.S. 735 (1979).

51. *Id.* at 737.

52. *Id.* at 744.

53. *Id.*

54. *Id*. at 745.

55. United States v. White, 401 U.S. 745, 768–95 (1971) (Harlan, J., dissenting).

56. *Smith*, 442 U.S. at 748–52 (Marshall, J., dissenting).

critics, individuals normally expect privacy in their bank records, phone records, and other third-party records.[57] Such expectations of privacy are common and reasonable, and Justices who cannot see that are simply out of touch with society and are misapplying the Fourth Amendment.[58] From this perspective, it "defies reality"[59] to say that a person "voluntarily" surrenders information to third parties like banks or telephone companies.[60] As Justice Marshall reasoned in his *Smith* dissent, "[i]t is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative."[61]

A corollary to this claim is that the Justices supporting the third-party doctrine have misunderstood the concept of privacy. The Justices envision privacy as an on-off switch, equating disclosure to one with disclosure to all, and as a result they miss the many shades of gray.[62] As Justice Marshall put the point in *Smith*, "[p]rivacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[63] Echoing Justice Marshall, Daniel Solove argues that the third-party doctrine is based on an incorrect "conception of privacy," a conception of privacy as total secrecy.[64] Along the same lines, Richard Posner argues that the *Miller* line of cases is "unrealistic."[65] "Informational privacy does not mean refusing to share information with everyone," he maintains, for "[o]ne must not confuse solitude with secrecy."[66] Sherry Colb agrees, writing that "treating exposure to a limited audience as identical to exposure to the world"[67] fails to recognize the degrees of privacy.

---

57. *See, e.g.*, Ashdown, *supra* note 5, at 1315 ("[T]elephone patrons undoubtedly would be shocked to learn that records of their calls either were available for third parties or were being distributed outside the telephone system."); Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society"*, 42 DUKE L.J. 727, 732 (1993) (arguing that some Supreme Court cases "do not reflect societal understandings" of when an expectation of privacy is "reasonable," and that "some of the Court's conclusions [about what expectations of privacy are reasonable] may be well off the mark").

58. *See* Slobogin & Schumacher, *supra* note 57, at 732.

59. Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 829 (2005).

60. *See also* Ashdown, *supra* note 5, at 1315.

61. *Smith*, 442 U.S. at 750 (Marshall, J., dissenting).

62. *See, e.g.*, Katz, *supra* note 5, at 564–66.

63. *Smith*, 442 U.S. at 749 (Marshall, J., dissenting).

64. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1086 (2002).

65. RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY 140 (2006).

66. *Id.*

67. Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122 (2002).

2. *The Functional Critique*

The second major critique of the third-party doctrine contends that it gives the government more power than is consistent with a free and open society. The first significant elaboration of this argument appears to be Justice Harlan's dissent in *United States v. White*.[68] Harlan argued that the government should not be permitted to use an undercover informant with a wire because leaving such a procedure unregulated would grant the government too much power:

> Were third-party bugging a prevalent practice, it might well smother that spontaneity—reflected in frivolous, impetuous, sacrilegious, and defiant discourse—that liberates daily life. Much off-hand exchange is easily forgotten and one may count on the obscurity of his remarks, protected by the very fact of a limited audience, and the likelihood that the listener will either overlook or forget what is said, as well as the listener's inability to reformulate a conversation without having to contend with a documented record. All these values are sacrificed by a rule of law that permits official monitoring of private discourse limited only by the need to locate a willing assistant.[69]

Justice Marshall's dissent in *Smith*[70] made a similar point. According to Marshall, exempting pen registers from Fourth Amendment scrutiny enabled unregulated monitoring that would be harmful to a free society:

> The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide. Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts. Permitting governmental access to telephone records on less than probable cause may thus impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society.[71]

Arnold Loewy picked up this theme in his 1983 article, *The Fourth Amendment as a Device for Protecting the Innocent*.[72] Loewy posited that Fourth Amendment protections should protect the innocent, and then reasoned that the third-party doctrine cases gave the police too much power to harass innocent citizens.[73] By allowing undercover agents to record suspects without judicial scrutiny, the Court had given them "the ability to use [the recordings] for parlor games, practical jokes, or harassment."[74] By allowing the police to install pen registers without oversight, the Court had left the

---

68. 401 U.S. 745 (1971).

69. *See id.* at 787–89 (Harlan, J., dissenting) (footnotes omitted).

70. Smith v. Maryland, 442 U.S. 735, 748–52 (1979) (Marshall, J., dissenting).

71. *Id*. at 751 (citations omitted).

72. Loewy, *supra* note 5.

73. *Id.* at 1252–56.

74. *Id.* at 1253.

police "perfectly free to learn every telephone number that any persons [sic] dials, subject only to the cooperation of the telephone company."[75]

Other scholars have made similar points,[76] often in discussions of how the Fourth Amendment applies to computers and the Internet. Internet services are third-party services, raising the prospect that the Fourth Amendment may apply only modestly to internet communications. Scholars have responded by contending that the third-party doctrine is "not responsive to life in the modern Information Age."[77] If third-party services play a growing role in government surveillance, the concern runs, then the Fourth Amendment will regulate a smaller and smaller portion of that surveillance; the government will be able to collect and assemble "digital dossiers" without Fourth Amendment scrutiny.[78] To ensure sufficient constitutional protection online, many argue, the third-party cases should be overruled or sharply limited to their facts.[79]

II. Substitution Effects and the Functional Role of the Third-Party Doctrine

The widespread criticism of the third-party doctrine overlooks two important benefits of the rule. This Part explains the first major benefit of the third-party doctrine: It ensures technological neutrality in Fourth Amendment rules. The use of third parties has a substitution effect. It enables wrongdoers to take public aspects of their crimes and replace them with private transactions. Without a third-party doctrine, suspects can act opportunistically to effectively hide their criminal enterprises from observation. The result upsets the basic balance of Fourth Amendment law, undercutting the deterrent and retributive force of criminal law. The third-party doctrine blocks such efforts, resulting in a rough equivalence in the overall amount of privacy for criminals acting alone and the amount of privacy for those using third parties.

To develop this argument, I will start with the basic balance of the Fourth Amendment. I will explain how third parties threaten this balance and how the third-party doctrine retains it. I will then cover a few examples

---

75. *Id.* at 1255.

76. *See, e.g.*, Katz, *supra* note 5, at 568–69 ("The government is free from any judicial oversight. Without a reasonableness limitation, we must rely on government officials to voluntarily respect our privacy.").

77. Solove, *supra* note 64, at 1087.

78. *Id.*; Joseph T. Thai, *Is Data Mining Ever a Search Under Justice Stevens's Fourth Amendment?*, 74 Fordham L. Rev. 1731, 1736–45 (2006).

79. *E.g.*, Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 Geo. Wash. L. Rev. 1375, 1403 (2004) (articulating that the third-party doctrine should be construed narrowly in the context of computer and internet communications); Freiwald, *supra* note 5, at ¶ 40; Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 Geo. Wash. L. Rev. 1557 (2004) (arguing that the third-party doctrine should be read narrowly in the case of computer and internet communications).

and conclude by showing how the doctrine is an essential aspect of the technological neutrality of Fourth Amendment rules.

A. *The Basic Division of the Fourth Amendment*

The Fourth Amendment's prohibition on unreasonable searches and seizures is premised on a balance between privacy and security. To implement that balance, the Supreme Court has created two basic categories of law enforcement conduct: investigative steps that the Fourth Amendment regulates and those that it does not. Under this scheme, the Fourth Amendment protects some things and some places while leaving others open to government surveillance. For example, the Fourth Amendment protects a person's home and private packages.[80] If the government wants access to those places, it must ordinarily have a search warrant.[81] On the other hand, occurrences in public or on open fields are not protected by the Fourth Amendment.[82] If the government wants to monitor such spaces, the Fourth Amendment does not interfere: The monitoring is not a search or seizure.

The Fourth Amendment's divide between unregulated and regulated spaces forms an essential part of how the amendment works. It divides evidence collection into two stages: less invasive steps the government can take at any time, and more invasive steps the government can only take when it has already collected enough evidence to demonstrate special conditions such as probable cause or exigent circumstances. From an investigative standpoint, the two categories work together. Investigations often start with the open surveillance, permitting the police to look for clues that may indicate criminal activity. If the open surveillance yields sufficient evidence, that evidence permits the government to take more invasive steps that are often necessary to prove cases beyond a reasonable doubt in court.[83]

The basic division into unregulated and regulated steps leads to a balance between privacy and security because most crimes have traditionally required suspects to carry out at least part of their crimes in spaces open to surveillance. To see why, consider a world with no advanced technology. Part of the crime will normally occur outside. If John wants to rob a person walking down the street, for example, he needs to leave his house and go out to the street. If he wants to purchase drugs, he needs to go out of his home and find a dealer who will sell them to him. If he wants to murder his coworker, he needs to go out and buy a knife; after the act, he needs to dispose

---

80. *E.g.*, Payton v. New York, 445 U.S. 573, 585 (1980) (noting that the "'chief evil against which the Fourth Amendment is directed'" is the warrant-less entry and search of a home (quoting United States v. United States Dist. Court, 407 U.S. 297, 313 (1972))).

81. *Id.*

82. California v. Ciraolo, 476 U.S. 207, 213 (1986) ("The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares.").

83. In the argot of existing doctrine, government conduct that violates a reasonable expectation of privacy is a "search" that ordinarily triggers the warrant requirement; other government conduct is not a "search" at all.

of the body. In all of these traditional types of crimes, the wrongdoer has to leave his home and go out into spaces unprotected by the Fourth Amendment.

The public component of most traditional crimes is critical to the traditional balance of Fourth Amendment rules. If at least part of a crime occurs in spaces unprotected by the Fourth Amendment, the police have at least some opportunity to look more closely at whether criminal activity is afoot. Because the police normally begin an investigation with only speculation that a particular person is a lawbreaker, the public portion of crimes give the police an opportunity to develop more evidence. The police will have access to the public portion of the crime free of legal regulation. If they are observing him, they will know where the suspect went and what he said in public. That information won't solve the crime in most cases: Unless an officer directly observes the crime, the publicly available evidence only provides a lead.[84] But it's a start. If the evidence is strong enough, it can support invasions of protected spaces with a warrant. And those steps help the police solve at least a moderate percentage of criminal cases. Of course, many cases won't be solved. But enough cases are solved that a significant prospect of criminal punishment exists, allowing the criminal justice system to serve its utilitarian and retributive ends.

B. *Third Parties and the Basic Division*

Third parties pose a major threat to the Fourth Amendment's basic division between unregulated and regulated steps. The reason is that third parties act as remote agents that permit wrongdoers to commit crimes entirely in private. Those committing crimes naturally try to hide them from the police; no criminal wants to get caught. If a wrongdoer can use third parties as remote agents, he can reduce his exposure to public surveillance. Instead of going out into the world and subjecting himself to exposure, a wrongdoer can bring third-party agents inside and share plans or delegate tasks to them. He can use the third-party services to commit his crimes without exposing himself to spaces open to government surveillance.

Put another way, the use of third parties often has a *substitution effect*.[85] Without the third party, the wrongdoer would have needed to go out into public spaces where the Fourth Amendment does not regulate surveillance. But use of a third party substitutes a hidden transaction for the previously open event. What would have been public now becomes hidden. The wrongdoer no longer needs to leave his home, as the third-party agents

---

84. Of course, this is not true in every case: It is possible to imagine an entirely private crime such as attempting suicide. But in most cases, some exposure is necessary.

85. In economics, a "substitution effect" generally refers to change in the amount of a product consumed if the relative price of a competing product is raised. The concept of a substitution effect can be applied more broadly, however, to show how two different means of committing a crime can compete with each other. *See, e.g.*, Neal Kumar Katyal, *Deterrence's Difficulty*, 95 MICH. L. REV. 2385, 2387 (1997) (applying the substitution effect framework to criminal conduct).

enable him to commit the crime remotely. The crime now comes to the criminal rather than the criminal going to the crime.[86]

Consider how a person might use third parties to commit crimes from the protection of his own home. A mob boss might summon his underlings to his house to give them orders. A stalker might call his victim on his home phone rather than lying in wait outside her door. A computer hacker might hack into computers thousands of miles away without leaving his bedroom. In all of these cases, individuals use third parties to carry on their crimes without exposing themselves to spaces unprotected by the Fourth Amendment. The third-party agents—the employee, the telephone, and the Internet—do the work remotely on the principal's behalf.

Now we can see the importance of the third-party doctrine. Without the doctrine, criminals could use third-party agents to fully enshroud their criminal enterprises in Fourth Amendment protection. A criminal could plot and execute his entire crime from home knowing that the police could not send in undercover agents, record the fact of his phone calls, or watch any aspect of his Internet usage without first obtaining a warrant. He could use third parties to create a bubble of Fourth Amendment protection around the entirety of his criminal activity.

The result would be a notable shift in the balance between privacy and security. If any observation of any part of the target's conduct violates his reasonable expectation of privacy, then the police would need a warrant to observe any aspect of his behavior. That is, they would need probable cause to believe that the evidence to be collected constitute evidence of the crime. But if the entire crime were protected by a reasonable expectation of privacy, they couldn't observe any aspect of the crime to develop that probable cause. The effect would be a Catch-22: The police would need probable cause to observe evidence of the crime, but they would need to observe evidence of the crime first to get to probable cause. In many cases, this would eliminate the use of third-party evidence in investigations altogether. By the time the police would have probable cause to believe that someone's third-party records are evidence of crime, they usually would already have probable cause to arrest and charge him with the crime.[87]

---

86. Further, the ability to harness outsourcing tools also often comes with a capacity to minimize the risk of betrayal. Criminals can control those in whom they confide, selecting only the most trustworthy to tell criminal secrets. The mob boss might require all his minions to prove their loyalty to him through deeds or a loyalty oath. The hacker will pick an Internet Service Provider that promises it will never under any circumstances cooperate with the police. For a rational criminal, all these steps make good sense. By only proceeding when the risk of betrayal is low, the criminal ensures the greatest chance of success for his criminal enterprise.

87. For investigators to obtain a probable cause warrant, they must establish ex ante a "fair probability" that evidence of the crime is located in the specific place the police wish to access. And "fair probability" ex ante turns into a high probability ex post: Studies have found that warrants prove successful—revealing the evidence sought—in the clear majority of cases. *See* RICHARD VAN DUIZEND ET AL., THE SEARCH WARRANT PROCESS 39 tbl.22 (1985) (reporting that warrants executed by the police yielded most or all of the items listed on the warrant in between sixty-four and eighty-two percent in the seven jurisdictions studied). Police will have such leads at the outset of investigations only rarely. In most cases they will begin with a victim's report or a crime scene or an anonymous tip; establishing probable cause about a particular wrongdoer and particular evidence

The third-party doctrine responds with a rule that ensures roughly the same degree of privacy protection regardless of whether a criminal commits crimes on his own or uses third parties. The part of the crime that previously was open to observation—the transaction itself—remains open to observation. The part of the crime that previously was hidden—what the suspect did without third parties in his home—remains hidden. The result leaves the Fourth Amendment rule neutral as to the means of committing the crime: Using a third party does not change the overall level of Fourth Amendment protection over the crime. If a person commits a crime on his own, the open part of the crime may be observed by the police without a warrant. If he harnesses a third party, the third party's involvement is treated as open, resulting in roughly the same amount of open conduct as the self-executed crime.

C. *Examples*

Examples help demonstrate how third parties create a substitution effect and how the third-party doctrine maintains the same degree of privacy protection regardless of whether third parties are used. In particular, consider the two most controversial applications of the third-party doctrine: the pen register installed in *Smith v. Maryland*,[88] and the bank account records retrieved in *United States v. Miller*.[89]

1. Smith v. Maryland—*Pen Registers*

Recall that in *Smith v. Maryland*,[90] Smith harassed a robbery victim by calling her repeatedly on the telephone. The police suspected Smith, and they asked the phone company to install a pen register device that would note any outgoing calls from his home phone. The pen register recorded the fact of the call to the victim, suggesting that Smith was the harasser and helping to provide the police with probable cause for a warrant to search his home.

To understand the substitution effect here, we need to see exactly how Smith used the third party of the telephone system to eliminate the public aspect of his crime. In a world without a telephone system, Smith would have been forced to stalk his victim the old-fashioned way. Smith would have left his house, walked to his car, and driven to his victim's home to harass her in person. Instead of having the phone company install a pen register, the police

---

requires a great deal of additional leads. Under the third-party doctrine, the police have many tools that they can use without probable cause to reach the probable cause threshold. They can ask around; they can go undercover; they can get bank records. Those tools may help prove the probable cause needed to obtain a warrant to search a home or to make an arrest. But if those tools *themselves* require probable cause, then in a practical sense those tools are no longer available to officers to help solve investigations.

88. 442 U.S. 735 (1979).

89. 425 U.S. 435 (1976).

90. *Smith*, 442 U.S. at 737–38.

would have assigned an officer to watch Smith from public streets and "tail" him around town. The officer would have watched Smith leave his home, enter his car, and drive to the victim's house.

When we introduce the third party of the telephone system, however, Smith no longer needs to leave home. To borrow from the old advertising campaign for the Yellow Pages, he can "let [his] fingers do the walking."[91] What formerly would have occurred in the open air now takes place inside the home using the third party of the telephone. Instead of watching Smith in public, the police now need to install a pen register to get the equivalent of the previously public information about what he was doing.

From this perspective, the Supreme Court's decision in *Smith v. Maryland* properly blocks Smith's attempted end-run around the balance of Fourth Amendment rules. Its conclusion that installation of the pen register is not a search matches the Fourth Amendment protection for third-party crimes to the preexisting protection for solo crimes. Smith's use of a third party withdrew his identity from public surveillance: Instead of having to travel to his victim, the telephone brought his victim to him (virtually, at least). The pen register information substituted for the same information that the police would have obtained by watching Smith on the public street. Smith's physical presence was not protected in the physical world version of the crime; under the third-party doctrine, his virtual presence is not protected in the third-party environment of the telephone network.[92]

2. United States v. Miller—*Bank Records*

Next consider *United States v. Miller*,[93] and its finding of no Fourth Amendment protection for bank records. The substitution effect is somewhat harder to see in this case, but I think it still explains the outcome. In *Miller*, the government wanted to prove that Miller had set up an illegal alcohol still. Prosecutors used Miller's bank records to show that he had purchased equipment for the still using his checking account.[94] In other words, the government used the checking account to prove a trade: Miller's

---

91. Paul R. La Monica, *Let your fingers do the walking*, CNNMONEY.COM, December 13, 2005, http://money.cnn.com/2005/12/13/news/fortune500/yellow.

92. During the editing stage, I learned that Ric Simmons recently made a similar argument about *Smith*. *See* Ric Simmons, *Why 2007 Is Not Like* 1984*: A Broader Perspective on Technology's Effect on Privacy and Fourth Amendment Jurisprudence*, 97 J. CRIM. L. & CRIMINOLOGY 531, 553–54 (2007). Simmons and I share a similar approach to how technology impacts Fourth Amendment protection; both of us have emphasized how technological change can both take away government power and expand it, and how Fourth Amendment rules respond to changes in both directions. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 864–67 (2004); Simmons, *supra*, at 535–36. Simmons ultimately condemns the third-party doctrine, calling it "dangerously short-sighted," but that is because he assumes that the doctrine must also apply to the contents of communications. Simmons, *supra*, at 555. As I explain in Section II.D, I do not think the third-party doctrine needs to apply to contents of communications. With that caveat, I agree with the basic approach of Professor Simmons.

93. 425 U.S. 435 (1976).

94. Specifically, Miller had written a check to rent a van and purchase radio equipment, sheet metal, and metal pipe. *See id.* at 438.

cash, drawn from the bank, in exchange for the items he was purchasing to build the still. The Supreme Court held that the Fourth Amendment did not protect Miller's bank records; specifically, it did not protect from government scrutiny the checks Miller had to written make those trades.[95]

In *Miller*, the checking account created a substitution effect by replacing a transaction that would have included substantial public components with a transaction that would normally occur entirely in private. To see how, imagine a world without banks. If you need to pay for something in this world, you would need to get the money to do it: You would need to travel to your stash, pick up the money, and then travel to the place where you are making your purchase. If you are the seller, you need to receive the money, take it back to your stash, and store it away for safekeeping. There are public parts of the transaction on both sides. Checks and other credit instruments eliminate the need to travel. The buyer no longer needs to travel to bring the money to the seller, and the seller no longer needs to travel to put the money away. Instead, the seller deposits the check and the funds from the bank are sent directly to him. The buyer and seller don't have to move anymore, as the check moves the funds out of and into their accounts without them needing to go anywhere. The third party of the checking account makes the entire economic transaction private.

Use of the third-party doctrine in the *Miller* case is plausible because checking services replace significantly public transactions with private ones. The third-party doctrine ensures that the same Fourth Amendment rules apply to checking account transactions that would have applied to the public transactions that they replace.

D. *Third Parties and Technology Neutrality*

I recognize that the model above is a bit artificial. It imagines a mythical year zero in which no third parties existed, whether of the human or mechanical type. Obviously, no such time existed. The model above also imagines that the substitution effect will occur equally in every case. It won't: Criminals can use third parties to withdraw the public portion of their crimes, but they certainly don't have to do so. In the *Smith* case, for example, Smith could have placed his anonymous stalking call from a public pay phone with the door open; or, in the modern equivalent, he could have used a cell phone in a crowded city street and spoken loudly so all could hear. If he had done this, using a third party would not have altered the open aspect of the crime.

---

95. The *Miller* court explained:

> The 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.

Id. at 443 (citations omitted).

At the same time, the somewhat simplified model reveals an essential dynamic about the use of third parties: In general, the use of a third party can create a substitution effect where the wrongdoer wishes it to do so. Hoffa could choose to speak only to close colleagues in the safety of his hotel room; Smith could choose to call his victim only from his own home phone. Use of a third party does not always have a substitution effect, but it enables the effect at the suspect's option. And any smart criminal will exercise the option. Those who have the most to hide have the most incentive to take advantage of how third-party services can hide their activity. Even without Fourth Amendment rules, third-party services will tend to hide otherwise public transactions. A rational actor bent on criminal conduct will use as many third-party services as he can to avoid detection.

Viewed from this perspective, the third-party doctrine is not some sort of mysterious hole in Fourth Amendment protection. To the contrary, it is a natural analog to the Supreme Court's decision in *Katz v. United States*.[96] *Katz* effectively required technological neutrality: Although its precise reasoning is opaque, it is often understood as concluding that telephone calls are protected because of the function they serve rather than the accident of the technology they use.[97] Indeed, this was the basic rationale of Justice Brandeis's dissent in *Olmstead v. United States*.[98] Brandeis feared that technological change could narrow Fourth Amendment protection: "Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."[99] Brandeis proposed that the Fourth Amendment should keep up as technology changed so that new technologies would not gut privacy.

But if we embrace this understanding of the Fourth Amendment, then surely it must be a two-way street. Just as the new technologies can bring "intimate occurrences of the home" out in the open, so can technological change and the use of third parties take transactions that were out in the open and bring them inside. If we accept that the Fourth Amendment should stay technology neutral, then we should accept that rule both when new technological practices threaten to expand Fourth Amendment protection as when they threaten to constrict it. Just as the Fourth Amendment should protect that which technology exposes, so should the Fourth Amendment permit access to that which technology hides. From this perspective, the third-party doctrine is needed to ensure the technology neutrality of the Fourth

---

96. 389 U.S. 347 (1967).

97. The *Katz* Court stated:

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

Id. at 352.

98. 277 U.S. 438, 471 (1928) (Brandeis, J., dissenting).

99. *Id.* at 474.

Amendment. It ensures that we have the same rough degree of Fourth Amendment protection independently of whether wrongdoers use third-party agents to facilitate their crimes.

More broadly, the third-party doctrine in no way undermines *Katz*, which famously held that the contents of a call from a public telephone receive Fourth Amendment protection. The contents of communications sent over third-party networks do not trigger substitution effects: The use of the network does not hide contents that previously were open. When a person visits another in his home, the fact of the visit occurs in public but the actual contents of their conversations remain shielded from observation. Extending the Fourth Amendment to contents of communications but excluding address information—as the Supreme Court did in *Katz* and *Smith*—maintains that status quo and follows a technologically neutral approach to constitutional protection.

III. The Third-Party Doctrine and Ex Ante Clarity

The second important role of the third-party doctrine is to foster ex ante clarity in Fourth Amendment rules. The on/off switch of the suppression remedy demands clear Fourth Amendment rules on what police conduct triggers Fourth Amendment protection and what police conduct does not.[100] The third-party doctrine creates ex ante clarity by matching the Fourth Amendment rules for information with the Fourth Amendment rules for location. Under the doctrine, rights in information extinguish when the information arrives at its destination. This means that the present location of information defines the Fourth Amendment rules for collecting it, and the Fourth Amendment rules are constant within each location.

Without the third-party doctrine, courts would have to develop some alternative test, with the same ex ante clarity, for identifying when information is protected under the Fourth Amendment. This task may not be impossible, but it is quite difficult. Few critics of the third-party doctrine have tried. And the difficulty of devising a clear alternative to the third-party doctrine provides a second argument in its favor.

A. *Ex Ante Clarity Under the Third-Party Doctrine*

To understand the importance of ex ante clarity, it is essential to recognize that the exclusionary rule provides the primary mechanism for enforcing the Fourth Amendment.[101] If the police violate a reasonable expectation of privacy and no exception applies, the evidence obtained ordinarily

100. *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 Stan. L. Rev. 503, 527 (2007) ("The Fourth Amendment's suppression remedy . . . generates tremendous pressure on the courts to implement the Fourth Amendment using clear ex ante rules rather than vague ex post standards.").

101. *See id.* at 527–28.

will be suppressed and the wrongdoer may go free.[102] The severe costs of the exclusionary rule require ex ante clarity in the rules for when a reasonable expectation of privacy exists. The police need to know when their conduct triggers Fourth Amendment protection. Uncertainty can both overdeter police from acting when no protection exists and can lead them to inadvertently trample on Fourth Amendment rights.[103]

The third-party doctrine ensures ex ante clarity by matching the Fourth Amendment rules for collecting information with the location of the information collected. When information arrives at its destination, the Fourth Amendment rules for collecting the information match with the rules for collecting other evidence there. This is true because rights in information extinguish when the information arrives at its destination; the information has been disclosed to its recipient, and any preexisting Fourth Amendment protection no longer exists.[104] This approach is essential to the clarity of Fourth Amendment rules because it guarantees that once information is present in a location it is treated just like everything else located there. Because the history of information is erased when it arrives, the law can impose rules as to what the police can or cannot do based on the known location of the search instead of the unknown history of the information obtained.

Consider a letter that arrives in the mail, is opened, and sits on the recipient's desk at home in a stack of other letters and other papers. The third-party doctrine dictates that the letter is treated just like all the other papers on the desk. The sender has Fourth Amendment rights in the letter during transmission, but once it arrives at its destination, those rights disappear.[105] If the police wish to search the home and come across a stack of papers including the letter, the Fourth Amendment rules they must follow will be set by the usual rules of home searches rather than special rules for each piece of paper defined by the history of each page. By erasing the history of information for Fourth Amendment purposes, the third-party doctrine ensures that all information in the same location is treated in the same way. This is critical because the police will normally know the status of the place they search but not the history of the items found inside it.

The significance of the ex ante clarity provided by the third-party doctrine is demonstrated by the surprising difficulty of developing alternatives to the doctrine that can retain that clarity. Under the third-party doctrine, if *A* tells a secret to *B*, *A* has no rights in *B*'s possession of the information. If the third-party doctrine is rejected, however, *A*'s rights in that information should continue even though *B* has the information now in addition to *A*. In other words, information should retain a history: The Fourth Amendment rules that apply to information should consider where the information has been in the past and in what circumstances it was held and disclosed. The

---

102. *See generally* Mapp v. Ohio, 367 U.S. 643 (1961) (applying the Fourth Amendment's suppression remedy to the states through the Fourteenth Amendment).

103. *See* Kerr, *supra* note 100, at 527–28.

104. *See supra* Section II.A.

105. *See* United States v. Villarreal, 963 F.2d 770, 774 (5th Cir. 1992).

question is, how far should those rights go? Should they extend forever? What should extinguish them? For the most part, the scholarly commentary has ignored this problem: Most scholars who criticize the doctrine do so without actually explaining what test should replace it.[106] But if it takes a theory to beat a theory, then surely it takes a doctrine to beat a doctrine. And it turns out to be quite difficult to devise a replacement for the third-party doctrine that would provide the needed clarity.

B. *Ex Ante Clarity Under a Probabilistic Alternative*

Because there are several different ways to determine when an expectation of privacy is reasonable,[107] it helps to consider two different alternatives to replace the third-party doctrine. One alternative is what I have termed the probabilistic model of Fourth Amendment protection.[108] Under this approach, whether government conduct violates a reasonable expectation of privacy depends on a fact-specific inquiry as to whether a reasonable person would have expected that the information would remain private.[109] This is a prospective inquiry from the standpoint of the suspect: The question is whether a reasonable person in the suspect's situation would expect the information to be widely disseminated. In this Section, I will explain why the probabilistic approach cannot create the needed clarity. A probabilistic approach would rest the inquiry on a largely unknowable question; the police would have difficulty applying the Fourth Amendment because they normally would be unable to reconstruct whether someone reasonably expected privacy in the information collected.

The core difficulty with applying a probabilistic approach to third-party information is that information's history is often complex and impossible to reconstruct. Just as a glass of water from a kitchen sink tap might have been rainwater in the Amazon thousands of years ago, information today often has a long past of interpersonal transmission. What a person knows and thinks reflects what he has seen, smelled, heard, touched, and felt. Our experiences reflect what the world has exposed to us. Many of those experiences hinge on what others thought and experienced long before us: Our thoughts are a combination of the views of generations past; our words are a pastiche of ourselves and others and the life experiences of many people at once. As a result, we can't model information transmission as a simple path from *A* to *B*. Rather, most transmissions will be a complex meandering journey from *A* to *B* to *C* to *D* to *E* with U-turns and curves along the way.

This complexity inhibits ex ante clarity for the police because they will necessarily collect information at the end of its dissemination, whereas judgments as to whether and when privacy is likely must be made prospectively.

---

106. *See, e.g.*, Solove, *supra* note 64, at 1083 (criticizing the third-party doctrine, but not proposing a clear alternative to it).

107. *See generally* Kerr, *supra* note 100, at 503.

108. *See id.* at 508–12.

109. *Id.*

From the perspective of the individual sending out information, who is curious about whether he will maintain his rights, he will assess whether the information recipient appears trustworthy. He might ask whether the recipient has a privacy policy, and might ask whether he has failed to maintain privacy in the past to predict what may happen in the future. But criminal investigators do not have this luxury. They must roll the tape backwards, starting with the present and trying to reconstruct the past. The determination of whether an expectation of privacy is reasonable in a probabilistic sense is highly contextual, and the context will be dramatically different at various transfer points in the history of information. As a result, the Fourth Amendment rules that the police must apply ex ante must hinge on details of the history of information that they cannot know ex ante and may be unable to reconstruct at all.

A simple example demonstrates the problem. Imagine that a federal prosecutor is a regular reader of CorruptionWatch.com, a blog about public corruption crimes. One day he visits the blog and finds an anonymous comment left by an unidentified reader: "I heard that Senator Smith was seen in public today depositing a $50,000 check from Jack Abramoff into Senator Smith's personal account at Ames Bank. Did Abramoff bribe him? Does anyone know? Email me at SenatorSmithsSecrets@gmail.com."

The prosecutor is curious about what the commenter knows, and he wants to subpoena the author of the comment. But what Fourth Amendment rule would govern such a subpoena? Under the third-party doctrine, the rule is the traditional one for issuing subpoenas. The history of the information is irrelevant to the legal rule that must be followed. But imagine a world in which the current third-party doctrine is replaced with a probabilistic model. Suddenly the Fourth Amendment rule is unclear. We do not know whether the subpoena will implicate Senator Smith's reasonable expectation of privacy because we don't know who the commenter is or how he came to know what he knows.

Consider five possibilities. In the first, the comment author is the bank teller who served Senator Smith and helped him deposit the check. In the second, the author is a fellow Ames Bank customer in line behind Senator Smith who overheard Senator Smith loudly announcing that he was there to deposit a $50,000 check from Jack Abramoff. In the third, the author is a bank robber who broke into the bank and looked through Senator Smith's files. In the fourth, the author is Jack Abramoff, who wants to get Senator Smith in trouble so he can negotiate a better deal with the feds. In the fifth, the author is Senator Smith himself, who was just curious to see if anyone would believe the story if he posted it online anonymously. In which of these cases would the subpoena violate Senator Smith's reasonable expectation of privacy under a probabilistic approach—that is, where a reasonable expectation of privacy is based on a probabilistic assessment of whether Senator Smith would reasonably expect his conduct to be widely disseminated? Perhaps the answer is that the first and third violate a reasonable expectation of privacy, the second and fifth do not, and the fourth depends on the details of the relationship between Smith and Abramoff. But how can

the police know this? They need to know what they will learn before they can know ex post if their conduct violated the Fourth Amendment.

And this is just the tip of the iceberg. Matters get much more complicated if the Fourth Amendment recognizes information history past the immediate question of the most recent "hop" back from its final resting point. For example, Joe might tell a secret to Jane, who might share it with Ben, who might write it in his diary that is stolen by Sarah, who might post it on a blog that is read by Earl, who might tell it in confidence to a government informant. Now ask the question: did the informant's learning the information violate anyone's reasonable expectation of privacy? We need to look past Earl, as we also need to answer the question for Sarah, Ben, Jane, and Joe. And for that matter, we need to know how Joe knew the secret in the first place; we need to trace the information to the very moment it appeared that someone's reasonable expectation of privacy might be violated. And of course all of that information must be known before the information is even acquired; somehow the police must know the detailed information history of information they have not yet seen. Under the third-party doctrine, these extremely difficult questions no longer need be asked. Information history becomes irrelevant.

C. *Ex Ante Clarity with a Policy-Based Alternative*

A second alternative to the existing third-party doctrine would be what I have termed a policy-based approach.[110] Under this approach, a reasonable expectation of privacy exists when, as a matter of policy, it is better for a particular practice to be regulated by a warrant requirement than for it to be unregulated by the Fourth Amendment.[111] When courts apply a policy model, they categorize the case before them and decide whether a reasonable expectation of privacy should extend as a matter of policy to that category of facts. A policy approach clearly can lead to greater clarity than the probabilistic method, as it provides a way for courts to generate rules that apply to categories of cases. However, generating clear Fourth Amendment rules based purely on policy considerations turns out to be relatively difficult.

In my view, there are two major difficulties with using policy-based rules to generate clear rules over third-party information. The first problem is that there are hundreds of potentially distinct applications of the third-party doctrine, and courts would need to apply the policy model to each of them to determine whether the information should be protected. The third-party doctrine is one size fits all; there is no need for case-by-case policy balancing. But if courts try to engage in policy balancing for each type of record, they will be forced to resolve how the balancing applies to a very wide range of cases. For example, many critics may want to overrule *Miller*, the case involving bank records, or *Smith*, the case involving pen registers.

---

110. *See id.* at 519–22.

111. *Id.*

But what about Fourth Amendment rules for credit card records? Electricity records? Gas meter records? Telephone records? Internet records? IP addresses? Book store records? Clothing store records? Record store records? iTunes accounts? Undercover agents wearing wires? Undercover agents not wearing wires? Until each of these questions was settled by the courts, agents would have no way of knowing how the law governed access to such information.

Second, because many applications of the third-party doctrine involve developing technologies, the outcome of a policy-based determination of how the Fourth Amendment should apply to third-party information can change over time.[112] Consider how the Fourth Amendment could apply to so-called trap-and-trace information: information obtained through the government's collection of incoming telephone numbers for a particular telephone account.[113] Until the spread of "caller ID" services, most individuals presumably thought of caller ID information as private; today, on the other hand, the disclosure of the incoming telephone number is simply a standard part of placing a telephone call. The changing social meaning of trap-and-trace information can create uncertainty for police investigators. If courts change the Fourth Amendment answer as the social meaning changes, how can police officers know when that will occur?

These challenges may not be insurmountable. Perhaps courts could hammer out rules for applying the Fourth Amendment to each of these types of records. Perhaps the answers would change only gradually and courts could keep up reasonably well. But at the same time, it is important to see that creating these doctrines would in fact pose a major practical challenge. All but a few critics have ignored this. As far as I know, only Professor Slobogin has attempted to offer a comprehensive alternative to the third-party doctrine.[114] Professor Henderson has offered a nine-factor totality-of-the-circumstances test,[115] but the factors and their application are so vague that they offer no clarity ex ante.[116] If critics want to replace the third-party doctrine with an alternative, they should be clearer about what that alternative would be and how it would apply in the wide range of cases courts regularly confront.

---

112. I have developed this argument in greater depth in Kerr, *supra* note 92, at 871–75.

113. *See generally* 18 U.S.C. § 3127(4) (Supp. V 2005) (defining trap-and-trace devices for purposes of the Pen Register statute).

114. SLOBOGIN, *supra* note 5, at 179–96. I critique Professor Slobogin's proposal elsewhere in this Volume of the *Michigan Law Review*. Orin S. Kerr, *Do We Need a New Fourth Amendment?*, 107 MICH. L. REV. (forthcoming April 2009) (reviewing SLOBOGIN, *supra* note 5).

115. Henderson, *supra* note 5.

116. Professor Henderson's nine factors are (1) the purpose of the disclosure, (2) the personal nature of the information, (3) the amount of information, (4) the expectations of the disclosing party, (5) the understanding of the third party, (6) positive law guarantees of confidentiality, (7) government need, (8) personal recollections, and (9) changing social norms and technologies. *Id.* at 975.

IV. Responding to Criticisms of the Third-Party Doctrine

The third-party doctrine is no panacea. Section I.B explained that the many critics of the third-party doctrine have made two primary arguments against it, one doctrinal and the other functional. The doctrinal claim is that the Justices are wrong when they contend that a person does not retain a reasonable expectation of privacy. According to these critics, people will often reasonably expect privacy in their third-party information.[117] The Justices misunderstand privacy because they fail to realize the difference between exposure to one person and exposure to the public.[118] The second argument, the functional claim, is that the third-party doctrine is incorrect because it gives the government too much power. It gives the police carte blanche power to access business records, and the prospect of abuses makes such powers inconsistent with a free society and therefore with the Fourth Amendment.[119]

This Part argues that while both criticisms have some force, both considerably overstate the case and ignore important counterarguments. First, the doctrinal argument ends up being mostly about form rather than substance. Although critics are right that the Court's applications of the *Katz* test to undercover agents and third-party records are awkward, that is largely because the third-party cases are better understood as consent cases. Disclosure to third parties eliminates protection because it implies consent. When the cases are understood as a subset of consent law rather than as applications of the reasonable expectation of privacy test, the doctrinal criticism ends up being much narrower than critics suggest.

The functional arguments about government power correctly note that the third-party doctrine permits invasive practices that could be abused by overzealous and even corrupt officials. However, they overlook the legal system's many substitutes for Fourth Amendment protection. In the absence of Fourth Amendment regulation, all three branches have created limits on the use of secret agents and access to business records that address many of the critics' concerns. Common law privileges, entrapment law, the *Massiah* doctrine, First Amendment doctrine, and statutory privacy protections have been designed specifically to address concerns of police harassment in the use of third parties.[120] Although the critics are justified in fearing abuses, they have wrongly viewed the Fourth Amendment in isolation. The full panoply of legal responses to third-party records and secret agents reveals that Fourth Amendment protection is only one among many legal tools to address these concerns. As a result, the functional argument against the third-party doctrine is significantly weaker than the critics imagine.

---

117. *See supra* Section I.B.1.

118. *See supra* Section I.B.1.

119. *See supra* Section I.B.2.

120. All of these doctrines are discussed *infra* Part IV.

A. *The Third-Party Doctrine as a Consent Doctrine*

First consider the doctrinal criticism that the Supreme Court is incorrect when it says that individuals cannot retain a reasonable expectation of privacy in third-party information. In my view, the doctrinal critics are partially right. The Supreme Court's applications of the reasonable expectation of privacy test to third-party information have been awkward and unconvincing. But the reason is that the third-party doctrine is better understood as a form of consent rather than as an application of *Katz*. Third-party disclosure eliminates privacy because the target voluntarily consents to the disclosure, not because the target's use of a third party waives a reasonable expectation of privacy. The difference is subtle but conceptually important, and I think it reveals that the doctrinal critique is a significantly narrower claim than critics believe.[121]

The notion of treating the third-party doctrine as a consent problem arguably goes back to the briefing of *Hoffa v. United States*[122] in 1966, the year before *Katz*. Hoffa's merits brief before the Supreme Court argued that the deception by a secret agent, Partin, had vitiated Hoffa's consent. Hoffa had been tricked, and his consent to let Partin listen in was no longer legally valid: "The Government's deception in hiding the informer under his [union] roles . . . prevented any intelligent and understanding waiver of Petitioner Hoffa's Fourth Amendment rights."[123] The government's brief responded that Partin's motive had not invalidated the consent: Hoffa had knowingly and intentionally admitted Partin into his private spaces and had shared evidence of his crime with Partin.[124] Having consented to Partin's presence, Hoffa had waived any Fourth Amendment rights.[125]

The Supreme Court should have accepted this consent-based formulation of the third-party doctrine. The parties in *Hoffa* accurately identified the issue raised by the third-party doctrine: When does a person's choice to disclose information to a third party constitute consent to a search? Further, the result in *Hoffa* sided with the correct answer: So long as a person knows that they are disclosing information to a third party, their choice to do so is voluntary and the consent valid. The fact that a person turns out to be an undercover agent should be irrelevant to whether the consent is valid, as that representation is merely fraud in the inducement rather than fraud in the factum.[126] A person who knowingly discloses information to a third party

---

121. A second response is that many critics wrongly assume that a probabilistic model of the "reasonable expectation of privacy" test is the only correct one. This is not true, as I have argued elsewhere. *See* Kerr, *supra* note 100.

122. 385 U.S. 293 (1966).

123. Brief for Petitioners at 35–36, Hoffa v. United States, 385 U.S. 293 (1966) (Nos. 32, 33, 34, 35).

124. Brief for the United States at 125–26, *Hoffa*, 385 U.S. 293 (Nos. 32, 33, 34, 35).

125. *Id.*

126. *See* ROLLIN M. PERKINS & RONALD N. BOYCE, CRIMINAL LAW 1079 (3d ed. 1982). Perkins and Boyce note:

may be tricked as to what the third party will do with the information. But trickery as to motive or design does not vitiate consent.[127]

How did the Supreme Court get off course? The critical juncture was *United States v. White*,[128] the first third-party case to follow *Katz*. In that case, Justice White tried to fit the third-party doctrine into the Court's post-*Katz* Fourth Amendment, but he simply chose the wrong doctrinal prong. Instead of grounding the doctrine in consent principles, he reasoned that use of a secret agent did not violate a reasonable expectation of privacy. The difference between the two is subtle: If government conduct does not violate a reasonable expectation of privacy, it is not a search,[129] whereas if it violates a reasonable expectation of privacy pursuant to consent, it is a search but one that is constitutionally reasonable.[130] At the same time, the two cover conceptually distinct ground. The reasonable expectation of privacy inquiry focuses on whether the government conduct intruded into constitutionally protected areas,[131] whereas consent asks whether it did so with permission.[132]

Later cases adopted Justice White's framework uncritically, establishing the third-party doctrine as an application of the *Katz* test.[133] But this doctrinal home never fit. Sharing space with others does not eliminate Fourth Amendment protection: The police need a warrant to enter a shared home just as much as they do an unshared one.[134] If two people share a home or an office, they still retain a constitutional reasonable expectation of privacy there.[135] Sharing space provides the co-occupant with common authority to permit their consent,[136] but it does not relinquish all Fourth Amendment protection. Similarly, the third-party doctrine is best understood as a shared space doctrine. By knowingly disclosing information to a third party, an individual consents to another person having control over it. The doctrine

---

> The general rule is that if deception causes a misunderstanding as to the fact itself (fraud in the *factum*) there is no legally-recognized consent because what happened is not that for which consent was given; whereas consent induced by fraud is as effective as any other consent . . . if the deception relates not to the thing done but merely to some collateral matter (fraud in the inducement).

Id.

127. *See id.* at 1075–84.

128. 401 U.S. 745 (1971).

129. Smith v. Maryland, 442 U.S. 735, 740 (1979).

130. *See* Georgia v. Randolph, 547 U.S. 103, 114–15 (2006).

131. *See* Kyllo v. United States, 533 U.S. 27, 31 (2001) (citing Silverman v. United States, 365 U.S. 505, 510–12 (1961)).

132. *See Randolph*, 547 U.S. at 114–15.

133. *See supra* Section II.B.

134. *See* Mancusi v. DeForte, 392 U.S. 364 (1968) (holding that a person retains a reasonable expectation of privacy in a shared office).

135. *Id.* at 369–70.

136. *See* United States v. Matlock, 415 U.S. 164, 171 n.7 (1974) (noting that "common authority" over spaces or property gives co-inhabitants the right to permit inspections of their own accord).

sounds in consent, not reasonable expectations of privacy, and it fits within the rest of Fourth Amendment law when so understood.[137]

Importantly, while this point narrows the scope of the doctrinal critique, it does not eliminate it entirely. In particular, it does not address cases like *Miller* where the government forces a third party to disclose records after the suspect voluntarily discloses the record to the third party. The suspect has consented to third-party access in such cases, but neither he nor the third party has consented to the subsequent government access. This is a fair point. But I think it is also a narrow one, as at this point the third-party doctrine becomes merely an application of the general rule that the Fourth Amendment does not regulate subpoenas to testify.[138] Any witness can be compelled to testify about what he knows and what he has seen without Fourth Amendment oversight,[139] and the third-party doctrine merely refrains from carving out an exception to this rule for confidential disclosures to third parties.

B. *Alternatives to Fourth Amendment Protections to Prevent Harassment—The Case of Secret Agents*

The second major criticism of the third-party doctrine is that it gives the police too much power.[140] The doctrine permits government officials to send in spies, use informants, get bank records, record numbers dialed, and obtain billing records of entirely innocent people without any cause or court-order requirement. According to critics, giving the government this much power is inconsistent with a free and open society; the risk of misuse and harassment is too great.[141]

The problem with this argument is that it assumes the Fourth Amendment is the only game in town. In truth, a wide range of tools exists for addressing police harassment of third-party information outside the Fourth Amendment. These tools substitute for Fourth Amendment protection, prohibiting or limiting access to third-party evidence in specific settings that may be subject to abuse. In the case of secret agents, the legal system uses entrapment law, the *Massiah* doctrine, the First Amendment, and internal regulations to limit the government's use of secret agents.

To be clear, there is considerable room for debate on the sufficiency of these substitutes for Fourth Amendment protection. The warrant requirement is strong medicine, and some of the nonconstitutional substitutes are modest by comparison. Most are designed to deter bad faith investigations

---

137. Notably, Professor Colb has argued that the Supreme Court's "knowing exposure" cases should be reanalyzed under consent principles. *See* Colb, *supra* note 67, at 123. However, Professor Colb does not focus this insight on the third-party doctrine cases specifically. Further, she does not suggest that the consent doctrine might help justify the existing third-party doctrine cases.

138. United States v. Dionisio, 410 U.S. 1, 9 (1973).

139. *See id.* at 10.

140. *See supra* Section II.B.2.

141. *See supra* Section II.B.2.

rather than to keep the government from accessing information altogether, and observers may disagree on which doctrines succeed or fail. But this should not obscure the deeper point: Fourth Amendment protection is only one tool among several for addressing police harassment. The absence of Fourth Amendment protection does not mean police practices go unregulated. Rather, it means a shift from regulation through a probable cause warrant requirement to regulation through privileges, entrapment doctrine, the Sixth Amendment, the First Amendment, statutes, and other forms of third-party protection.

In short, critics suffer from constitutional myopia. While they focus on the failure of the Fourth Amendment to stop government harassment and limit the power of the state, they tend to overlook the substitutes that already address the same concerns through other means. Properly conceived, the choice is not between Fourth Amendment protection and none, but rather between regulation by a diverse set of doctrines or that diverse set of doctrines plus the added protection of the Fourth Amendment. As a result, critics overstate the degree of government power that the third-party doctrine authorizes.

We can begin by considering how the law outside the Fourth Amendment tries to regulate secret agents. Although the Fourth Amendment does not regulate the use of secret agents,[142] four other bodies of law help fill in the gap: entrapment law; the *Massiah* doctrine; the First Amendment; and internal agency regulations. All four bodies of law deter abuses of secret agents. They prohibit the use of secret agents in some cases and ensure that they are used only in relatively limited ways in others.

1. *Entrapment Law*

Entrapment law provides the first substitute for Fourth Amendment regulation of secret agents. Entrapment is a judicially created doctrine,[143] recognized by statute in some states,[144] that regulates how the police use secret agents. Although there are several forms of entrapment law, the overarching purpose of the doctrine is to impose a requirement of reasonable police practices in the use of secret agents. If the police target an innocent person, one who has shown no predisposition to commit an offense, the undercover officer cannot induce the target into committing a crime.[145] "Inducement" occurs when the undercover agent pressures the suspect to commit the offense, either by badgering him or encouraging him to commit the offense in a way calculated to persuade the suspect based on his personality.[146] The remedy is an affirmative defense to prosecution rather

142. *See supra* Section I.A.1.

143. *See* 2 WAYNE LAFAVE ET AL., CRIMINAL PROCEDURE § 5.1(b) (3d ed. 2007).

144. *Id.*

145. *See, e.g.*, Sherman v. United States, 356 U.S. 369 (1958).

146. United States v. Gendron, 18 F.3d 955, 961–62 (1st Cir. 1994). Examples listed by then-Judge Breyer in *Gendron* include cases in which the secret agent (1) used intimidation and threats

than the suppression of evidence, meaning that the reasonableness of the government's conduct is evaluated by a jury instead of a judge.

Entrapment law does directly what critics of the third-party doctrine want done indirectly: It regulates abusive law enforcement practices targeting innocent defendants who are not actually suspected of a crime. The basic concern animating entrapment law is much the same as the concern animating the functional critique of the third-party doctrine: "The crucial question . . . is whether the police conduct revealed in the particular case falls below standards . . . for the proper use of governmental power."[147] But instead of regulating the use of undercover investigations ex ante, entrapment law prohibits their abuse in practice ex post. Instead of regulating *when* secret agents can be used, it regulates *how* they are used. The principles of entrapment law monitor the government's conduct, giving the jury a basis to acquit a defendant if the government implants the idea of the crime in the suspect's mind.

If the Fourth Amendment regulated secret agents, entrapment law would not be necessary. In such a world, the government would only use secret agents when it had probable cause that the suspect would reveal evidence of a crime, and that evidence would prove predisposition to defeat an entrapment defense.[148] Entrapment law has evolved as a byproduct of the third-party doctrine; it was created by the courts to fill in gaps that the third-party doctrine leaves open.

2. *The* Massiah *Doctrine*

The second substitute for Fourth Amendment regulation of secret agents is the *Massiah* doctrine. In *Massiah v. United States*,[149] the Supreme Court held that an agent of the government cannot question a person who has been charged with a crime.[150] Massiah had been indicted on drug charges, retained a lawyer, and was released on bail. Massiah later met with his co-conspirator Colson, and discussed his drug crimes with Colson when in Colson's car.[151] Unbeknownst to Massiah, Colson had flipped and was acting

---

against a defendant's family; (2) called every day, began threatening the defendant, and was belligerent; (3) engaged in forceful solicitation and dogged insistence until defendant capitulated; (4) played upon defendant's sympathy for informant's common narcotics experience and withdrawal symptoms; (5) played upon sentiment of one former war buddy for another to get liquor (during prohibition); (6) used repeated suggestions which succeeded only when defendant had lost his job and needed money for his family's food and rent; and (7) told defendant that she (the agent) was suicidal and in desperate need of money.

147. *Sherman*, 356 U.S. at 382 (Frankfurter, J., concurring).

148. If the government cannot use a secret agent without probable cause to believe that the agent will uncover evidence of crime from the target, presumably that means that the government has prior evidence that the target is predisposed to engage in criminal activity.

149. 377 U.S. 201 (1964).

150. *Id.* at 207 ("[W]e hold . . . that the defendant's own incriminating statements, obtained by federal agents under the circumstances here disclosed, could not constitutionally be used by the prosecution as evidence against *him* at his trial.").

151. *Id.* at 202–03.

as an informant for the government. Agents had bugged Colson's car and directed Colson to discuss his crimes with Massiah. An agent named Murphy listened in on the conversation and heard Massiah's incriminating statements.[152] At trial, Murphy testified about what he heard over Massiah's objection. When the *Massiah* case reached the Supreme Court, Massiah argued that the secret surveillance violated the Fourth, Fifth, and Sixth Amendments.[153]

The Supreme Court ruled that this use of a secret agent had violated Massiah's Sixth Amendment rights.[154] First, the Court held for the first time that a person who has been indicted and is represented by counsel has a right not to be questioned by an agent of the state outside the presence of his attorney.[155] Second, the Court held that the fact that the "agent" was a confidential informant made no difference.[156] Indeed, the fact that Massiah had been questioned by a confidential informant instead of a uniformed police officer made the violation of his rights more egregious: " 'Massiah was more seriously imposed upon . . . because he did not even know that he was under interrogation by a government agent.' "[157]

The *Massiah* doctrine regulates the use of third parties at the opposite end of the investigative process from entrapment law. Entrapment law concerns itself with how the government approaches suspects on the front end of investigations: The government cannot use third parties to create crime that otherwise would not have occurred. The *Massiah* doctrine concerns itself with how the government approaches suspects near the end of the process: Under *Massiah*, the government cannot use secret agents to obtain information about the crime from a target who has already been charged. While the Fourth Amendment permits the use of secret agents generally, the *Massiah* doctrine carves out one potentially abusive consequence of this rule by prohibiting the practice after a person has been represented by counsel.[158]

3. *The First Amendment*

The First Amendment may also impose restrictions on the use of undercover operations. Generally speaking, the First Amendment is implicated when government investigators infiltrate groups that engage in First

---

152. *Id.*

153. *Id.* at 203–04.

154. *Id.* at 205–06.

155. *Id.* at 207.

156. *Id.* at 206.

157. *Id.* at 206 (alteration in original) (quoting United States v. Massiah, 307 F.2d 62, 72–73 (2d Cir. 1962) (Hays, J., dissenting)).

158. This is true so long as the secret agent asks about the crime charged; the Sixth Amendment does not prohibit inquiries about unrelated crimes. *See* Texas v. Cobb, 532 U.S. 162, 172–74 (2001).

Amendment activities without a good faith reason for doing so.[159] This good faith test addresses one result that critics of the third-party doctrine fear the Fourth Amendment allows: investigations that are designed to target individuals exercising their First Amendment rights.

United States v. Mayer[160] offers a recent example. In *Mayer*, an undercover FBI agent infiltrated the North American Man/Boy Love Association ("NAMBLA"): a group that claimed to be " 'a political, civil rights and educational organization' " opposed to age-of-consent laws.[161] After becoming an active member of the group, the undercover agent encountered several discussions of illegal activity. One group member named Mayer expressed in frustration that "NAMBLA kept up pretenses of trying to change society when in fact its members only wanted to travel to meet boys."[162] The undercover agent then arranged a trip for NAMBLA members to meet boys, and Mayer signed up to go on the trip. When Mayer was arrested for traveling in interstate commerce with intent to engage in illegal sexual activities, he claimed that the government's infiltration of NAMBLA violated the First Amendment.

The Ninth Circuit explained that use of a secret agent to infiltrate a First Amendment-related group is permitted only when it is "justified by a legitimate law enforcement purpose that outweighs any harm to First Amendment interests."[163] The court found that this requirement was satisfied, under the circumstances, by reports of illegal activity the police had received relating to members of the NAMBLA group: Given the facts, the government's "interests in pursuing legitimate law enforcement objectives outweighed any harm to First Amendment interests."[164] Had the undercover investigation lacked a legitimate law enforcement purpose, or been undertaken to abridge First Amendment freedoms, then the investigation would have violated the First Amendment even though it did not implicate the Fourth Amendment.

4. *Internal Agency Regulations*

Internal agency regulations provide a fourth tool for limiting the use of secret agents. At the federal level, for example, the Justice Department has promulgated the *Attorney General's Guidelines on Federal Bureau of*

---

159. *Cf.* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958) (invalidating a production order for members of the local NAACP on the ground "that the production order, in the respects here drawn in question, must be regarded as entailing the likelihood of a substantial restraint upon the exercise by petitioner's members of their right to freedom of association").

160. 503 F.3d 740 (9th Cir. 2007).

161. *Id.* at 745.

162. *Id.* at 747.

163. *Id.* at 753.

164. *Id.*

Investigation Undercover Operations.[165] The *Guidelines* require the Special Agent in Charge of each FBI office to preapprove every FBI undercover investigation based on a written determination, supported by specific facts, that the proposed operation will be effective and will be conducted in a minimally intrusive way.[166] Undercover operations can be approved for up to six months and renewed for one more six month period.[167] They ordinarily cannot involve expenditures of more than $50,000.[168]

The *Guidelines* have special rules for particularly sensitive undercover investigations. FBI Headquarters must preapprove investigations of political organizations, religious groups, the news media, or public officials.[169] A Criminal Undercover Operations Review Committee consisting of FBI and DOJ officials meets to review these applications, and it must reach a consensus as to the appropriateness of each application.[170] If the Committee recommends approval of an application, it must include a statement as to why the operation merits approval in light of the sensitive nature of such investigations.[171] The Justice Department has promulgated roughly analogous guidelines for the use of confidential informants.[172] Like the limitations imposed by entrapment law, *Massiah*, and the First Amendment, these agency rules attempt to foreclose use of secret agents in bad faith or abusive contexts.

C. *Substitutes for Fourth Amendment Protection in Business Record Cases*

Just as several legal tools regulate the use of secret agents, there are many substitutes for Fourth Amendment protection of business records. The three legal tools that predominate are statutory protections, common law privileges, and rights of the third parties themselves. These doctrines regulate the government's access to business records outside the Fourth Amendment, deterring the kinds of abuses that critics fear may come to pass under the third-party doctrine. In some instances these tools require court orders or special cause to access third-party records; in other instances they block access to third-party records altogether. Taken together, these doctrines limit considerably the threat that the third-party doctrine poses to civil liberties. Once again, reasonable minds can differ about whether they do

165. JOHN ASHCROFT, ATT'Y GEN., THE ATTORNEY GENERAL'S GUIDELINES ON FEDERAL BUREAU OF INVESTIGATION UNDERCOVER OPERATIONS (2002), *available at* http://www.usdoj.gov/olp/fbiundercover.pdf.

166. *Id.* at 3–4.

167. *Id.* at 4.

168. *Id.*

169. *Id.* at 6.

170. *Id.* at 8.

171. *Id.* at 8.

172. *See* Department of Justice Guidelines Regarding the Use of Confidential Informants (Jan. 8, 2001), http://www.usdoj.gov/ag/readingroom/ciguidelines.htm.

enough in specific cases. But these doctrines help address the threat to privacy and individual rights that critics observe when viewing the third-party doctrine in isolation.

1. *Statutory Protections*

The most obvious alternatives to constitutional regulation for access to business records are statutory protections. Statutory privacy laws can impose a court-order requirement on government evidence collection even if the Fourth Amendment does not. The result can deter harassment of the innocent by introducing judicial supervision over investigations and effectively requiring officials to prove a legitimate government interest in the information sought.

For example, in response to *Smith*,[173] Congress enacted the Pen Register and Trap and Trace Devices Statute, codified at 18 U.S.C. 3121–3127.[174] *Smith* held that the Fourth Amendment does not limit the use of pen register devices to determine the numbers dialed from a telephone.[175] However, the Pen Register statute makes it a crime to install a pen register without a court order, subject to some exceptions. Obtaining a court order is quite easy under the statute: Investigators need only certify that "the information likely to be obtained . . . is relevant to an ongoing criminal investigation."[176] But this still imposes a good faith test: The law requires an actual ongoing investigation and a good faith belief in the likelihood that evidence to be obtained is relevant to that investigation.

Similarly, in response to *Miller*,[177] Congress enacted the Right to Financial Privacy Act ("RFPA").[178] RFPA responds to *Miller* by limiting government access to "the information contained in the financial records of any customer from a financial institution"[179] where the Fourth Amendment, thanks to *Miller*, does not. Under RFPA, the government can obtain such financial records with a subpoena only if the government has "reason to believe that the records sought are relevant to a legitimate law enforcement inquiry" and the government first provides the suspect with prior notice of the planned action that gives him an opportunity to move to quash the subpoena.[180]

In some cases, statutory protections for third-party records have been enacted even absent court decisions. For example, the Health Insurance

---

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

174. 18 U.S.C. §§ 3121–3127 (2000 & Supp. V 2005).

175. *Smith*, 442 U.S. at 743.

176. 18 U.S.C. § 3123(a) (2000).

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

178. 12 U.S.C. §§ 3401–3422 (2006).

179. 12 U.S.C. § 3402.

180. 12 U.S.C. § 3407.

Portability and Accountability Act ("HIPAA") protects medical records;[181] the Privacy Protection Act restricts government access to third-party records held by newsgathering organizations;[182] the Video Privacy Protection Act provides special privacy protections for video rental records;[183] the Stored Communications Act restricts access to email account records;[184] and the Cable Act restricts access to cable account records.[185] These laws all impose statutory restrictions on access to records that the third-party doctrine leaves unprotected under the Fourth Amendment.

In many (but not all) of these cases, the statutory privacy laws provide less protection than would the analogous Fourth Amendment standard of a probable cause warrant.[186] But that is a good thing rather than a bad one. The fact that standards are low prevents the end-run around the balance of Fourth Amendment rules that outsourcing can permit. At the same time, the standards are substantial enough to make it quite unlikely that the police would use the investigative powers solely to harass innocent suspects. In the case of financial records, a suspect could move to quash the subpoena, which would provide a court audience to hear his complaint of government overreaching. And in the case of pen registers, the government must first go to a judge and seek an order, certifying under oath that an ongoing investigation exists and that the information collected is likely to be relevant. These intermediate standards deter wrongful abuse while permitting legitimate investigations. They strike a middle ground not possible under the Fourth Amendment.

2. *Common Law Privileges*

Common law privileges provide a second tool for regulating access to business records. When a suspect has a privileged relationship with a third party, the third-party records cannot be accessed by the government. As a practical matter, the privilege trumps the third-party doctrine. It forces the government to take a hands-off approach to what otherwise might be very embarrassing information or important evidence of criminal activity.

The most obvious example of a privilege that trumps the third-party doctrine is the attorney-client privilege. In the federal system, privileges are recognized by Federal Rule of Evidence 501: "[T]he privilege of a witness [or] person . . . shall be governed by the principles of the common law as they may be interpreted by the courts of the United States in the light of reason and

---

181. 45 C.F.R. § 164.512(f)(1)(ii)(A) (2007) (permitting disclosure of medical records pursuant to "[a] court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer").

182. 42 U.S.C. § 2000aa (2000).

183. 18 U.S.C. § 2710.

184. 18 U.S.C. § 2703(c) (Supp. V 2005).

185. 47 U.S.C. § 551(h).

186. The major exception is the Cable Act, which allows disclosure of cable records only in very narrow circumstances. *Id.*

experience."[187] Under the attorney-client privilege, "[c]onfidential disclosures by a client to an attorney made in order to obtain legal assistance are privileged."[188] This rule encourages "full and frank communication between attorneys and their clients and thereby promote[s] broader public interests in the observance of law and administration of justice."[189] Evidence collected in violation of the privilege must be suppressed.[190]

The attorney-client privilege is not the only privilege recognized by federal courts. The Supreme Court recognized a psychotherapist-patient privilege in *Jaffee v. Redmond*.[191] And although the Supreme Court has not addressed the issue, lower federal courts have generally recognized a priest-penitent privilege.[192] All of these privileges effectively trump the third-party doctrine in specific settings where outsourcing of crime is particularly unlikely or there are powerful competing needs beyond evidence collection. A suspect is unlikely to use his attorney, his priest, or his psychotherapist to facilitate his crimes, and professional lawyers, clergymen, and psychologists are unlikely to be willing to participate in advancing a client's criminal scheme. At the same time, the privilege is needed to permit individuals to benefit from the advice of their lawyers, priests, and therapists. In these settings, the privilege effectively ameliorates the potential threat of government abuses raised by the third-party doctrine.

3. *The Rights of Third Parties*

The final tool for regulating government access to third-party business records is through the rights of the third parties themselves. In some cases, third parties in possession of business records may be willing to cooperate with the police. In many contexts, however, third parties may want to assert the rights of their customers. Protecting customer privacy is good for business, and third-party record holders often have a considerable incentive to keep the government at bay. An early illustration is the famous amicus brief that the telephone companies filed in the Supreme Court's first wiretapping case, *Olmstead v. United States*.[193] The phone companies urged the Supreme Court to rule that the government could not wiretap telephone lines.[194] Such a rule made good business sense for the telephone companies: It would both encourage customers to use the telephone and keep the government from interfering with their networks.

---

187. FED. R. EVID. 501.

188. Fisher v. United States, 425 U.S. 391, 403 (1976).

189. Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

190. *See* United States v. White, 887 F.2d 267, 275 (D.C. Cir. 1989).

191. 518 U.S. 1, 15 (1996).

192. Cox v. Miller, 296 F.3d 89, 102 n.6 (2d Cir. 2002) (citing cases).

193. 277 U.S. 438 (1928).

194. Brief for Pacific Telephone & Telegraph Co. et al. as Amici Curiae Supporting Petitioners, Olmstead v. United States, 277 U.S. 438 (1928) (Nos. 493, 532, 533).

A more recent example demonstrates how modern third-party providers can assert the rights of customers despite the third-party doctrine. In 2006, in the midst of civil litigation on the constitutionality of the Child Online Protection Act, the Department of Justice issued subpoenas ordering several search engine companies to disclose user queries for a two-month window.[195] DOJ claimed to need this information to determine how internet users used search engines to obtain pornography, which could then help determine the effectiveness of Internet filters.[196] When Google objected to the subpoenas, DOJ agreed to a narrower subpoena seeking a million random queries and all of the searches for a one-week window.[197] Google then continued to object, and moved to quash the subpoenas on the grounds that they sought information that was irrelevant and that production would be an undue burden. Google made the case somewhat creatively, arguing that "potential for loss of user trust" was a "burden" on Google that should require the subpoenas to be quashed.[198]

District Court Judge James Ware used these legal principles to fashion a narrow subpoena that protected the privacy interests of Google users. As modified by Judge Ware, the subpoena required Google to create a database that offered a random selection of 50,000 website addresses that could be accessed through the Google search engine.[199] Judge Ware raised sua sponte the question of the privacy interests of Google users—not Fourth Amendment privacy interests, to be clear, but more general privacy interests in the disclosure of information users had sent to Google in their queries.[200] Judge Ware noted that search queries could contain personal information, citing vanity queries or queries for sexually explicit information as examples of queries that raise privacy concerns.[201] And he fashioned a subpoena that would allow the government to conduct a study on Google's results without resulting in the disclosure of third-party queries made by users.

In a number of cases, third parties have also successfully asserted First Amendment interests of users in response to subpoenas allowed under the Fourth Amendment. For example, in *Doe v. Gonzales*,[202] a Connecticut Internet Service Provider successfully argued that the First Amendment afforded it a right to disclose service of a National Security Letter for third-party record information. In another recent subpoena case, a magistrate judge ruled that a grand jury subpoena for third-party records of book purchases violated the First Amendment by triggering a likely chilling effect on

---

195. *See* Declan McCullagh, *FAQ: What does the Google subpoena mean?*, CNET NEWS, Jan. 20, 2006, http://news.cnet.com/2100-1029_3-6029042.html.

196. *Id.*

197. *Id.*

198. Gonzales v. Google, Inc., 234 F.R.D. 674, 683 (N.D. Cal. 2006).

199. *Id.* at 688.

200. *Id.* at 687.

201. *Id.*

202. 500 F. Supp. 2d 379 (S.D.N.Y. 2007).

purchasing.[203] In addition, several courts have imposed First Amendment restrictions on subpoenas for third-party records in the civil context.[204]

I do not argue that third-party business record holders will always assert these arguments in defense of their customers. Indeed, recent headlines[205] about how telecommunications providers voluntarily assisted the NSA in collecting third-party records (quite possibly in violation of statutory privacy laws)[206] reaffirm that sometimes third-party providers will cooperate eagerly with the government. But the point is broader. Third-party business record holders can recognize the advantages of fighting for the privacy rights of their customers even absent Fourth Amendment protection. The prospect of resistance from the legal teams of third-party record holders often creates a substantial deterrence against government overreaching even when the third-party doctrine does not.

CONCLUSION

This Article has argued for a new understanding of the third-party doctrine. Critics of the doctrine portray it as a choice between all or nothing, between Fourth Amendment protection or no protection at all.[207] In their view, the third-party doctrine cases "make[] a mockery of the Fourth Amendment,"[208] leaving a constitutional void that is both illogical and inconsistent with a free society.[209] This Article has suggested that this widely held view tells only half the story. The third-party doctrine serves two important roles: blocking substitution effects that upset the technological neutrality of Fourth Amendment law and furthering clarity of Fourth Amendment rules. Further, the effects of the doctrine are much less dire than critics tend to suggest; the doctrine is only one tool among many for addressing abuses of third parties.

In short, both the costs and benefits of the third-party doctrine must account for substitution effects. On the cost side, fears of excessive government power must be offset by the substitution effects of doctrines like entrapment, common law privileges, statutory protections, and the *Massiah* doctrine. On the benefit side, courts should consider how the substitution

---

203. *In re* Grand Jury Subpoena to Amazon.com Dated Aug. 7, 2006, 246 F.R.D. 570, 573 (W.D. Wis. 2007).

204. *See generally* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112 (2007) (exploring the relationship between the First Amendment and criminal procedure).

205. *See, e.g.*, Jason DeParle, *Deal Close on Wiretap Law, a Top Democrat Tells CNN*, N.Y. TIMES, Mar. 3, 2008, at A13. Of course, by the time this Article is published, this story will be "old news"!

206. *See generally* Orin S. Kerr, Civil Liability and the NSA Call Records Program, http://www.orinkerr.com/2006/05/12/civil-liability-and-the-nsa-call-records-program/ (May 12, 2006, 17:00 EST).

207. *See supra* Section I.B.

208. 1 LAFAVE, *supra* note 7, § 2.7(b), at 736.

209. *See supra* Section I.B.

effects of third-party services can upset the traditional balance of Fourth Amendment rules. A full appreciation of the role of the third-party doctrine reveals it as much more complicated than critics have claimed. This does not mean that every application of the doctrine is indisputably correct; there is room for disagreement in specific cases, especially given the difficulty of weighing the costs and benefits involved. But when the entire picture is understood, the third-party doctrine has an important place within a proper system of criminal procedure rules.

More broadly, the role of the third-party doctrine reveals an all-too-common blind spot among criminal procedure scholars. Critics have often focused on powers of the government to harass innocent individuals, and have looked for ways that the Constitution can block the harassment.[210] But the Justices of the Supreme Court do not have this luxury. They must create rules that apply for investigations of both the innocent and the guilty in a world in which the government often cannot distinguish the two at the outset. They must look systemically to generate a set of rules that will apply to both.

From this perspective, the Fourth Amendment's warrant requirement is strong medicine—sometimes too strong. True, it deters abuse, but it also stops legitimate good faith investigations. At the preliminary stages of investigations, the police must have tools to gather evidence to determine if probable cause exists; the warrant requirement can then be saved for limiting more invasive practices like searches of homes and packages. While this removes Fourth Amendment scrutiny from a set of third-party practices, it tends to do so when the practices are essentially transactional—a matter of who did what, not what someone was thinking or saying or feeling. Other sources of privacy law can then fill the gap, deterring against abusive practices without imposing the high threshold of the Fourth Amendment's warrant requirement. The result is a system of procedural rules that both protects the innocent and permits investigations and prosecutions of the guilty.

Unfortunately, the Supreme Court has failed miserably at articulating these principles. When faced with the facts of specific cases, the Court has reached results that I think are correct. But by lodging the issue incorrectly in the reasonable expectation of privacy test instead of consent law, the Court has backed itself into a rhetorical corner and left the doctrine largely unexplained. The importance of third-party records in new technologies and the continuing criticisms of the Court's case law suggest that the time has come for courts and commentators alike to develop a more sophisticated understanding of the third-party doctrine. The doctrine should be recast rather than cast aside.

---

210. *See supra* notes 5–11 and accompanying text.