Article

Restoring Reason to the Third Party Doctrine

Lucas Issacharoff[†] **& Kyle Wirshba**[††]

INTRODUCTION

Since 1967, the Supreme Court has defined the protections of the Fourth Amendment as extending only to information in which one has "[a] reasonable expectation of privacy."[1] A key application of that principle is the third party doctrine, which allows the government to collect any information a criminal suspect has entrusted to a third party without falling afoul of the Fourth Amendment.[2] The basis for the rule is simple: once information is relinquished to another, its original owner loses any expectation of privacy he or she may once have had in the information.[3]

The third party doctrine has the virtue of simplicity and administrability. It also once had the great virtue of corresponding to the core intuitions of the citizenry in terms of expectations of privacy and confidentiality.[4] Unfortunately, the third party doctrine turned heavily on the limited forms of in-

---

† Law Clerk, Hon. Reena Raggi, United States Court of Appeals for the Second Circuit.

†† Law Clerk, Hon. Ronnie Abrams, United States District Court for the Southern District of New York. We would like to thank Professors Jack Goldsmith, Samuel Issacharoff, Orin Kerr, and Carol Steiker for their invaluable feedback.

1. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

2. *See* Orin S. Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009) (defining the third party doctrine).

3. *Id.*

4. *But cf.* Smith v. Maryland, 442 U.S. 735, 749–50 (1979) (Marshall, J., dissenting) (arguing that the third party doctrine, even at its inception, never corresponded to a realistic account of individuals' expectations of privacy); Couch v. United States, 409 U.S. 322, 342–44 (1973) (Douglas, J., dissenting) (arguing that taxpayers are forced by the tax code's complexity to use accountants as intermediaries, and that people have a reasonable expectation of privacy in the information they share with an accountant).

teraction in a prior technological era. As society has changed, the presumption of limited means of dissemination of information has all but collapsed, and the scope of what is covered by the third party doctrine has thus expanded. Communications, commerce, and finance increasingly take place online and operate through private intermediaries; accordingly, the third party doctrine has left an immense amount of personal information unprotected by the Fourth Amendment. The impact of these technological developments on police surveillance is most hotly debated today in the field of data mining,[5] but the third party doctrine is implicated at every level of law enforcement, from cops on the beat to the National Security Agency.

Perhaps bowing to the inevitable, in 2012 five justices of the Court in *United States v. Jones*[6] suggested that the third party doctrine could no longer be maintained in its current, absolute form, although the same five justices were unable to offer a controlling alternative. The necessity of doctrinal overhaul was further reinforced by the Court's recent decision in *Riley v. California*.[7] In evaluating the search of a cell phone incident to a suspect's arrest, the Court unanimously found that rapid technological change and societal expectations had rendered impracticable the simple application of a pre-digital Fourth Amendment doctrine. These acknowledgments of doctrinal desuetude have only increased the tempo of suggested alternatives. Proposals for doctrinal tweaks of the doctrine are virtually a cottage industry today, but the various critiques are for the most part chasing a moving target of evolving technology. Instead, reform must engage the twin aims of the doctrine in terms of protecting citizen expectations of privacy and providing rational tools for law enforcement.

This Article takes up the challenge left open by the incomplete resolution in *Jones.* Attempting to fill this doctrinal void, we look not to further tweaks from within the third party doctrine but instead to the Court's development of the exceptions to the Fourth Amendment's Warrant Clause. Following this doctrinal foundation, we believe that courts can determine the

5. *See, e.g.*, Joseph T. Thai, *Is Data Mining Ever a Search Under Justice Stevens's Fourth Amendment?*, 74 FORDHAM L. REV. 1731, 1735 (2006) (arguing data mining and the third party doctrine adversely affect the protections provided by the Fourth Amendment); Note, *Data Mining, Dog Sniffs, and the Fourth Amendment*, 128 HARV. L. REV. 691, 693–701 (2014) (analyzing how data mining is regulated by the Fourth Amendment, how it is outside the scope of a search, and providing available alternatives).

6. 132 S. Ct. 945, 957–60 (2012).

7. 134 S. Ct. 2473, 2493–95 (2014).

reasonableness of third party searches through a uniform standard that both protects legitimate expectations of privacy in the citizenry and at the same time is easily administrable by law enforcement. We argue that this standard offers a workable middle ground between the current absence of constitutional protection of information in the hands of third parties and the overburdening of law enforcement that the imposition of warrant and probable cause requirements would entail.

In Part I we discuss the third party doctrine, examining its roots and its current state of flux following *Jones*, as well as the critiques leveled against it. In Part II we evaluate the potential judge-made replacements put forward by courts and scholars, concluding that they cannot offer a satisfactory solution. In Part III we offer a new doctrinal approach. Looking to other cases in which searches are deemed to fall outside the Warrant Clause, we argue that third party searches are better characterized as a new type of warrant exception than as either a search subject to the warrant and probable cause requirements or a nonsearch unregulated by the Fourth Amendment. Thus, our proposal shifts the focus of analysis from whether or not examination of information in the hands of third parties should be considered a search to when such a search is reasonable. In Part IV we examine *Terry v. Ohio*[8] as a model for how courts could apply such a reasonableness inquiry while avoiding the pitfalls of freeform judicial balancing. Instead of weighing the interests at stake in each case, courts should weigh the interests at stake in third party searches as a general matter, and then craft a reasonable suspicion standard that can be applied on a uniform basis. Finally, in Part V we assess the limitations and potential applications of this new test for third party searches.

I. THE RISE AND FALL OF THE THIRD PARTY DOCTRINE

A. THE EVOLUTION OF THE THIRD PARTY DOCTRINE

As with much of Fourth Amendment jurisprudence, the starting point for the third party doctrine is *Katz v. United States*[9] and its "reasonable expectation of privacy" test.[10] In that case, the government's interception of Katz's call from a public phone booth was deemed a search because Katz, despite being outside his home, had a reasonable expectation that his call

8. 392 U.S. 1 (1968).
9. 389 U.S. 347, 360–62 (1967) (Harlan, J., concurring).
10. *Id.* at 360.

would remain private.[11] *Katz* overturned a prior decision refusing to find a Fourth Amendment search in similar circumstances;[12] the earlier decision had rested upon the fact that the police had eavesdropped upon the defendant's phone call from the street and thus did not enter any constitutionally protected space.[13] The *Katz* Court declared that "the Fourth Amendment protects people, not places," and renounced the theory that Fourth Amendment interests must be tied to property.[14] The Supreme Court would later adopt a two-part framework for the *Katz* test,[15] first asking whether an individual had a subjective expectation of privacy in the information, and then whether that expectation is one that "society is prepared to recognize as reasonable."[16]

Following *Katz*, the Court was faced with the task of squaring the reasonable-expectation-of-privacy test with cases allowing the use of undercover agents or informants in whom suspects had placed their trust.[17] In those prior cases, the Court had held that 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."[18] In 1971, the Supreme Court found that the earlier cases survived the *Katz* test.[19] It held that "however strongly a defendant may trust an apparent colleague, his expectations in this respect are not pro-

11. *Id.*

12. *Id.* at 352–53 (majority opinion).

13. Olmstead v. United States, 277 U.S. 438, 464 (1928) (stating that "the sense of hearing" does not constitute a search or a seizure).

14. *Katz*, 389 U.S. at 351. As the majority held in *Jones*, the *Katz* test supplemented rather than supplanted the physical trespass doctrine of *Olmstead*. *See* United States v. Jones, 132 S. Ct. 945, 950–54 (2012); *Olmstead*, 277 U.S. at 466.

15. The test is based on Justice Harlan's *Katz* concurrence, which was applied by the Supreme Court thereafter. *See Jones*, 132 S. Ct. at 950 ("Our later cases have applied the analysis of Justice Harlan's concurrence in [*Katz*], which said that a violation occurs when government officers violate a person's 'reasonable expectation of privacy.'").

16. Bond v. United States, 529 U.S. 334, 338 (2000) (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

17. *See, e.g.*, Lewis v. United States, 385 U.S. 206, 211–12 (1966) (admitting evidence of undercover officer despite entry into defendant's home); Hoffa v. United States, 385 U.S. 293, 311 (1966) (admitting evidence of confidential informant); Lopez v. United States, 373 U.S. 427, 440 (1963) (admitting evidence of bribe of undercover agent wearing a wire); Lee v. United States, 343 U.S. 747, 757–58 (1952) (admitting evidence of undercover informant wearing a wire).

18. *Hoffa*, 385 U.S. at 302.

19. *See* Kerr, *supra* note 2, at 568–69.

tected by the Fourth Amendment when it turns out that the colleague is a government agent."[20]

Systematizing this principle, the Court articulated the third party doctrine in a series of cases throughout the 1970s. First, in *Couch v. United States*[21] and *United States v. Miller*,[22] the Court found that the defendants had no reasonable expectation of privacy in records given to an accountant in *Couch*[23] and a bank in *Miller*.[24] Relying in part on the undercover cases, the Court reasoned that any person "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[25] Therefore, the Court explained,

> 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.[26]

Then, in 1979, the Court expanded the third party doctrine in *Smith v. Maryland*.[27] Moving beyond business records, *Smith* approved the admission at trial of data from a pen register—or a device that keeps track of dialed numbers—obtained without a warrant.[28] Investigating threatening and obscene phone calls following a robbery, law enforcement officers asked the phone company to install a pen register to record the phone numbers dialed by their primary suspect, Smith.[29] When the pen register confirmed that Smith had been calling the victim, police used the information to obtain a search warrant for Smith's home and thereafter secure an indictment and conviction.[30] Though the police had no warrant for the pen register, the Court denied Smith's argument that the pen register should have been suppressed. It held, consistent with *Couch* and *Miller*, that because Smith "voluntarily conveyed numerical information to the tele-

---

20. United States v. White, 401 U.S. 745, 749 (1971). Although *White* rested on only a plurality, Justice Black's concurrence was quite broad, signaling the holding rested with Justice White's plurality opinion. *See* Kerr, *supra* note 2, at 568 n.38.

21. 409 U.S. 322 (1973).

22. 425 U.S. 435 (1976).

23. *Couch*, 409 U.S. at 335–36.

24. *Miller*, 425 U.S. at 445–46.

25. *Id.* at 443 (citing *White*, 401 U.S. at 751–52).

26. *Id.*

27. 442 U.S. 735 (1979).

28. *See* Kerr, *supra* note 2, at 570.

29. *Smith*, 442 U.S. at 747.

30. *Id.*

phone company and 'exposed' that information to its equipment in the ordinary course of business," he could "claim no legitimate expectation of privacy."[31] Further, whether or not the phone company independently chose to keep track of these phone records was of no moment; "that [the phone company] had facilities for recording and that it was free to record" was sufficient.[32]

Thereafter, the Supreme Court[33] and circuit courts[34] dutifully reaffirmed the third party doctrine until the D.C. Circuit's and the Supreme Court's decisions in *United States v. Jones*.[35] *Jones*, discussed more fully below, turned on whether extended Global Positioning System (GPS) monitoring violated the Fourth Amendment. While the case itself did not directly implicate the third party doctrine, five justices in concurring opinions indicated a willingness to rethink parts of the doctrine.[36] Justice Sotomayor went so far in her concurring opinion as to note that, given advances in technology, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[37] She reasoned that the third party doctrine

> is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.[38]

Following Justice Sotomayor's dicta, the solid edifice of the third party doctrine has begun to erode. While some courts con-

---

31. *Id.* at 744.

32. *Id.* at 745.

33. *See, e.g.*, California v. Greenwood, 486 U.S. 35, 41 (1988) (relying on *Smith* in finding no expectation of privacy in garbage left on curtilage); United States v. Payner, 447 U.S. 727, 736–37 (1980) (refusing to suppress evidence stolen from the defendant's banker on third party doctrine grounds).

34. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 330–31 (6th Cir. 2010) (finding that e-mail metadata—primarily to/from addresses—fall within the third party doctrine); United States v. Forrester, 512 F.3d 500, 509 (9th Cir. 2008) (refusing to suppress website visitation information acquired by computer surveillance).

35. United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd in part sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

36. *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring in the judgment).

37. *Id.* at 957 (Sotomayor, J., concurring) (citing *Smith*, 442 U.S. at 742; United States v. Miller, 425 U.S. 435, 443 (1976)).

38. *Id.*

tinue to adhere to the doctrine's strictures,[39] other judges have seized on the *Jones* concurrences and found a reasonable expectation of privacy in telephonic metadata and cell-site data.[40]

Two terms ago, the Court dealt another indirect blow to the third party doctrine. In *Riley v. California*,[41] the Court refused to extend the traditional Fourth Amendment exception for searches incident to arrest to searches of an arrestee's cellphone. Decades earlier, in *United States v. Robinson*,[42] the Court had upheld the "unqualified authority of the arresting officer to search the arrestee's person" and accompanying effects.[43] The Government argued that searches of cellphones were "materially indistinguishable" from the searches of wallets, purses, and other effects that had been upheld under *Robinson*,[44] and the *Riley* Court acknowledged that a "mechanical application of Robinson might well support the warrantless searches at issue here."[45] Yet the Court found that mechanically equating wallets and cellphones would be "like saying a ride on horseback is materially indistinguishable from a flight to the moon . . . . Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a ciga-

39. *See, e.g.*, *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (allowing the collection of cell site data under the third party doctrine); ACLU v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013) (permitting the mass collection of telephonic metadata), *vacated*, 785 F.3d 810, 824–25 (2d Cir. 2015) (discussing *Jones* and noting the "seriousness of the constitutional concerns" implicated by the National Security Agency's mass collection of metadata).

40. *See, e.g.*, United States v. Graham, 796 F.3d 332, 344–61 (4th Cir. 2015) (finding the third party doctrine inapplicable based in part on the *Jones* concurrences), *reh'g en banc granted*, Nos. 12-4659(L), 12-4825, 2015 WL 6531272 (Oct. 28, 2015); United States v. Davis, 754 F.3d 1205, 1215 (11th Cir. 2014) (endorsing the *Jones* mosaic theory but finding it "not necessary to establish the invasion of privacy in the case of cell site location data"), *rev'd en banc*, 785 F.3d 498, 511 (11th Cir. May 5, 2015) ("[L]ike the bank customer in *Miller* and the phone customer in *Smith*, Davis has no subjective or objective reasonable expectation of privacy in MetroPCS's business records showing the cell tower locations that wirelessly connected his calls at or near the time of six of the seven robberies. . . . We find no reason to conclude that cell phone users lack facts about the functions of cell towers or about telephone providers' recording cell tower usage."); Klayman v. Obama, 957 F. Supp. 2d 1, 33 (D.D.C. 2013), *vacated*, 800 F.3d 559 (D.C. Cir. 2015).

41. 134 S. Ct. 2473, 2494–95 (2014).

42. 414 U.S. 218, 229, 235 (1973).

43. *Id.* at 229.

44. *Riley*, 134 S. Ct. at 2488.

45. *Id.* at 2484.

rette pack, a wallet, or a purse."[46] The Court went on to conclude that

> [m]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life." The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.[47]

More directly relevant to the third party doctrine, the Court noted that evolving technology might render other digital-analog comparisons inapplicable: "Is an e-mail equivalent to a letter? Is a voicemail equivalent to a phone message slip?"[48] The assumption of technological neutrality between such analog and digital communications has been critical to defenses of the third party doctrine,[49] and the Court's apparent rejection of this assumption undermines the doctrine's foundation.

Today the third party doctrine remains an important part of Fourth Amendment law, but has been called into serious question by cases that did not directly resolve questions over its vitality and extent. It is worth considering, therefore, whether the third party doctrine deserves to survive, and if so in what form.

B. EVALUATING THE THIRD PARTY DOCTRINE

Academics and the lower courts have long been sharply critical of the third party doctrine, though notably almost invariably on the expectation of privacy side of the divide, with correspondingly little attention to the legitimacy of law enforcement objectives.[50] Following *Katz*'s formulation, scholars have launched a two-fold critique of the third party doctrine: first, that people's subjective expectations of privacy do not accord with the third party doctrine, and second, that society should not discount these expectations as unreasonable.

Technological change, many argue, has shifted people's subjective expectations of privacy. At one time, the argument

---

46. *Id.* at 2488–89.

47. *Id.* at 2494–95 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

48. *Id.* at 2493.

49. *See, e.g.*, Kerr, *supra* note 2, at 579–81 (discussing the drawbacks of the analog test).

50. Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 585 (2011) ("While *Smith* and the Third Party Doctrine were heavily criticized even before the Internet age, the drumbeat of criticism has intensified . . . ." (footnotes omitted)).

often goes, a person's decision to provide information to third parties may have evinced a lack of expectation of privacy, but current expectations are different. In modern digital society, individuals routinely use the Internet to communicate and to store information that they would regard as quite private.[51] For example, the growth of "cloud storage" subjects significantly more private data to the third party exception.[52] Whereas data may once have stayed tucked away on a computer as it could in a file cabinet, once stored on the cloud it would be subject to law enforcement's prying eyes.[53] Putting this intuition to the test, one study has exposed the increasing disconnect between actual and doctrinal expectations of privacy: people surveyed reported that they regard many types of information falling squarely within the third party doctrine (and thus unprotected by the Fourth Amendment) as significantly more private than other types that are protected by the Fourth Amendment, thus requiring law enforcement to demonstrate reasonable suspicion or even probable cause.[54]

Critics further argue that the basic conception of privacy inherent in the third party doctrine is outmoded. The doctrine defines privacy as an on/off trigger—nondisclosure keeps information private, while any disclosure completely waives one's privacy interest. The doctrine refuses to recognize the real possibility that individuals could disclose information to third parties for limited purposes. But there is no reason to "treat[] exposure to a limited audience as morally equivalent to exposure

---

51. *See generally* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1571 (2004) (questioning whether privacy standards set by the ECPA provide adequate protection).

52. Cloud storage is the warehousing of digital information on a shared server owned by a third party instead of on local hard drives. *See* Aaron J. Gold, *Obscured by Clouds: The Fourth Amendment and Searching Cloud Storage Accounts Through Locally Installed Software*, 56 WM. & MARY L. REV. 2321, 2323 (2015) ("[C]loud storage is a term for storing data and files on remote drives.").

53. *See* William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1223 (2010) (arguing that free cloud services are not protected); *see also* David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2219–20 (2009) ("[I]s it not reasonable to consider a digital account containing the same types of materials [as a briefcase], stored in the cloud rather than on a computer hard drive, as serving that purpose as well?").

54. *See* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 184, 186 (2007) (finding that government examination of email metadata is regarded as more invasive than pat downs and vehicle searches).

to the whole world."[55] In fact, a more nuanced conception of privacy might be desirable, as it could encourage the sharing of sensitive information[56] and prevent the creation of "Information Age hermits" unwilling to meaningfully participate in digital society.[57]

Technology has also altered whether such subjective expectations should be regarded as objectively reasonable. Not only do people expect privacy on the Internet, critics of the third party doctrine argue, but they also should be entitled to that expectation of privacy. Transacting in sensitive information through the Internet is, in many ways, no longer a choice. Justice Marshall expressed such concerns in his dissent in *Smith*:

> Implicit in the concept of assumption of risk is some notion of choice. . . . [H]ere, unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of "assuming" risks in contexts where, as a practical matter, individuals have no realistic alternative.[58]

Justice Marshall's critique has even more force today, when eighty percent of Americans now rely on the Internet daily.[59] As more vital services move online, it will become increasingly difficult to apply for jobs,[60] access government services,[61] or even communicate without using the Internet.[62] Many have

---

55. 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) ("[T]reating exposure to a limited audience as identical to exposure to the world[] means failing to recognize degrees of privacy in the Fourth Amendment context.").

56. *See id.* at 123 ("[O]ne might choose to forfeit some of her freedom from exposure without thereby forfeiting all of it.").

57. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 217 (2004) (arguing that maintaining the third party doctrine mantra "if people want to protect privacy, they should not share their information with third parties," will create "Information Age hermits").

58. Smith v. Maryland, 442 U.S. 735, 749–50 (1979) (Marshall, J., dissenting).

59. Tokson, *supra* note 50, at 588.

60. *See* Anushka Asthana & Tracy McVeigh, *Government Services To Be Online-Only*, OBSERVER (Nov. 20, 2010), http://www.guardian.co.uk/society/2010/nov/20/government-services-online-only.

61. *See* DARRELL M. WEST, BROOKINGS, STATE AND FEDERAL ELECTRONIC GOVERNMENT IN THE UNITED STATES 2–3 (2008), http://www.brookings.edu/~/media/research/files/reports/2008/8/26%20egovernment%20west/0826_egovernment_west.pdf (explaining how government services are increasingly being moved online).

62. Leslie Meredith, *U.S. Considers "Internet Access for All,"* TECHNEWSDAILY (Jan. 28, 2010, 9:45 AM), http://www.livescience.com/8062-considers-internet-access.html (reporting on the increasing role governments are taking in making sure their citizens have access to the internet, and how

argued that routing private information through the Internet is now simply inevitable.[63] Given this inevitability, Professor Richard A. Epstein contends that use of third party intermediaries cannot be regarded as consent to government surveillance, or even as a legitimate assumption of the risk of surveillance.[64]

From a functional perspective,[65] some maintain that the third party doctrine exposes individuals to too much government snooping.[66] Because "it is not far-fetched for government officials to amass data for use in silencing or attacking enemies, critics, undesirables, or radicals,"[67] the third party doctrine prevents the courts from using the Fourth Amendment as a tool to limit government misbehavior.[68] Such concerns have not only led eleven state supreme courts to interpret their constitu-

---

that affects communication).

63. *See, e.g.*, SOLOVE, *supra* note 57 ("[P]eople . . . have little choice but to hand over information to third parties. Life in the Information Age depends upon sharing information with a host of third party companies."). In this vein, some scholars have argued that internet access is a human right. *See* Young Joon Lim & Sarah E. Sexton, *Internet as a Human Right: A Practical Legal Framework To Address the Unique Nature of the Medium and To Promote Development*, 7 WASH. J.L. TECH. & ARTS 295, 315 (2012) (exploring the protection of the internet as a human right). Thus far France, Estonia, Finland, Greece, Spain, and the United Nations Human Rights Council have declared internet access to be a human right. *See* Brandon Wiebe, *BART's Unconstitutional Speech Restriction: Adapting Free Speech Principles to Absolute Wireless Censorship*, 47 U.S.F. L. REV. 195, 219 (2012) (discussing the restriction of the Internet during times of crisis).

64. Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199, 1205 (2009) ("[S]uppose the government gave notice to the world that it would engage in surveillance of all private activities at will; so draw your curtains, but the government can still peek through. People would have to alter their conduct in order not to assume the risk. No one would accept such unilateral legislative declaration as sufficient to undermine constitutional rights that are intended to limit the scope of permissible government action.").

65. *See* Kerr, *supra* note 2, at 572–73 (describing what Professor Kerr calls "the functional critique" of the third party doctrine).

66. Thai, *supra* note 5 ("[T]he Court has handed the government a blank check to conduct mass surveillance through data mining third-party records for suspicious persons and activities.").

67. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1112 (2002) (cataloguing instances of government misuse of personal data).

68. *See generally* Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1272 (1983) ("[The Fourth Amendment] has been restricted so much that it fails to offer innocent citizens the protection to which they should be entitled under the fourth amendment.").

tions to avoid the doctrine,[69] but have also led Congress to resist the broad exposure, passing the Right to Financial Privacy Act in response to *Miller* and the Pen Register Act in response to *Smith*.[70]

C. WHY A JUDICIAL SOLUTION?

The legislative responses to the privacy concerns engendered by the third party doctrine—including the Right to Financial Privacy Act, the Pen Register Act, the Electronic Communications Privacy Act of 1986,[71] and the recently passed USA FREEDOM Act of 2015[72]—raise the possibility that the third party doctrine should simply be left alone. To the extent it is flawed, legislatures, rather than courts, may be the proper agents to calibrate law enforcement needs with privacy concerns. The two main arguments for this position are that legislative solutions possess flexibility unavailable to constitutional law, and that the tradeoff between security and privacy is appropriately within the realm of democratic accountability.

Professor Orin Kerr has argued that such legislative "intermediate standards deter wrongful abuse while permitting legitimate investigations. They strike a middle ground not possible under the Fourth Amendment."[73] Yet as Kerr himself has acknowledged, this argument "assumes the standard all-or-nothing options of Fourth Amendment law,"[74] where an investigative technique is either a search, requiring a warrant supported by probable cause, or not a search, in which case no protections apply. Adding an intermediate category—particularly, as proposed here, one that incorporates a reasonableness standard—significantly diminishes the inflexibility objection.

---

69. *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, 376 (2006) (documenting state court decisions on adoption of the third party doctrine).

70. *See* Elspeth A. Brotherton, *Big Brother Gets a Makeover: Behavioral Targeting and the Third-Party Doctrine*, 61 EMORY L.J. 555, 576 (2012) (citing Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, tit. XI, 92 Stat. 3697 (codified as amended at 12 U.S.C. §§ 3401–22 (2012)); Pen Register Act, Pub. L. No. 99-508, tit. III, 100 Stat. 1868 (1986) (codified as amended at 18 U.S.C. §§ 3121–27 (2012))).

71. Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

72. Pub. L. No. 114-23, tit. L, 129 Stat. 268.

73. Kerr, *supra* note 2, at 597.

74. Orin S. Kerr, *Defending the Third-Party Doctrine: A Response to Epstein and Murphy*, 24 BERKELEY TECH. L.J. 1229, 1232 (2009).

The second objection is standard to any proposal to raise the floor of constitutional protections: why not allow society, through democratic mechanisms, to set its own tradeoffs? And relatedly, why not allow states to experiment with different heightened protections, as many are already doing?[75] There are three reasons why the protection of one or more legislatures is insufficient. First, and most basically, rights are "rights" because their enforcement does not depend on the acquiescence of others: "[F]undamental rights may not be submitted to a vote; they depend on the outcome of no elections."[76] The Supreme Court has recently reaffirmed this principle in response to a suggestion that privacy concerns with regard to evolving technology are best left to administrative protocols: "Probably a good idea, but the Founders did not fight a revolution to gain the right to government agency protocols."[77]

Second, democratic mechanisms may be particularly suspect when it comes to regulating police practices. Majorities will often perceive, correctly, that the brunt of the costs of intrusive police practices are borne by others: "The core justification for legal enforcement of rights is the risk that a majority will *not* bear the burdens of its laws but instead will abridge the liberties of a powerless or despised minority."[78] Professors Tracey L. Meares and Dan M. Kahan have noted the example of sex offender registration,[79] while others have linked the rise of modern constitutional criminal procedure to the need to curb majority abuse of minority populations in the Jim Crow South.[80] While rising minority political participation somewhat ameliorates such concerns, post-September 11th police practices and the targeting of certain groups suggests the continued need for judicial enforcement of rights.[81]

---

75. *See* Henderson, *supra* note 69.

76. Obergefell v. Hodges, 135 S. Ct. 2584, 2606 (2015) (quoting W. Va. State Bd. of Educ. v. Barnette, 319 U.S. 624, 638 (1943)).

77. Riley v. California, 134 S. Ct. 2473, 2491 (2014).

78. Tracey L. Meares & Dan M. Kahan, *The Wages of Antiquated Procedural Thinking: A Critique of* Chicago v. Morales, 1998 U. CHI. LEGAL F. 197, 209.

79. *Id.* ("A requirement that sex offenders register with local authorities after being released from prison is a notable example.").

80. *See* David Alan Sklansky, *Police and Democracy*, 103 MICH. L. REV. 1699, 1729 (2005) ("[T]he Court's initial forays into state criminal procedure are best understood as responses to . . . cases in which Black defendants were sentenced to death with barely the façade of trial.").

81. *See* OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, SUPPLEMENTAL REPORT ON SEPTEMBER 11 DETAINEES' ALLEGATIONS OF ABUSE AT THE METROPOLITAN DETENTION CENTER IN BROOKLYN, NEW YORK, (Dec.

Finally, the federalism-based democratic response is unsatisfying where the collection and analysis of third party information will often cross state lines. Citizens of one state may be relieved to know that the legislature of their state has protected them from overbroad collection of information by state authorities, or prosecution by those authorities based on such collection, but where fifty other sovereigns collect information across state lines the protections of a single state may be somewhat ephemeral.[82]

It is not our intent to rehash the shortcomings of the third party doctrine, which have been thoroughly dissected in the academic literature.[83] We largely agree with those critiques, but express some doubt as to whether courts and scholars have identified a viable alternative. In the next Part we examine the success of those critiques in identifying a promising alternative to the third party doctrine, and subsequently we offer and evaluate our own (hopefully superior) alternative.

II. SURVEYING THE ALTERNATIVES TO THE THIRD PARTY DOCTRINE

Despite the near-consensus that technological development has altered the expectations of privacy around third party information, both courts and the academy have struggled to develop a workable scheme for determining which third party information the Fourth Amendment should protect, and what should remain available to police investigations without judi-

---

2003) (describing post-9/11 abuses against Muslims in Brooklyn federal prison); *see also* Turkmen v. Hasty, No 13-981, 2015 WL 3756331, at *38 (2d Cir. June 17, 2015) (reinstating *Bivens* claims against high-level executive officials after 9/11).

82. *See generally* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1403 (2001) (documenting state and federal collection of data).

83. *See, e.g.*, SLOBOGIN, *supra* note 54; SOLOVE, *supra* note 57; Epstein, *supra* note 64; Jessica K. Fink, *Protected by Association? The Supreme Court's Incomplete Approach To Defining the Scope of the Third-Party Retaliation Doctrine*, 63 HASTINGS L.J. 521, 534 (2012); Tokson, *supra* note 50, at 588; Aubrey H. Brown III, Note, Georgia v. Randolph*, The Red-Headed Stepchild of an Ugly Family: Why Third-Party Consent Search Doctrine Is an Unfortunate Fourth Amendment Development that Should Be Restrained*, 18 WM. & MARY BILL RTS. J. 471, 473 (2009); Colleen Maher Ernst, Note, *Looking Back To Look Forward: Reexamining the Application of the Third-Party Doctrine to Conveyed Papers*, 37 HARV. J.L. & PUB. POL'Y 329, 336 (2014); Matthew D. Lawless, Note, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, UCLA J.L. & TECH., Fall 2007, at 1, 33–35; Loewy, *supra* note 68, at 1234. *See generally* Kerr, *supra* note 2, at 570–73 (collecting scholarship).

cial oversight. Competing and complementary theories have been advanced from across the ideological spectrum. These theories can be separated into three groups: the mosaic theory originating in the courts; categorization approaches crafted by different scholars; and case-by-case balancing pushed by more textualist thinkers.

A. MOSAIC THEORY

The first approach, "mosaic theory," was developed by the D.C. Circuit in *United States v. Maynard*,[84] and has since been carried forward by other judges[85] and academics.[86] Most significantly, five Supreme Court justices signaled agreement with the underlying principles of the mosaic theory in the course of affirming *Maynard* in *United States v. Jones*.[87]

The D.C. Circuit in *Maynard* reversed Antoine Jones's conviction because it found that the government's extended surveillance using GPS data had violated the Fourth Amendment.[88] During their investigation, police tracked Jones's movements using a GPS device planted on a car for twenty-eight days.[89] In finding that a search occurred, Judge Ginsburg compared the aggregation of data to the creation of a mosaic in which the whole reveals more than the sum of its parts.[90] In Freedom of Information Act (FOIA) cases, the government has

84. 615 F.3d 544 (D.C. Cir. 2010), *aff'd in part sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

85. *See, e.g.*, United States v. Pineda-Moreno, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc); *id.* at 1126–27 (Reinhardt, J., dissenting from denial of rehearing en banc) ("[C]ourts have gradually but deliberately reduced the protections of the Fourth Amendment to the point at which it scarcely resembles the robust guarantor of our constitutional rights we knew when I joined the bench."); *In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 543 (D. Md. 2011); *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 840 (S.D. Tex. 2010), *vacated*, 724 F.3d 600 (5th Cir. 2013); *In re* Application of U.S. for an Order Authorizing Release of Historical Cell-Site Info., 736 F. Supp. 2d 578, 585 (E.D.N.Y. 2010).

86. *See, e.g.*, David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381, 411 (2013); Benjamin M. Ostrander, *The "Mosaic Theory" and Fourth Amendment Law*, 86 NOTRE DAME L. REV. 1733, 1765 (2011). *But see* Courtney E. Walsh, *Surveillance Technology and the Loss of Something a Lot Like Privacy: An Examination of the "Mosaic Theory" and the Limits of the Fourth Amendment*, 24 ST. THOMAS L. REV. 169, 233 (2012) (concluding that the mosaic theory is unworkable).

87. 132 S. Ct. 945 (2012).

88. *Maynard*, 615 F.3d at 549.

89. *Id.* at 558.

90. *Id.* at 561.

made use of the mosaic theory, warning that "[d]isparate items of information, though individually of limited or no utility to their possessor, can take on added significance when combined with other items of information."[91] Analogizing to this oft-taken FOIA position,[92] the *Maynard* court found that "[w]hat may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene."[93] To a greater extent than when the key Fourth Amendment precedents had been decided, knowledge of "all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, . . . an unfaithful husband, . . . an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts."[94]

On appeal, though the Supreme Court ultimately decided the case on a "narrower basis,"[95] two Justices penned concurrences indicating approval of the application of the mosaic theory to the Fourth Amendment. Justice Alito, speaking for four justices, and Justice Sotomayor, writing for herself, believed "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[96] As noted in Part I, other judges have since followed the lead of Justices Alito and Sotomayor, applying the mosaic theory to find the third party doctrine inapplicable and upholding an expectation of privacy even in situations where information was somehow no longer privately held.[97]

---

91. Bethany L. Dickman, Note, *Untying* Knotts*: The Application of Mosaic Theory to GPS Surveillance in* United States v. Maynard, 60 AM. U. L. REV. 731, 736 (2011) (quoting David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628, 630 (2005)).

92. *See* Anna-Karina Parker, *Dragnet Law Enforcement: Prolonged Surveillance & the Fourth Amendment*, 39 W. ST. U. L. REV. 23, 32 n.20 (2011); Julian Sanchez, *GPS Tracking and a "Mosaic Theory" of Government Searches*, CATO INST. (Aug. 11, 2010, 9:22 PM), http://www.cato.org/blog/gps-tracking-mosaic-theory-government-searches ("The theory holds that pieces of information that are not in themselves sensitive . . . can nevertheless be withheld, because in combination . . . [they] permit the inference of facts that are sensitive . . . ." (emphasis omitted)).

93. *Maynard*, 615 F.3d at 561 (quoting CIA v. Sims, 471 U.S. 159, 178 (1985)).

94. *Id.* at 562.

95. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring). Writing for the majority, Justice Scalia relied upon the physical trespass of the tracking device onto Jones's car, arguing that the trespassory theory of the Fourth Amendment had survived the decision in *Katz*. *Id.* at 949–51 (majority opinion).

96. *Id.* at 955 (Sotomayor, J., concurring) (quoting *id.* at 964 (Alito, J., concurring in the judgment)).

97. *See, e.g.*, Klayman v. Obama, 957 F. Supp. 2d 1, 36 (D.D.C. 2013) (cit-

While the mosaic theory has intuitive appeal—that the accumulation of vast amounts of information can pose a threat to privacy greater than the sum of its parts—it works better as a metaphor than as a constitutional doctrine. Despite the evocative imagery, the mosaic theory faces a significant hurdle due to its impracticality as an administrable standard for both law enforcement and courts. At what point does any unit of information interact with other data to form the recognizable mosaic? The mosaic theory complicates "all of the problems of line drawing which must be faced in any conscientious effort to apply the Fourth Amendment."[98]

The most obvious problem with such an approach is determining what amount of information constitutes a mosaic as opposed to a scattered collection of tiles.[99] Justice Alito recognized this pitfall when he noted that the Court "need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark."[100] Line drawing problems are presented, however, not only in the duration and scope of investigation, but also in determining which investigative techniques add to the mosaic and how investigations should be grouped across officers, departments, or sovereigns.[101] While many have taken up the mantle of the mosaic theory,[102] no one has advanced satisfying answers to these difficult line-drawing questions.[103]

---

ing *Maynard*, 615 F.3d at 562–63) ("Records that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic—a vibrant and constantly updating picture of the person's life."), *vacated*, 800 F.3d 559 (D.C. Cir. 2015). *But see* ACLU v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013) (reaching the opposite conclusion on nearly identical facts), *vacated*, 785 F.3d 787 (2d Cir. 2015).

98. Rakas v. Illinois, 439 U.S. 128, 147 (1978).

99. *See* Walsh, *supra* note 86, at 236–37.

100. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment).

101. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 333–36 (2012).

102. *See, e.g.*, Dickman, *supra* note 91; Parker, *supra* note 92, at 32; Priscilla J. Smith et al., *When Machines Are Watching: How Warrantless Use of GPS Surveillance Technology Violates the Fourth Amendment Right Against Unreasonable Searches*, 121 YALE L.J. ONLINE 177, 201 (2011); Erin Smith Dennis, Note, *A Mosaic Shield:* Maynard*, the Fourth Amendment, and Privacy Rights in the Digital Age*, 33 CARDOZO L. REV. 737, 770–71 (2011); Justin P. Webb, Note, *Car-ving Out Notions of Privacy: The Impact of GPS Tracking and Why* Maynard *Is a Move in the Right Direction*, 95 MARQ. L. REV. 751, 788–96 (2012).

103. Kerr, *supra* note 101, at 346 ("I find it particularly telling that not even the proponents of the mosaic theory have proposed answers for how the theory should apply." (citing Smith et al., *supra* note 102)); *see also* Brief of Yale Law School Information Society Project Scholars and Other Experts in

Yet even if a standard could be reasonably set, the mosaic theory is further flawed because of its continued reliance on a search/nonsearch distinction. Under the theory, aggregation of data amounting to a mosaic constitutes a search subject to the full warrant and probable cause requirements of the Fourth Amendment, but only slightly fewer data points entirely evade Fourth Amendment scrutiny. Such a wide gap between outcomes separated by so little additional aggregation will lead to arbitrary and inconsistent results. To make matters worse, the threshold between search and nonsearch may not be apparent to either the individual under surveillance or to law enforcement compiling the final piece of the puzzle. This means that neither the citizen nor the police officer knows where the boundary lines are *ex ante* in terms of conduct, but only *ex post* in terms of results.

B. CATEGORIZATION

In search of a solution to the third party doctrine problem, other authors have taken to categorization as a means of articulating coherent Fourth Amendment principles.[104] The critical benefit of such an approach is to give clearer *ex ante* commands than would be possible under the mosaic approach. In turn, this puts great pressure on the ability to draw lines around certain forms of communication or conduct that can be subject to a clearer regulatory approach. The categorization strategy therefore typically identifies a special category for exemption, relies on empirical studies, or creates a totally new scheme.

One strategy is to identify certain categories of information particularly well suited for exemption from the current third party doctrine; these categories typically are identified in the digital sphere and thus sit on the forefront of technological change. Social networking data is one particularly compelling category.[105] Arguments in favor of heightened protections for

---

the Law of Privacy and Technology as Amici Curiae Supporting Respondent at 25–27, *Jones*, 132 S. Ct. 945 (No. 10-1259), 2011 WL 4614429, at *25–27.

104. *See* Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 309 (2003) (noting that although there "exists among privacy scholars a general consensus that privacy law and theory must change to meet the needs of the digital age," no agreement on achieving that goal has appeared).

105. *See, e.g.*, Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1, 27 (2013); Saby Ghoshray, *Privacy Distortion Rationale for Reinterpreting the Third-Party Doctrine of the Fourth Amendment*, 13 FLA. COASTAL L. REV. 33, 67–68 (2011); Stephen E. Henderson, *Expectations of Privacy in Social Media*, 31 MISS. C. L. REV. 227, 247 (2012); Katherine J. Strandburg, *Home, Home on the Web and*

social networks proceed both from a Fourth Amendment basis—arguing that individuals have a reasonable expectation of privacy in social networking data[106]—and from a First Amendment basis—arguing that protections are needed lest law enforcement activity chill novel digital communication.[107] As social relationships and interactions increasingly extend into cyberspace, scholars argue, courts should extend the protections typically afforded to such interactions when they occur in the analog world.[108] As one scholar puts it, putting information on the Internet does not make it any less private because "life in the twenty-first century occurs in cyberspace."[109]

Yet identifying which data constitute social networking information can prove difficult. Different theories such as "interpersonal privacy,"[110] "technosocial extension,"[111] and "[f]reedom of [a]ssociation [f]ramework"[112] attempt to draw lines between less important digital communication, which the police are free to intercept, and data requiring protection. For example, one scholar attempts to differentiate a permissible law enforcement sting in a public chat room from a police officer's "friending" a suspect on Facebook with a fake account, because the former is more similar to interactions that occur in a public space.[113] Yet both appear to contain an element of voluntary disclosure or waiver, making it difficult to cleanly identify one as more public than the other.[114] Even if the line could be drawn, what

Other Fourth Amendment Implications of Technosocial Change, 70 MD. L. REV. 614, 675 (2011).

106. *See, e.g.*, Henderson, *supra* note 105, at 239.

107. *See, e.g.*, Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 795 (2008); *see also id.* at 751 ("For these emergent associations, and even for traditional associations that make extensive use of digital communications, the potential chilling effects of relational surveillance are profound.").

108. *See* Strandburg, *supra* note 105.

109. Ghoshray, *supra* note 105, at 67.

110. Bedi, *supra* note 105, at 59 (advocating the protection of Facebook friendships because they maintain the same aspects of "interpersonal privacy" as offline relationships).

111. Strandburg, *supra* note 105, at 664 (defining social networks as "a technosocial extension of the home or office").

112. Strandburg, *supra* note 107 (advocating for judges to "view the Fourth Amendment through a special First Amendment lens in cases implicating expressive activity"); *see also* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 163 (2007) (suggesting that the First Amendment can provide an independent means for protecting third party information from government investigation).

113. *See* Strandburg, *supra* note 105, at 671–75.

114. *See* Bedi, *supra* note 105, at 28 ("It is not clear why these types of dis-

about activity that falls between the two, such as gaining access to a members-only message board?

Categorization based on empirical studies is another strategy for updating the third party doctrine. Advocates of this strategy utilize survey data to test the public's reasonable expectation of privacy in various areas.[115] Professor Christopher Slobogin has conducted the most comprehensive such study, attempting to measure the public's perception of the level of intrusiveness of different government interventions.[116] Slobogin uses these data to inform his longstanding proportionality proposal for the Fourth Amendment, in which different levels of protection shield various categories of information.[117] Under this theory, the more intrusive the public regards a police tactic, the greater protection the third party information implicated receives.[118] Thus, records about a corporation would require a subpoena supported by the relevance standard, whereas publicly held personal records could be accessed with a "*Terry* Or-

closures do not stand or fall together . . . .").

115. *See, e.g.*, Aya Gruber, *Garbage Pails and Puppy Dog Tails: Is That What* Katz *Is Made of?*, 41 U.C. DAVIS L. REV. 781, 829 (2008) (advocating for use of empirical data in future Fourth Amendment decisions); Tokson, *supra* note 50, at 622–27; Sonia K. McNeil, Note, *Privacy and the Modern Grid*, 25 HARV. J.L. & TECH. 199, 215 (2011) ("[T]he Court's interpretation of the third-party doctrine has fallen out of step with the 'reasonable expectations' of the people whom the Fourth Amendment protects. Empirical evidence offers one way to resolve the dissonance between the Court's opinion and public opinion."); *see also* Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 46–49 (2011) (using Tokson's survey).

116. 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, 728 (1993) (examining an extensive survey in which 217 subjects were presented with questions intending to determine their perception of intrusiveness in response to fifty scenarios).

117. Christopher Slobogin, *Let's Not Bury* Terry*: A Call for Rejuvenation of the Proportionality Principle*, 72 ST. JOHN'S L. REV. 1053, 1082 (1998). Though Professor Slobogin identifies *Terry v. Ohio* as valuable inspiration for a reexamination of the third party doctrine, he focuses on the proportionality principles instead of the usefulness of the Court's one-time balancing. *Compare id.* at 1056–57 ("This relaxation of the probable cause standard can be, and largely was, justified on proportionality grounds . . . ."), *with infra* Part IV (advocating for an evaluation of reasonableness in third party searches).

118. Slobogin & Schumacher, *supra* note 116, at 757–58 ("Under proportionality analysis, rankings [of search intrusiveness] . . . would serve as a useful device for determining how much 'probable cause' is necessary to conduct a particular search or seizure.").

der," in effect a warrant supported by reasonable suspicion rather than probable cause.[119]

The proportionality model, however, suffers from two major shortcomings: unreliable data and rigidity. First, surveys are a poor way to measure expectations of privacy. Not only are surveys difficult to administer,[120] quickly out of date,[121] and highly sensitive to slight variations in phrasing,[122] but also respondents tend to overstate privacy interests.[123] Of course, courts can ascribe different degrees of protection based upon sensitivity without recourse to survey data. Professor Orin Kerr has noted that the New Jersey Supreme Court has taken this approach, "appl[ying] a balancing test that considers 'the type of protection' that should be afforded 'in the face of legitimate investigative needs' that 'will arise [and] justify State intrusion upon that interest.'"[124] Yet while such proportional approaches at first appear quite flexible, their reliance on categorization breeds rigid and potentially arbitrary line-drawing.[125] While Slobogin has added a "quasi-private" category to his initial distinction between publicly and privately held records, for example,[126] one cannot envy the jurist forced to distinguish private records from quasi-private records, and quasi-private records from public records, in an endless series of technologically evolving iterations.

---

119. Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139, 169 (2005).

120. Tal Z. Zarsky, *Governmental Data Mining and Its Alternatives*, 116 PENN ST. L. REV. 285, 320–21 (2011) ("Yet administering such surveys would be a very difficult, perhaps near-impossible task.").

121. Orin S. Kerr, *Do We Need a New Fourth Amendment?*, 107 MICH. L. REV. 951, 964–65 (2009) ("[W]hat if public opinion changes over time—should the courts change the rule when public opinion changes, such as after a terrorist attack or the release of an influential movie about surveillance?").

122. *Id.* at 964 ("Survey responses can be highly sensitive to the audience, to the phrasing of the question, and to the timing of the survey.").

123. Daniel J. Solove, Essay, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1522–24 (2010) (outlining academic research indicating survey respondents overstate privacy interests when compared to their revealed preferences, as the same individuals willingly give up privacy for small benefits).

124. *See* Kerr, *supra* note 121, at 965 (latter alteration in original) (quoting State v. Reid, 945 A.2d 26, 35 (N.J. 2008); State v. McAllister, 875 A.2d 866, 875 (N.J. 2005)).

125. *See id.* at 964 ("Slobogin's approach also appears unnecessarily complicated.").

126. *Compare* SLOBOGIN, *supra* note 54 (containing an updated chart with more categories), *with* Slobogin, *supra* note 119 (using a chart to demonstrate proposed categories).

Most ambitiously, a final strategy attempts to completely reframe the protective scheme for third party material through categorization. In one well-thought-out example, Professor Daniel Solove attempts to "[r]econstruct[] the [a]rchitecture" by drawing a new line in the sand for the protection of third party material.[127] He proposes borrowing from the Privacy Act, disallowing the government from obtaining without legal process any "system of records," defined as "a group of any records . . . from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[128] This distinction, he claims, separates information obtained coercively by the private sector or hospitals from that given freely to friends and neighbors.[129] But if the third party doctrine as it currently exists is overly lenient toward the government, restricting access to any system of records is likely too burdensome.[130]

Ultimately, the categorical approach has not yielded a satisfactory solution. Third party information may once have been susceptible to categorization, but as the types of information trusted to third parties proliferate and the need to divulge information to a variety of actors becomes unavoidable,[131] such an endeavor becomes increasingly Sisyphean. The source of categorization's demise may stem from its reliance on bright-line rules—long thought to be incompatible with the Fourth Amendment.[132] Judicially created rules have many pitfalls, including their preemption of legislative alternatives;[133] but it is bright-line rules' inflexibility that most plagues categoriza-

127. Solove, *supra* note 67, at 1151.

128. SOLOVE, *supra* note 57, at 214 (quoting 5 U.S.C. § 552(a)(5) (2012)).

129. *See id.* at 216 ("Currently, employers and landlords have a substantial amount of power to extort personal information.").

130. *See* Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 1019 (2007) ("Solove's solution is overinclusive. It would require probable cause before the police could obtain everything from basic subscriber information to the most personal of records." (footnote omitted)).

131. SOLOVE, *supra* note 57, at 216 ("[P]eople . . . have little choice but to hand over information to third parties. Life in the Information Age depends upon sharing information with a host of third party companies.").

132. *See* Albert W. Alschuler, *Bright Line Fever and the Fourth Amendment*, 45 U. PITT. L. REV. 227, 230 (1984) (describing Professor Wayne LaFave's longstanding opposition to bright line rules in the Fourth Amendment context).

133. *See* Kyllo v. United States, 533 U.S. 27, 51 (2001) (Stevens, J., dissenting) ("It would be far wiser to give legislators an unimpeded opportunity to grapple with these emerging issues rather than to shackle them with prematurely devised constitutional constraints.").

tion.[134] In the ever-evolving and expanding world of digital information,[135] the inflexibility of bright-line rules will lead inevitably to difficulties in administration.[136] Under such a system, judges would be left with the unenviable task of creating new categories—further complicating an already complex scheme—or making unjust decisions, potentially damaging the court's credibility.[137]

C. BALANCING

A third approach for rethinking the third party doctrine relies on a single inquiry into reasonableness. Most famously, Professor Akhil Amar argues that the Fourth Amendment's Reasonableness and Warrant Clauses are disjunctive, and should be read without reference to one another.[138] Thus, investigatory tactics should be evaluated not with reference to probable cause or the existence of a warrant, but only with regard to the reasonableness of law enforcement action.[139] Reasonableness being a broad inquiry, Amar outlines the potential process through which judges could look for reasonableness: "Common sense tells us to look beyond probability to the importance of finding what the government is looking for, the intrusiveness of the search, the identity of the search target, the availability of other means of achieving the purpose of the search, and so on."[140] Fourth Amendment decision-making, then, requires bal-

134. *See* Joshua S. Levy, *Towards a Brighter Fourth Amendment: Privacy and Technological Change*, 16 VA. J.L. & TECH. 502, 517 (2011) (cataloguing the pitfalls of bright line rules for the Fourth Amendment).

135. *See, e.g.*, Laurie Thomas Lee, *Can Police Track Your Wireless Calls?: Call Location Information and Privacy Law*, 21 CARDOZO ARTS & ENT. L.J. 381, 381–82 (2003) (describing how cell phone data—shared with cellular providers—is rapidly expanding and easily accessed).

136. *See* Levy, *supra* note 134 ("[C]ourts should only adopt bright-line rules for activities that are recurring in nature, clearly understandable, and affected by rapid technological changes.").

137. *Id.* ("Incorrect or unjust results risk severely damaging the institutional credibility of the judiciary.").

138. *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 761 (1994) ("The words of the Fourth Amendment really do mean what they say. They do not require warrants, even presumptively, for searches and seizures. They do not require probable cause for all searches and seizures without warrants."). Amar relies on colonial-era cases to argue that the Warrant Clause, along with the probable cause requirement, was merely intended to address the founders' fears of general warrants. *Id.* at 772 (citing Wilkes v. Wood (1763) 98 Eng. Rep. 489; 19 Howell's State Trials 1153).

139. *See id.* at 801 ("The core of the Fourth Amendment, as we have seen, is neither a warrant nor probable cause, but reasonableness.").

140. *Id.* Amar goes on to note how law enforcement tactics' reasonableness can be greatly affected by implication of some other protected constitutional

ancing all interests—from the perspective of the community—to determine a search's reasonability.[141]

While Amar is right that the Supreme Court long ago rejected such a freewheeling inquiry for all Fourth Amendment questions,[142] at times the Court has looked to reasonableness to guide its jurisprudence. A prime example is the "special needs doctrine,"[143] applicable in "exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable."[144] In such a situation, courts use a balancing test[145] to evaluate the reasonableness of the proposed activity.[146] This balancing measures the government's intrusion on Fourth Amendment interests against the promotion of legitimate governmental interests.[147] The Supreme Court identified three factors for evaluation: "(1) 'the nature of the privacy interest allegedly compromised by the [challenged governmental conduct],' (2) 'the character of the intrusion imposed by the [challenged conduct],' and (3) 'the nature and immediacy of the [state's] concerns and the efficacy of the [governmental conduct] in meeting them.'"[148]

Close examination of the special needs doctrine reveals the difficulties with applying Amar's uniform reasonability test to third party material. Beyond the typical criticisms of balancing tests such as their susceptibility to judicial policymaking,[149]

---

right. *Id.* at 804–11. He terms this modification of the inquiry "constitutional reasonableness." *Id.* at 804.

141. *See id.* at 780–82 (explaining that juries, whose opinions reflect the community, are the proper vehicle for the weighing of interests).

142. *Id.* at 757, 761 (referring to Fourth Amendment doctrine as an "embarrassment" and a "mess" for its failure to seize on a simpler framework).

143. *See generally* WAYNE R. LAFAVE, 5 SEARCH & SEIZURE § 10 (5th ed. 2012) (describing inspections and administrative searches); Antoine McNamara, *The "Special Needs" of Prison, Probation, and Parole*, 82 N.Y.U. L. REV. 209, 212–21 (2007) (offering an overview of special needs jurisprudence).

144. New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring).

145. *See, e.g.*, Bd. of Educ. v. Earls, 536 U.S. 822, 828 (2002) (approving suspicionless drug testing for high school students who participate in extracurricular activities).

146. *T.L.O.*, 469 U.S. at 337 ("The determination of the standard of reasonableness governing any specific class of searches requires 'balancing the need to search against the invasion which the search entails.'" (quoting Camara v. Mun. Court of S.F., 387 U.S. 523, 536–37 (1967)).

147. *See* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652–53 (1995) (quoting Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 619 (1989)).

148. Palmieri v. Lynch, 392 F.3d 73, 81 (2d Cir. 2004) (alterations in original) (citations omitted) (quoting *Earls*, 536 U.S. at 830, 832, 834).

149. *See* Carol S. Steiker, *Second Thoughts About First Principles*, 107

pure reasonability is impractical outside special needs cases. The difficulty once again is in crafting a doctrine that can guide *ex ante* behavior by law enforcement. When addressing constitutional challenges to specific governmental initiatives in the special needs context—whether searches of school lockers for drugs[150] or roadblocks of motorists for driving under the influence[151]—the Court can step back to examine a government program in its entirety before identifying and weighing interests. Asking law enforcement officers to make the same judgments before seeking each phone record defies reality.[152] These concerns led to the Court's recognition that "a responsible Fourth Amendment balance is not well served by standards requiring sensitive, case-by-case determinations of government need, lest every discretionary judgment in the field be converted into an occasion for constitutional review."[153] As Professor Anthony Amsterdam recognized, relying on reasonableness alone "converts the fourth amendment into one immense Rorschach blot."[154]

The problem with Amar's framework, however, is not the recourse to the Reasonableness Clause, but the particular application of the clause. In the next Part we argue that, even within the Fourth Amendment's current framework (which by default conflates reasonableness with a warrant), third party searches fit comfortably within the category of searches analyzed under the Reasonableness Clause. And in Part IV, we go on to demonstrate a workable model for applying this clause to third party searches.

III. THIRD PARTY SEARCHES AND THE FOURTH AMENDMENT'S TWO CLAUSES

As noted in Part I, five justices of the Supreme Court appear to have recognized that third party searches cannot be categorically excluded from the ambit of the Fourth Amend-

---

HARV. L. REV. 820, 855 (1994) (criticizing Amar's "reasonableness" approach because it is similar to "rational basis" review, which has proven to be no scrutiny at all).

150. *See T.L.O.*, 469 U.S. at 328–29.

151. *See* Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 447–48 (1990).

152. *See* Wayne B. LaFave, *"Case-By-Case Adjudication" Versus "Standardized Procedures": The* Robinson *Dilemma*, 1974 SUP. CT. REV. 127, 141 (describing the need for Fourth Amendment law to be "readily applicable by the police").

153. Atwater v. City of Lago Vista, 532 U.S. 318, 347 (2001).

154. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 393 (1974).

ment. At the same time, there is widespread (though hardly unanimous) scholarly agreement that the third party doctrine can neither be maintained in its current absolute form nor scrapped entirely.[155] But even those courts willing to rethink the third party doctrine have fallen into the pattern of treating the question as one of an on/off switch. These courts focus almost entirely on whether the Fourth Amendment should come into play at all—i.e., whether an investigatory technique is a search or not—rather than the *extent* to which the Fourth Amendment should come into play.[156] The operational assumption is that if the Fourth Amendment applies, the challenged practice must adhere to the probable cause and warrant requirements—a Fourth Amendment variant of the "'strict' in theory and fatal in fact" standard of review under the Equal Protection Clause.[157] But the Fourth Amendment, after all, contains not one but two clauses: the Warrant Clause and the Reasonableness Clause.[158] Instead of continuing to chafe against the ill-fitting mantle of the search/nonsearch distinction, courts should recognize third party searches as another of the exceptions to the warrant requirement, and accordingly craft a reasonableness test to gauge when third party searches are constitutionally appropriate.[159]

In this Part, we first provide an overview of the Warrant Clause exceptions that have been recognized by the Court, drawing out their key features. We then examine the third party doctrine, demonstrating its doctrinal fit among these exceptions. Finally, we argue that the probable cause requirement of the Warrant Clause should not attach by default to third party searches, which should instead be governed by the Reasonableness Clause.

A. THE WARRANT EXCEPTIONS

The Supreme Court has recognized a number of exceptions to the warrant requirement. These exceptions carry a variety of different rationales—some, such the arrest exceptions, stem

155. *See supra* note 83 and accompanying text.

156. *See supra* Part II.A.

157. *See* Gerald Gunther, Foreword, *In Search of Evolving Doctrine on a Changing Court: A Model for a Newer Equal Protection*, 86 HARV. L. REV. 1, 8 (1972) ("Some situations evoked the aggressive 'new' equal protection, with scrutiny that was 'strict' in theory and fatal in fact; in other contexts, the deferential 'old' equal protection reigned, with minimal scrutiny in theory and virtually none in fact.").

158. *See* U.S. CONST. amend. IV.

159. *See infra* Part IV.C.

from the impracticability of obtaining a warrant,[160] while others, such as the vehicular search exceptions, involve diminished expectation of privacy or limited scope of intrusion.[161] Generally speaking, however, the exceptions can be grouped into three categories.[162] First, there are a handful of exceptions that dispense with the warrant requirement for reasons of necessity or historical practice but maintain the probable cause standard unaltered. Second, there are certain narrowly drawn contexts in which the Court will dispense with individualized suspicion altogether, generally in the context of border searches or programmatic searches. And third, the Court has carved out and slowly expanded an intermediate category where officers may conduct a search or seizure based upon reasonable suspicion rather than probable cause.

1. Probable Cause Without Warrants

The Supreme Court has held that in limited circumstances, officers may take action implicating the Fourth Amendment without a warrant, subject to the action satisfying a probable

160. *See, e.g.*, Gerstein v. Pugh, 420 U.S. 103, 113 (1975) (stating that requiring a warrant prior to arrest is an "intolerable handicap for legitimate law enforcement").

161. *See, e.g.*, California v. Carney, 471 U.S. 386, 392 (1985) ("The public is fully aware that it is accorded less privacy in its automobiles because of this compelling governmental need for regulation."); South Dakota v. Opperman, 428 U.S. 364, 367 (1976) ("[L]ess rigorous warrant requirements govern because the expectation of privacy with respect to one's automobile is significantly less than that relating to one's home or office.").

162. Some sources identify three additional types of warrantless searches and seizures: plain view seizures, consent searches, and searches and seizures of abandoned property. *See, e.g.*, *Warrantless Searches and Seizures*, 42 GEO. L.J. ANN. REV. CRIM. PROC. 46, 80–84, 96–112, 150–51 (2013). Plain view seizures rest upon the principle that an incriminating item discovered during the course of legitimate police activity—whether a search or not a search—may be seized without a warrant. *E.g.*, *id.* at 80–82. As the Court noted in *Texas v. Brown*, 460 U.S. 730, 738–39 (1983), "'[p]lain view' is perhaps better understood, therefore, not as an independent 'exception' to the Warrant Clause, but simply as an extension of whatever the prior justification for an officer's 'access to an object' may be." Consent searches, meanwhile, constitute a waiver of the Fourth Amendment's applicability entirely, *see* Zap v. United States, 328 U.S. 624, 628 (1946), *vacated*, 330 U.S. 800 (1947), albeit a waiver confined to a reasonable understanding of the waiver's scope, *see* Florida v. Jimeno, 500 U.S. 248, 250–51 (1991). Similarly, one who has abandoned property has relinquished a Fourth Amendment interest in it. *See* Abel v. United States, 362 U.S. 217, 241 (1960) (Douglas, J., dissenting) ("There can be nothing unlawful in the Government's appropriation of . . . abandoned property." (citation omitted)). As such, we do not consider these types of searches and seizures as separate exceptions to the warrant requirement here.

cause standard.[163] First, the Court has stated that a warrantless arrest can occur where "officers have probable cause to believe that a person has committed a crime in their presence."[164] The Court has not spent a great deal of time justifying this exception, but has noted at various points that warrantless arrests were "'taken for granted' at the founding,"[165] and that a warrant requirement for arrests for crimes committed in front of officers would constitute an "intolerable handicap for legitimate law enforcement."[166]

Second, it is a "settled rule that warrantless arrests in public places are valid" where supported by probable cause,[167] though there has been even less effort put into justifying this result (a point Amar has seized upon to cast doubt upon the general applicability of the warrant requirement[168]). Most cases trace the rule back to *Carroll v. United States*,[169] which offered merely that "the reason for arrest without warrant on a reliable report of a felony was because the public safety and the due apprehension of criminals charged with heinous offenses required that such arrests should be made at once without warrant."[170] The Court appears to balance this public safety need against the interest in the sanctity of the home protected by the Fourth Amendment, thus finding that arrests upon probable cause require a warrant within the home but do not require a warrant in public.[171]

Third, the Court has sanctioned dispensing with the warrant requirement for searches and seizures in exigent circumstances.[172] For exigent circumstances to excuse the need for a warrant, the Court has made clear that "police officers need . . .

163. *See Pugh*, 420 U.S. at 120 ("The standard is the same as that for arrest.").

164. Virginia v. Moore, 553 U.S. 164, 178 (2008) (Ginsburg, J., concurring).

165. *Id.* at 170 (majority opinion) (citing TELFORD TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 45 (1969)).

166. *Pugh*, 420 U.S. at 113.

167. Payton v. New York, 445 U.S. 573, 587 (1980).

168. Amar, *supra* note 138, at 764.

169. 267 U.S. 132 (1925).

170. *Id.* at 157.

171. *Payton*, 445 U.S. at 586–87 ("[S]earches and seizures inside a home without a warrant are presumptively unreasonable . . . [but] objects such as weapons or contraband found in a public place may be seized by the police without a warrant.").

172. *See, e.g.*, Mincey v. Arizona, 437 U.S. 385, 393–94 (1978) (stating that officers usually require warrants unless exigent circumstances override Fourth Amendment concerns).

probable cause plus exigent circumstances."[173] The Court has identified a variety of "exigencies of the situation [that] make the needs of law enforcement so compelling that the warrantless search is objectively reasonable under the Fourth Amendment,"[174] including the need to render emergency aid, hot pursuit of a fleeing suspect, and the danger of destruction of evidence.[175]

The final context in which the Court has allowed warrantless action while maintaining the probable cause requirement is for searches of vehicles.[176] The Court initially rested this waiver of the warrant requirement upon the portable nature of automobiles and the risk that evidence would move beyond the officer's control or jurisdiction before a warrant could be obtained.[177] However, the Court has made clear that "[b]esides the element of mobility, less rigorous warrant requirements govern because the expectation of privacy with respect to one's automobile is significantly less than that relating to one's home or office."[178] And in fact, the Court has "upheld warrantless searches where no immediate danger was presented that the car would be removed from the jurisdiction,"[179] including after the vehicle has already been impounded.[180] In these cases, it would appear that the lesser expectation of privacy provides an independently sufficient justification to dispense with the warrant requirement.

2. Searches Without Individualized Suspicion

Several warrant exceptions dealing with searches in "exceptional"[181] circumstances dispense with the individualized

173. Kirk v. Louisiana, 536 U.S. 635, 638 (2002) (allowing officers to enter a home under exigent circumstances).

174. *Mincey*, 437 U.S. at 394.

175. Kentucky v. King, 563 U.S. 452, 459–60 (2011). One wrinkle, orthogonal to this discussion, is that the officers need only "an objectively reasonable basis for believing" that the exigent circumstance at issue exists. Brigham City v. Stuart, 547 U.S. 398, 406 (2006).

176. *See* California v. Carney, 471 U.S. 386, 394–95 (1985) (holding that a warrantless vehicular search was not unreasonable because the officers had probable cause).

177. *See id.* at 390–91.

178. South Dakota v. Opperman, 428 U.S. 364, 367 (1976).

179. *Id.*

180. Chambers v. Maroney, 399 U.S. 42, 52 & n.10 (1970) (finding no difference under the Fourth Amendment between searching a vehicle immediately and searching it after impoundment).

181. New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring) (noting that the Court has recognized certain exceptional circumstances

suspicion requirement altogether. First, the border has long been held to a different standard, operating on a sliding scale of suspicion needed to justify increasingly obtrusive searches. For example, routine stops at fixed border points may be conducted without any individualized suspicion,[182] while detention beyond the scope of routine inspection requires reasonable suspicion.[183] The Court justified these practices by noting that "not only is the expectation of privacy less at the border than in the interior, [but] the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is also struck much more favorably to the Government at the border."[184]

Another well-established exception to the Warrant Clause is searches incident to arrest. "The exception derives from interests in officer safety and evidence preservation that are typically implicated in arrest situations."[185] Where the police make a valid arrest, they are permitted to search "the person of the arrestee . . . [and] the area within the control of the arrestee."[186] Both types of searches must be reasonable in scope (and have been the subject of considerable contestation over scope),[187] but individualized suspicion is not required.[188] Similarly, upon taking property into custody, the police may inventory it according to standardized procedures without any individualized suspicion.[189] As discussed above, the scope of the search-incident-to-arrest exception has recently been constricted by *Riley v. Cali-*

---

under which warrant and probable-cause requirements are impracticable).

182. United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985).

183. *Id.* at 541.

184. *Id.* at 539–40 (citations omitted). A similar scheme prevails with regard to Coast Guard inspections at sea. *See* United States v. Villamonte-Marquez, 462 U.S. 579, 591 (1983) (observing that the government's interests in regulating sea traffic are more substantial at checkpoints where vessels depart to foreign ports).

185. Arizona v. Gant, 556 U.S. 332, 338 (2009).

186. United States v. Robinson, 414 U.S. 218, 224 (1973) (emphasis omitted).

187. *See, e.g.*, *Gant*, 556 U.S. at 339 (surveying the turbulent legal history of searches of vehicles pursuant to arrest of an occupant); Winston v. Lee, 470 U.S. 753, 766 (1985) (holding it unreasonable to surgically extract a bullet). To many observers, *Gant* further threw into confusion the permissible scope of a search incident to arrest as it pertains to vehicle occupants. *See, e.g.*, George M. Dery III, *A Case of Doubtful Certainty: The Court Relapses into Search Incident to Arrest Confusion in* Arizona v. Gant, 44 IND. L. REV. 395, 396 (2011) ("*Gant* . . . may lead to further confusion in this troubled area of Fourth Amendment litigation.").

188. *Robinson*, 414 U.S. at 234–35.

189. *See* Colorado v. Bertine, 479 U.S. 367, 371–72 (1987).

fornia,[190] but outside of cellphones and perhaps other electronic devices the core features of the exception remain intact.[191]

A final category falls under the catch-all of "special needs," also examined in Part II. The Court has held that "[i]n limited circumstances, where the privacy interests implicated by the search are minimal, and where an important governmental interest furthered by the intrusion would be placed in jeopardy by a requirement of individualized suspicion, a search may be reasonable despite the absence of such suspicion."[192] The governmental interest must go "beyond the normal need for law enforcement . . . ."[193] Accordingly, the Court has upheld mandatory drug tests in some contexts, such as for high school athletes,[194] but not in others, such as for pregnant mothers.[195] One variant of such special needs searches are administrative searches of "pervasively regulated industries."[196] In such cases, where "the privacy interests of the owner are weakened and the government interests in regulating particular businesses are concomitantly heightened," the government can craft a regulatory scheme that dispenses with warrants and with individualized suspicion.[197]

3. Searches and Seizures upon Reasonable Suspicion

The final category of exceptions to the Warrant Clause involves a pure application of the Fourth Amendment's second clause: that searches and seizures must be reasonable. In *Terry v. Ohio*,[198] to be explored in more depth in Part IV, the Court permitted officers to make investigatory stops of persons on the basis of reasonable suspicion without a warrant. Writing for the majority, Chief Justice Warren focused on three primary rationales for allowing the police to proceed without a warrant. First, it is simply impracticable (if not impossible) for the police to obtain a warrant at every investigatory encounter on the street. The Court found that such "police conduct—necessarily

190. 134 S. Ct. 2473, 2485 (2014) (declining to extend *Robinson* to an arrestee's cellphone).

191. *Id.* at 2493–94 (stating that the Court's exception for cellphones did not otherwise disturb the doctrine).

192. Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 624 (1989).

193. Griffin v. Wisconsin, 483 U.S. 868, 873 (1987) (quoting New Jersey v. T.L.O., 469 U.S. 325, 351 (1985)).

194. *See* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 654–66 (1995).

195. *See* Ferguson v. City of Charleston, 532 U.S. 67, 76–86 (2001).

196. New York v. Burger, 482 U.S. 691, 693 (1987).

197. *Id.* at 702.

198. 392 U.S. 1 (1968).

swift action predicated upon the on-the-spot observations of the officer on the beat—. . . historically has not been, and as a practical matter could not be, subjected to the warrant procedure."[199] Second, there is an important "need for law enforcement officers to protect themselves and other prospective vicvictims of violence in situations where they may lack probable cause for an arrest."[200] And third, "[a]n arrest is a wholly different kind of intrusion upon individual freedom from a limited search for weapons . . . ."[201] Whereas an arrest involves significant infringement upon personal liberty, a *Terry* stop "constitutes a brief, though far from inconsiderable, intrusion upon the sanctity of the person."[202] Weighing these three factors, the Court's "evaluation of the proper balance that has to be struck in this type of case" led it to conclude that police should possess a narrowly drawn stop-and-frisk authority without a warrant requirement and upon reasonable suspicion.[203]

Two rationales that the Court declined to pursue in *Terry* are worth noting. First was the Ohio Court of Appeals' suggestion that a "stop and frisk" should be excluded from the definition of search or seizure entirely, and thus moved outside the purview of the Fourth Amendment.[204] Second, the majority did not adopt Justice Douglas's exhortation in dissent that the Court retain the probable cause standard despite discarding the warrant requirement.[205] The majority's "evaluation of the proper balance that has to be struck in this type of case" led it, instead, to the reasonable suspicion standard.[206]

In *United States v. Place*,[207] the Court considered whether to extend the reasoning of *Terry* to the detention of luggage at airports. The Court held that "seizures on the basis of reasonable, articulable suspicion, premised on objective facts, that the luggage contains contraband or evidence of a crime" were valid under the Fourth Amendment.[208] Following the formula laid down by *Terry*, the Court "balance[d] the nature and quality of the intrusion on the individual's Fourth Amendment interests

199. *Id.* at 20.
200. *Id.* at 24.
201. *Id.* at 26.
202. *Id*.
203. *Id.* at 27.
204. *See id.* at 16–20, 16 n.12 (citing State v. Terry, 214 N.E.2d 114, 120 (Ohio 1966)).
205. *See id.* at 35–39 (Douglas, J., dissenting).
206. *Id.* at 27 (majority opinion).
207. 462 U.S. 696 (1983).
208. *Id.* at 702.

against the importance of the governmental interests alleged to justify the intrusion."[209] As in *Terry*, the Court pointed to the government's interest in detecting and preventing crime; in *Place*, however, the Court lacked (and found unnecessary) the officer safety rationale upon which *Terry* had, in part, rested.[210] The Court also noted "the inherently transient nature of drug courier activity at airports," and rejected the respondents' argument that "a generalized interest in law enforcement" could not "justify an intrusion on an individual's Fourth Amendment interests in the absence of probable cause."[211] Set against these governmental interests, the Court found that "[t]he intrusion on possessory interests occasioned by a seizure of one's personal effects can vary both in its nature and extent."[212] Where the detention was only temporary and the examination of the property did not independently violate the Fourth Amendment, detention on reasonable suspicion would be valid.[213]

4. Common Themes

A handful of common themes emerge from these scattered warrant exceptions: the practicality of obtaining a warrant, whether there is a diminished expectation of privacy, and the significance of the law enforcement interest. The first, distinctly not applicable to run-of-the-mill third party searches, is that of the practical impossibility of the interposition of a magistrate between officer and search. There is little risk that data or documents held by third parties will drive off into the sunset before the officer can secure a warrant, as with vehicles, or that a suspect will destroy them or use them for violence against officers, as with searches incident to arrest.

But practical impossibility is not a necessary condition for warrantless searches; significant as well is the privacy interest at stake. As noted above, the Court has found a diminished expectation of privacy in vehicles sufficient to justify dispensing with the warrant requirement even where mobility concerns

209. *Id.* at 703.

210. *Id.* at 703–04.

211. *Id.*

212. *Id.* at 705. Interestingly, the Court offered an example of a situation in which expectations of privacy could be diminished: "[t]he seizure may be made after the owner has *relinquished control of the property to a third party* or, as here, from the immediate custody and control of the owner." *Id.* (emphasis added).

213. The Court held in *Place* that the ninety-minute detention exceeded the permissible scope of a *Terry* stop. *Id.* at 709–10.

are obviated.[214] The exception for administrative searches of closely regulated industries does not depend upon the impossibility of obtaining prior approval, but rather upon the owner's diminished expectation of privacy.[215] And in other contexts where practicality *is* at play, such as *Terry* stops and border searches, the Court has been careful to note as well a diminished expectation of privacy where it has abandoned the warrant requirement (and particularly where it has lowered the probable cause threshold).[216]

In addition to the degree of expectation of privacy, the Court has often looked to the countervailing government interest. In the context of special needs, the Court has stated that the government interest must be distinct from (though not necessarily to the exclusion of) ordinary law enforcement.[217] But this is not a general rule: in extending *Terry* stops to luggage, the Court in *Place* rejected the proposition that, "absent some special law enforcement interest such as officer safety, a generalized interest in law enforcement cannot justify an intrusion on an individual's Fourth Amendment interests in the absence of probable cause."[218]

B. SHOULD THIRD PARTY SEARCHES REQUIRE A WARRANT?

Looking to the factors the Court has highlighted as favoring an exception from the warrant requirement, the most salient for third party searches are law enforcement needs and a reduced expectation of privacy. As noted above, third party searches *could*, in circumstances not covered independently by the exigent circumstances exception, be preapproved by a neutral magistrate. But as the Court said in *United States v.*

214. *See* South Dakota v. Opperman, 428 U.S. 364, 367 (1976) (discussing the traditional distinction between automobiles and homes or offices in the context of the Fourth Amendment).

215. *See* New York v. Burger, 482 U.S. 691, 702 (1987) (recognizing the lessened application of warrant and probable cause requirements in the context of a closely regulated industry).

216. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 539 (1985) (identifying the lessened expectation of privacy at the border compared to the interior); Terry v. Ohio, 392 U.S. 1, 26 (1968) (rejecting the argument that an officer is unjustified in making an intrusion short of an arrest absent evidence sufficient to warrant a belief that the person has committed or is committing a crime).

217. *See* New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring) (arguing that the Court uses a balancing test only in the context of "a special law enforcement need for greater flexibility").

218. United States v. Place, 462 U.S. 696, 703–04 (1983).

Rabinowitz,[219] "[a] rule of thumb requiring that a search warrant always be procured whenever practicable may be appealing from the vantage point of easy administration. But we cannot agree that this requirement should be crystallized into a *sine qua non* to the reasonableness of a search."[220] The constitutional imposition of a warrant requirement would both overprotect information in which individuals have a diminished expectation of privacy and unduly hamper law enforcement interests.

1. Diminished Expectation of Privacy

In addition to the significant government interest in access to third party records, the Court has repeatedly recognized a diminished expectation of privacy in such records.[221] Of course, the Court's declaration, that "a person has *no* legitimate expectation of privacy in information he voluntarily turns over to third parties,"[222] has been roundly condemned. But even if a person does not *entirely* lack a legitimate expectation in privacy, it does not necessarily follow that her expectation of privacy is not at all diminished. Accepting that there are diminished—but not nonexistent—expectations of privacy in third party records would, unlike the approach of *Miller* and *Smith*, render the Fourth Amendment applicable to such searches. As the Court noted in *Riley*, "[t]he fact that an arrestee has diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely."[223]

It is widely recognized that individuals cannot, or should not, actually expect all of the information disclosed to third parties to remain private. Justice Alito, concurring in *Jones*, acknowledged that "even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable."[224] But what are we to make of this inevitability? The *Miller* Court implicitly analogized this potential exposure to the common law doctrine of assumption of risk: a "depositor takes

219. 339 U.S. 56 (1950), *overruled in part by* Chimel v. California, 395 U.S. 752 (1969).

220. *Id.* at 65.

221. *Cf. Place*, 462 U.S. at 705 ("The intrusion on possessory interests occasioned by a seizure of one's personal effects can vary both in its nature and extent. The seizure may be made after the owner has relinquished control of the property to a third party . . . .").

222. Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (emphasis added).

223. Riley v. California, 134 S. Ct. 2473, 2488 (2014).

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

the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[225] Kerr has picked up on this notion of assumption of risk to argue that the depositor (or other person engaging in transactions with third parties) has voluntarily consented to the disclosure.[226]

Epstein has powerfully critiqued the idea that *knowledge* of risk is analytically equivalent to *assumption* of risk in this context because individuals cannot contract out of it: "The supposed assumption of the risk is forced on individuals by positive law. It is not consensually assumed."[227] Such an approach finds some support in *Georgia v. Randolph*,[228] in which the Court refused to recognize a co-occupant's consent to search an apartment where the physically present defendant refused entry.[229] The *Randolph* majority critiqued "the dissent's easy assumption that privacy shared with another individual is privacy waived for all purposes including warrantless searches by the police."[230] Defenders of the traditional third party doctrine might respond that an individual could simply decline to contract with third parties whenever they seek to keep given information private, but such an option may never have been practical,[231] and certainly is even less so in the modern world.[232] And indeed, the *Katz* majority would likely find quite alien the notion that pervasive electronic surveillance, if carried out through third parties, could be justified under the rubric of consent.[233]

So where does this leave us? According to Kerr and the *Miller* and *Smith* Courts, one's knowledge that she is turning

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

226. Kerr, *supra* note 2, at 588–90.

227. Epstein, *supra* note 64, at 1206.

228. 547 U.S. 103 (2006).

229. *Id*. at 122–23.

230. *Id.* at 115 n.4.

231. *See* Smith v. Maryland, 442 U.S. 735, 749–50 (1979) (Marshall, J., dissenting) ("It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative.").

232. *Cf.* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("[T]he premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties . . . is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.").

233. *See* Katz v. United States, 389 U.S. 347, 358 n.22 (1967) ("A search to which an individual consents meets Fourth Amendment requirements, but of course 'the usefulness of electronic surveillance depends on lack of notice to the suspect.'" (quoting Lopez v. United States, 373 U.S. 427, 463 (1963) (Brennan, J., dissenting)) (citing Zap v. United States, 328 U.S. 624 (1946))).

over her information to third parties—and potentially to the government—would defeat her reasonable expectation of privacy under the *Katz* test. Yet according to Epstein,[234] the *Randolph* majority, and the *Jones* concurrences, such knowledge should not constitute waiver. Faced with these conflicting supportable positions, it seems clear that people retain a diminished, though not nonexistent, expectation of privacy in information they disclose to third parties.

2. Law Enforcement Needs

The government has a substantial interest in access to information held in the hands of third parties. Of course, the government *always* has a law enforcement interest in escaping the strictures of the Warrant Clause. But "[a] generalized interest in expedient law enforcement cannot, without more, justify a warrantless search."[235] What the Court asks, in weighing an exception to the warrant requirement, is whether warrants would pose a particular burden in a given situation.[236] In the case of third party searches, there are good reasons to find that this heightened law enforcement interest is present.

As Epstein and Slobogin have pointed out, the Fourth Amendment (and in fact, the entirety of criminal procedure) operates on a graduated scale: ordinary police work operates outside the parameters of the Fourth Amendment, minimally intrusive searches are subject to reasonableness, more invasive searches and arrest require warrants and probable cause, and conviction requires proof beyond reasonable doubt.[237] This pro-

234. *See supra* note 64 and accompanying text.

235. *Randolph*, 547 U.S. at 115 n.5. These *dicta* in *Randolph* would appear to coexist uneasily with the Court's rejection in *Place* of the "suggest[ion] that, absent some special law enforcement interest such as officer safety, a generalized interest in law enforcement cannot justify an intrusion on an individual's Fourth Amendment interests in the absence of probable cause." *Place*, 462 U.S. at 703–04 (1983). In context, however, it is clear that the *Place* Court intended to place the inquiry on the substantiality, rather than the type, of the law enforcement interest. *See id.* at 704 ("The test is whether those interests are sufficiently 'substantial,' not whether they are independent of the interest in investigating crimes effectively and apprehending suspects." (quoting Michigan v. Summers, 452 U.S. 692, 699 (1981))).

236. *See* Terry v. Ohio, 392 U.S. 1, 20 (1968) ("But we deal here with an entire rubric of police conduct—necessarily swift action predicated upon the on-the-spot observations of the officer on the beat—which historically has not been, and as a practical matter could not be, subjected to the warrant procedure.").

237. Epstein, *supra* note 64, at 1211 ("The basic pattern is that in principle, it should take more to convict than it does to arrest, and more to arrest than it does to search, and more to search than it does to investigate.");

gression was similarly noted by the *Terry* Court: "[I]n dealing with the rapidly unfolding and often dangerous situations on city streets the police are in need of an escalating set of flexible responses, graduated in relation to the amount of information they possess."[238]

As argued in Part II, there is increasing recognition that third party searches—or at least some third party searches—cannot be located on the lowest rung of that ladder. But it is equally unrealistic to think that the entire panoply of third party searches can be subject to the requirements necessary to effectuate a forcible entry into the home. As Kerr notes, "[t]he repeated use of nonsearch techniques has been considered an essential way to create probable cause that justifies searches rather than an unlawful search itself."[239] To prohibit any access to third party information would be "devastating to the legitimate needs of law enforcement."[240] Although law enforcement's use of third party information is difficult to quantify, the practice is widespread[241] and by all accounts extraordinarily effective. As Slobogin points out, the warrant and probable cause requirements could pose an insurmountable barrier to standard police investigations.[242] He explains:

> [I]magine that police want to find out from the phone company who called a murder victim in the two weeks prior to the murder (a scenario often depicted on TV shows like Law & Order). While they would certainly be able to demonstrate the relevance of this . . . data, they would not have probable cause with respect to any of the callers, and thus would not be able to obtain the regulated subpoena for the phone company's records . . . .[243]

Lacking the ability to access third party information without a warrant supported by probable cause, police tactics would revert to the pre-modern era, where officers must resort to prohibitively expensive low-tech surveillance such as knocking on doors or staking out suspected criminals.[244]

Slobogin, *supra* note 119, at 164–67.

238. *Terry*, 392 U.S. at 10.

239. Kerr, *supra* note 101, at 328.

240. Henderson, *supra* note 115, at 44.

241. *See* Dennis, *supra* note 102, at 757 ("[I]n 2004, federal law enforcement utilized 10,874 pen register and trap and trace orders; by 2008, that number had almost doubled, to 20,889 orders.").

242. *See* Slobogin, *supra* note 119, at 185.

243. *Id.*

244. *See* Blake Ellis Reid, Note, *Substitution Effects: A Problematic Justification for the Third-Party Doctrine of the Fourth Amendment*, 8 J. ON TELECOMM. & HIGH TECH. L. 613, 620 (2010) ("Low-tech surveillance, such as committing officers to stakeouts and tracking work, is expensive—and funding of boots-on-the-ground police presence seems to be on a problematic decline in

Furthermore, requiring warrants for third party searches is even less feasible today than it would have been in the late 1970s, when *Smith* and *Miller* were decided. The Court has signaled its awareness of "[r]apid changes in the dynamics of communication and information transmission,"[245] and Kerr has noted that such changes "place[] more and more communications in the hands of third parties."[246] This change is, of course, a double-edged sword: the migration of personal transactions from the analog to the digital sphere heightens both the government interest in access and the individual's interest in protection. But the government interest is particularly significant because of the growing threat of cybercrime, which takes place entirely across platforms controlled by third parties.[247] For example, "tracing an IP address is a common and effective way for authorities to identify perpetrators of cyberharassment crimes."[248] If drug courier activity at airports is sufficient to deprive luggage of the full protection of the Warrant Clause,[249] the shift of criminal activity to the Internet should similarly push in favor of a warrant exception for third party searches.

3. Applying the Rationales

If an activity is to be deemed a search but excused from the warrant requirement, a specific exception must be made.[250] Such a burden is not easily overcome, but the third party doctrine shares two important features with other exceptions to the warrant requirement. Like the heightened law enforcement concerns over the border (as in *United States v. Montoya de Hernandez*[251]) or drug courier activity at airports (as in *United*

---

the United States.").

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

246. Kerr, *supra* note 2, at 566.

247. *Cf.* David Gray et al., *Fighting Cybercrime After* United States v. Jones, 103 J. CRIM. L. & CRIMINOLOGY 745, 759 (2013) ("[T]he third-party doctrine[] play[s] a critical role in law enforcement's efforts to detect and prosecute many crimes, particularly cybercrimes.").

248. *Id.* at 797.

249. *See* United States v. Place, 462 U.S. 696, 704 (1983) ("Because of the inherently transient nature of drug courier activity at airports, allowing police to make brief investigative stops of persons at airports on reasonable suspicion of drug-trafficking substantially enhances the likelihood that police will be able to prevent the flow of narcotics into distribution channels.").

250. *See* Riley v. California, 134 S. Ct. 2473, 2482 (2014) ("In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement.").

251. 473 U.S. 531, 538 (1985).

States v. Place[252]), third party searches implicate a zone of special law enforcement concern. And as with vehicles (as in *Arizona v. Gant*[253]) and closely regulated industries (as in *New York v. Burger*[254]), the intrusion on personal privacy is limited by the diminished expectation of privacy. Given the current status of third party searches as wholly outside the Fourth Amendment, defining third party searches as an exception to the warrant requirement offers a sensible avenue to bring them within the ambit of the Fourth Amendment without dramatically upending law enforcement practice.

C. WARRANTLESS THIRD PARTY SEARCHES: PROBABLE CAUSE OR REASONABLENESS?

Having determined that the warrant requirement should not apply to third party searches, the next question is whether the Warrant Clause's probable cause standard should apply. The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[255]

As Professor Amsterdam famously observed, the problem with interpretation of the Fourth Amendment is that "[i]ts language is no help and neither is its history."[256] The unclear relationship between the two clauses raises the question of whether, if courts are to bring third party searches under the Fourth Amendment without a warrant requirement, they should impose a probable cause requirement. There are two competing views on this question, among both jurists and academics, but the more appropriate path for third party searches is to adopt the reasonableness standard of the Fourth Amendment's first clause, rather than the probable cause standard of its second clause.

One view, espoused prominently by Professor Amar, is that the two clauses are disjunctive: searches are generally to be governed by the Reasonableness Clause, and only those partic-

252. 462 U.S. at 704.

253. 556 U.S. 332, 339 (2009) (describing the Court's precedents allowing vehicle searches in the course of arresting suspects).

254. 482 U.S. 691, 693 (1987) (referring to "the exception to the warrant requirement for administrative inspections of pervasively regulated industries").

255. U.S. CONST. amend. IV.

256. Amsterdam, *supra* note 154, at 395.

ular circumstances in which warrants are required are to be governed by the probable cause and specificity requirements of the Warrant Clause.[257] As Professor Tracey Maclin has noted, this view had early adherents among the Court prior to the Warren Court's procedural revolution.[258] In 1950, the Court stated: "It is unreasonable searches that are prohibited by the Fourth Amendment. It was recognized by the framers of the Constitution that there were reasonable searches for which no warrant was required."[259]

This view appeared to fall out of favor over the following decades in favor of the conjunctive reading of the two clauses: that the Reasonableness Clause, in most cases, incorporates the warrant and probable cause requirements of the second clause.[260] In *Katz*, the Court stated that "searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."[261] According to Maclin, this view continued to prevail through the 1970s, with some dissenting voices urging a return to the disjunctive model.[262]

But by the 1990s, the worm had begun to turn.[263] In 1989, the Court stated a notably watered-down version of the conjunctive view with regard to warrantless searches:

> Our cases indicate that even a search that may be performed without a warrant must be based, as a general matter, on probable cause to believe that the person to be searched has violated the law. When the balance of interests precludes insistence on a showing of probable cause, we have usually required "some quantum of individualized suspicion" before concluding that a search is reasonable.[264]

Over the past few years, the Court has more openly embraced the view that the Warrant Clause's requirements are confined to certain situations, with the Reasonableness Clause

---

257. *See* AKHIL AMAR, THE CONSTITUTION AND CRIMINAL PROCEDURE 3–17 (1997); *see also* TAYLOR, *supra* note 165, at 23–50.

258. *See* Tracey Maclin, *The Central Meaning of the Fourth Amendment*, 35 WM. & MARY L. REV. 197, 202–04 (1993).

259. United States v. Rabinowitz, 339 U.S. 56, 60 (1950) (citation omitted).

260. Amsterdam, among others, has argued that, under the Fourth Amendment, warrants are the touchstone of reasonableness, with only limited exceptions. *See* Amsterdam, *supra* note 154, at 395–99.

261. Katz v. United States, 389 U.S. 347, 357 (1967) (footnote omitted).

262. *See* Maclin, *supra* note 258, at 204–05.

263. *See id.* at 205.

264. Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 624 (1989) (citations omitted) (upholding warrantless, suspicionless drug tests of railway employees).

governing by default. As Professor Erin Murphy describes, "whereas 'reasonableness' cases used to fashion themselves as deviations from the rule, paying homage to warrants and suspicion, such opinions increasingly have moved away from these qualifiers to more expressly embrace pure 'reasonableness.'"[265] In the October 2012 Term the preference for reasonableness over a presumptive warrant requirement gained explicit adherence among a minority of the Court.[266] And in upholding the collection of DNA from certain arrestees in *Maryland v. King*,[267] a majority of the Court signed on to Justice Kennedy's quick dismissal of the Warrant Clause. He explained: "To say that no warrant is required is merely to acknowledge that 'rather than employing a *per se* rule of unreasonableness, we balance the privacy-related and law enforcement-related concerns to determine if the intrusion was reasonable.'"[268]

Viewed in this light, the warrant exceptions that adhere to probable cause look increasingly like isolated exceptions. The arrest exceptions may retain probable cause requirements due to the fact that "[a]n arrest is a wholly different kind of intrusion upon individual freedom from a limited search,"[269] while the vehicle exception's probable cause requirement may stem as much from historical pedigree (having been established in 1925[270]) as from a commitment to a probable cause presumption. More recent exceptions, such as that for *Terry* stops and special needs searches, have looked to reasonableness as the "touchstone of the Fourth Amendment,"[271] whether that reasonableness is through individualized suspicion or programmatic balancing of needs. Accordingly, if the courts are to craft a new exception to the warrant requirement, they should do so

265. Erin Murphy, *License, Registration, Cheek Swab: DNA Testing and the Divided Court*, 127 HARV. L. REV. 161, 184 (2013) (citing, *inter alia*, Kentucky v. King, 563 U.S. 452, 459 (2011)); *see also id.* at 185 ("Although the text of the Fourth Amendment does not specify when a search warrant must be obtained, this Court has inferred that a warrant must generally be secured. . . . But we have also recognized that this presumption may be overcome in some circumstances because the ultimate touchstone of the Fourth Amendment is reasonableness." (citations omitted)).

266. *See id.* at 185–86 (citing Missouri v. McNeely, 133 S. Ct. 1552, 1569 (2013) (Roberts, C.J., concurring in part and dissenting in part)); *see also* Bailey v. United States, 133 S. Ct. 1031, 1048 (2013) (Breyer, J., dissenting).

267. 133 S. Ct. 1958 (2013).

268. *Id.* at 1970 (quoting Illinois v. McArthur, 531 U.S. 326, 331 (2001)).

269. Terry v. Ohio, 392 U.S. 1, 26 (1968).

270. *See* Maryland v. Dyson, 527 U.S. 465, 466 (1999) (tracing the automobile exception back to *Carroll v. United States*, 267 U.S. 132, 153 (1925)).

271. *King*, 133 S. Ct. at 1970.

through the lens of the Reasonableness Clause. The next Part discusses how that application might work.

IV. CRAFTING A REASONABLENESS INQUIRY

The question is whether the reasonableness standard can help courts make headway in the third party context. To our mind, the inherited third party doctrine has two key disabilities. First, it tends to deploy the Fourth Amendment in an on/off manner, yielding a test that has difficulty accepting both that the Fourth Amendment should apply and that the conduct at issue is reasonable in light of the nature of the intrusion and the information sought. Second, courts and commentators contemplating alternatives to the third party doctrine too readily assume that if the Fourth Amendment does apply, it must be through the Warrant Clause and not the Reasonableness Clause. Thus far we have tried to soften each of these assumptions in favor a reasonableness-based inquiry that does not simply toss the Fourth Amendment out the door when information is stored on a cloud server or when an individual transacts with her bank.

We want to establish that third party searches should fall within the ambit of the Fourth Amendment, while at the same time arguing that their legality need not be tethered to the warrant or probable clause requirements. Rather we want to redirect the constitutional inquiry to how courts should evaluate reasonableness. One option would be follow Amar and apply a kitchen-sink reasonableness inquiry in every case.[272] Another would enlist "special needs" cases in requiring a controlled balancing of government and private interests for different types of third party search programs.[273] A third option, meanwhile, would dispose with the weighing of interests in every case, while retaining the flexibility to be applied to individual cases.

We take as our signpost the recognition in *Terry v. Ohio*[274] that there is more than one way of evaluating reasonableness. The famous "*Terry* stop" that grew out of the Court's balancing was not a subjective assessment of the expectation of the detainee and the police officer in any particular case. Rather, it was an objective assessment of the types of circumstances in which persons are likely to have a diminished expectation of privacy and in which the ambit of police conduct is correspond-

272. *See* Amar, *supra* note 138, at 801.

273. *See, e.g.*, New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring).

274. Terry v. Ohio, 392 U.S. 1 (1968).

ingly broader. The *Terry* Court balanced the interests not on the specific facts, but for frisks in general, thereby allowing the Court to distill a single test that law enforcement and lower courts could implement moving forward: reasonable suspicion.

We are not the first to realize *Terry*'s special place amongst Fourth Amendment precedents and its potential for reformation of the third party doctrine. Both Slobogin and Epstein have pointed to *Terry* before. Slobogin sees *Terry* as an invitation to set many standards varied by the level of intrusion.[275] For example, a home search would require "clear and convincing" evidence, which he estimates as having a "quantitatively defined" equivalent of 75% certainty; prolonged stops would require probable cause, or 50% certainty; and short *Terry* stops or roadblocks would require reasonable suspicion, or 20% to 30% certainty.[276] Slobogin uses a survey of federal judges to tie his percentages to jurisprudential reality, but he does not concentrate on the reasoning in *Terry* and its progeny or its slow development in the Supreme Court.[277] These components of the *Terry* opinion deserve analysis and provide further valuable lessons for expanding reasonable suspicion into the third party area.

Epstein, on the other hand, values *Terry*'s reasonable suspicion insofar as it allows him to split the difference between full protection and no protection at all.[278] Epstein has long argued that an examination of privacy, specifically the common-law tort of invasion of privacy, can have a meaningful impact on clarifying longstanding constitutional principles.[279] With respect to the Fourth Amendment, Epstein explains *Katz* and its progeny through the private law privacy torts.[280] He argues that, as a starting point, the police can at least act as any private citizen would act under the private law.[281] Thus, he approves of *Terry v. Ohio* in its permitting police to follow suspects on the street—the right of any private person—and its "operat[ion] as a sensible middle ground between a rule that allowed the police to stop and frisk at will and one that required

275. *See* Slobogin, *supra* note 117, at 1056–57.

276. *Id.* at 1082–83.

277. *Id.*

278. *See* Epstein, *supra* note 64, at 1206.

279. *See, e.g.*, Richard A. Epstein, *Privacy, Publication, and the First Amendment: The Dangers of First Amendment Exceptionalism*, 52 STAN. L. REV. 1003, 1007 (2000) (examining the First Amendment through common law privacy torts).

280. *See* Epstein, *supra* note 64, at 1212–14.

281. *Id.* at 1214.

them to demonstrate probable cause for arrest."[282] We too recognize the doctrinal advantages of *Terry* as enabling a reasonableness inquiry. But we base our doctrinal justification primarily in the constitutional law of the Fourth Amendment—and in particular the specific reasoning of *Terry* itself—rather than the common law of privacy, and attempt to more fully play out the implications of the *Terry* approach.

A. BUILDING BLOCKS: *TERRY V. OHIO*

In *Terry v. Ohio*, the Supreme Court faced a situation in which it could neither deny that a law enforcement tactic constituted a search nor burden officers with the full weight of the Warrant Clause. Prior to *Terry*, brief investigative stops—often accompanied by a limited frisk for weapons—were a standard practice for law enforcement. Yet it was not until the exclusionary rule was imposed upon the states[283] that courts began to confront the informal police procedure.[284] In 1967, a case finally reached the Court.

Detective Martin McFadden of the Cleveland Police Department was on patrol in plainclothes when he saw two men, John Terry and Richard Chilton, standing on a corner.[285] Detective McFadden continued to observe the two as each of them walked down the street, peered into a storefront, and returned to confer with the other.[286] After several repetitions of this pattern, the two men briefly met with a third person, who then walked away.[287] McFadden suspected that the men were casing the storefront for a robbery and "feared they may have [had] a gun."[288] When Terry and Chilton rejoined the third man, McFadden confronted the group, identifying himself as a police officer and asking for their names.[289] Not receiving a response, McFadden "grabbed petitioner Terry, spun him around so that they were facing the other two, with Terry between McFadden

282. *Id.* at 1216.

283. The Court adopted the exclusionary rule as a method of Fourth Amendment enforcement in 1914, *see* Weeks v. United States, 232 U.S. 383, 398–99 (1914), and incorporated the Fourth Amendment against the states in 1949, *see* Wolf v. Colorado, 338 U.S. 25, 27–28 (1949), but did not incorporate the exclusionary rule itself against the states until 1961, *see* Mapp v. Ohio, 367 U.S. 643, 655–60 (1961).

284. WAYNE R. LAFAVE, 4 SEARCH AND SEIZURE § 9.1(a) (5th ed. 2012).

285. Terry v. Ohio, 392 U.S. 1, 5 (1968).

286. *Id.* at 5–6.

287. *Id.*

288. *Id.* at 6 (internal quotation marks omitted).

289. *Id.* at 6–7.

and the others, and patted down the outside of his clothing," finding a revolver in one pocket.[290] At trial, the court denied Terry's motion to suppress the gun and convicted him of carrying a concealed weapon.[291] An appellate court upheld the conviction on the basis that the stop and frisk at issue in *Terry* did not constitute a "full-blown search," and thus fell outside the perimeter of the Fourth Amendment.[292] The Supreme Court of Ohio dismissed the appeal, finding that "no substantial constitutional question was involved."[293]

Considering Terry's motion to suppress the gun, Chief Justice Warren delivered the opinion of the Court. He began by rejecting the logic of the Ohio courts, stating that the Fourth Amendment was surely implicated in the brief stop and subsequent search.[294] The *Terry* Court nonetheless refused to suppress the weapons, thus approving the police conduct at issue.[295] Although the result itself was significant, the Court's reasoning was an equally momentous break with prior Fourth Amendment jurisprudence.

Chief Justice Warren's novel approach to the question facing the Court in *Terry* provides a blueprint for a workable approach to the third party doctrine. Of critical importance is how Chief Justice Warren parsed the Fourth Amendment to separate the probable cause requirement for a warrant from what constitutes reasonable conduct in the search context. The Court accepted that the stops at issue in *Terry* implicated the Fourth Amendment. But that fact alone did not trigger the Warrant Clause or its attendant probable cause requirement as noted in Part III.[296] Instead, the Court set out to determine the reasonableness of McFadden's actions.

In crafting its reasonableness inquiry, the Court could have followed the path set out by prior cases. Only one year before, in *Camara v. Municipal Court of San Francisco*,[297] the Court approved an administrative search through a reasona-

290. *Id.*
291. *Id.* at 7–8.
292. *Id.* at 8.
293. *Id.* (internal quotation marks omitted).
294. *Id.* at 19–20.
295. *Id.* at 30–31.
296. *See id.* at 18–19 (finding that the Fourth Amendment "permit[ted] a reasonable search for weapons for the protection of the police officer . . . regardless of whether he has probable cause to arrest the individual for a crime").
297. 387 U.S. 523 (1967).

bleness inquiry.[298] There the Court determined reasonableness by balancing the government interest against the private interest. The Court lamented that "[u]nfortunately, there can be no ready test for determining reasonableness" other than by case-by-case fact intensive balancing of "the need to search against the invasion which the search entails."[299] But while judges were capable of weighing systematic programs through *Camara*-like balancing, the *Terry* Court recognized a need for a test that law enforcement officers in one-off encounters could apply in the field.[300]

Accordingly, the Court adopted a new type of reasonableness inquiry. Instead of requiring lower courts to weigh independently the interests of officer and citizen in each case, the Court sought to create a single test, equally administrable by courts and law enforcement alike. Rather than looking at the specific facts of the case, the *Terry* Court performed a one-time high-level balancing of frisks "as a general proposition."[301] Ultimately, the government's interest prevailed, so long as the frisk was limited in scope.[302]

Next, the Court used the balancing it had just completed to create a new test: "whether a reasonably prudent man in the circumstances would be warranted in the belief that his safety or that of others was in danger . . . [giving] due weight . . . to the specific reasonable inferences which he is entitled to draw from the facts in light of his experience."[303] This is the remaining piece of the puzzle. So long as reasonableness was locked in an individual-specific inquiry into subjective expectations, no generalizable doctrine could emerge. In *Terry*, therefore, the Court declined to require the weighing of government and private interests in every case; the Court instead called for an objective evaluation of the specific situation at hand, but under the single, newly crafted standard.[304] Such an approach relieved police from the burdens of examining the extent of government interest in a given pat down, allowing officers like McFadden to rely on the good judgment that led to his suspicion.

---

298. *Id.* at 536–37 (describing the process of "balancing the need to search against the invasion which the search entails").

299. *Id*.

300. *Terry*, 392 U.S. at 27.

301. *Id.* at 19–20.

302. *Id.* at 26.

303. *Id.* at 27 (citation omitted).

304. *Id.*

Although the *Terry* majority never uttered the words, "reasonable suspicion" has become *Terry*'s legacy.[305] The Court for a time resisted the "reasonable suspicion" standard, urging lower courts to eschew specific articulations that "fall short of providing clear guidance dispositive of the myriad factual situations that arise."[306] More recently, however, the Court has succumbed to the necessity of a uniform standard, characterizing *Terry* as allowing police officers "to act instantly on reasonable suspicion that the persons temporarily detained are armed and dangerous."[307] As noted above,[308] the doctrine has been extended to temporary detentions of suitcases[309] and even cars.[310] Irrespective of whether a uniform phrase or a more cumbersome articulation of the *Terry* standard is used, the Court's reasoning is useful in crafting a new third party doctrine.

B. THIRD PARTY BALANCING ACT

The *Terry* Court's move from case-by-case balancing to a uniform standard can be used to create an equally administrable standard for third party materials. As discussed in Part III, though the Fourth Amendment is implicated in police acquisition of third party information, the diminished expectation of privacy attending to such information counsels against requiring either a warrant or probable cause.[311] Only a determination of reasonableness remains. Attempts to look at reasonableness by distinguishing either by types of third party information or total quantity of information, evaluated in Part II, suffer from significant shortcomings.

Instead, courts should take a step back and conduct a one-time balancing of the reasonableness of government access to third party material "as a general proposition," in the hopes of distilling a uniform standard that can be applied across contexts. In *Terry*, the significant governmental interest in police safety and unfettered police investigation outweighed the intrusion into a protected space.[312] The Court pointed to a trial

305. The "reasonable suspicion" language that has become synonymous with *Terry* can be found in Justice Douglas's dissent. *Id.* at 37 (Douglas, J., dissenting) ("The term 'probable cause' rings a bell of certainty that is not sounded by phrases such as 'reasonable suspicion.'").

306. United States v. Cortez, 449 U.S. 411, 417 (1981).

307. Arizona v. Johnson, 555 U.S. 323, 330 (2009).

308. *See supra* Part III.

309. *See* United States v. Place, 462 U.S. 696, 698 (1983).

310. *See* Alabama v. White, 496 U.S. 325, 328 (1990).

311. *See supra* Part III.

312. Terry v. Ohio, 392 U.S. 1, 27 (1968) ("[T]here must be a narrowly

court's finding that the suspect "presented a threat to the officer's safety while he was investigating his suspicious behavior."[313]

First, the privacy interests at stake in third party searches differ from those searches subject to the Fourth Amendment's full warrant and probable cause requirements. While much ink has been spilled arguing that third party information merits Fourth Amendment protection,[314] such a conclusion means only that people have a reasonable expectation of privacy in the information turned over to others. Measuring the extent of the privacy interest, however, is another matter. As has been established, the expectation of privacy is much diminished as compared to the prototypical home invasion that invokes the full protections of the Warrant Clause.[315] Indeed, currently the Supreme Court recognizes no such expectation.[316] Thus, without vastly departing from current doctrine, the Court could find a private interest at stake comparable to the interest in being free from a brief pat down, due to the legitimate but lesser expectation of privacy in each case.

Turning to the government interest at stake, the absence of the officer safety rationale obviously distinguishes third party searches from *Terry*. Whereas the interactions contemplated by *Terry* offer the potential for violent confrontation between officers and suspects, third party searches are defined by a lack of contact between officers and suspects (this lack of contact, in fact, is part of what makes such searches valuable).[317] Yet the logic of *Terry* does not rise or fall with officer safety; in *Place*, the Court extended *Terry* to brief detentions of luggage at airports.[318] The Court found "a generalized interest in law enforcement" sufficient to "justify an intrusion on an individual's Fourth Amendment interests in the absence of probable

drawn authority to permit a reasonable search for weapons . . . regardless of whether [the police officer] has probable cause to arrest the individual for a crime.").

313. *Id.* at 28.

314. Andrew J. DeFilippis, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1108 (2006) (advocating that the Court overrule the third party doctrine); *see also supra* Part I.B.

315. *See supra* Part III.B.2.

316. *See* California v. Greenwood, 486 U.S. 35, 41 (1988) (citing Smith v. Maryland, 442 U.S. 735, 743–44 (1979)); *see also supra* Part I.

317. *See* Kerr, *supra* note 2, at 562–63 (explaining that third party information is valuable to investigators "as [third parties] are more likely to cooperate and less likely to tip off the suspect that an investigation is afoot").

318. United States v. Place, 462 U.S. 696, 702–04 (1983).

cause."[319] As discussed in Part III, there is a substantial law enforcement interest in access to third party information at the initial stages of investigation—not merely after probable cause sufficient to obtain a warrant has already been established. Developing leads and building probable cause requires the gathering of clues nearly impossible without access to at least *some* third party information.

Weighing the privacy interest with the government need, courts should, as in *Terry*, craft a uniform standard that takes account of the different sides of the ledger. In the next section, we explain what such a standard should look like, taking as its cue the reasonable suspicion standard created in *Terry*.

C. A NEW THIRD PARTY TEST

A reasonable suspicion test for third party searches could operate as a practical middle ground between requiring warrants and probable cause, and the Court's current refusal to recognize any reasonable expectation of privacy. To articulate the test, we propose looking to *Terry* and its progeny: *officers should be able to point to specific, articulable facts supporting a reasonable suspicion that the third party search will turn up information relevant to an ongoing investigation, and searches should be reasonable in scope*. Both of these elements are present in *Terry* and its kin. While, as noted above, the common interpretation of the case focuses on the reasonable suspicion prong,[320] the Court has also been careful to note that a search that strays beyond the scope set by *Terry* runs afoul of the Fourth Amendment.[321] The application of this test will be discussed in turn.

1. Reasonable Suspicion

The reasonable suspicion test is familiar from *Terry*: the officer must have "reason to believe" that the search is necessary, based upon "the specific reasonable inferences which he is entitled to draw from the facts in light of his experience."[322] In the context of a third party search, there would have to be a reasonable belief that the search will turn up relevant information. Courts have found such a standard administrable in the context of the Stored Communications Act (the SCA),[323]

319. *Id.* at 703–04.
320. *See* Arizona v. Johnson, 555 U.S. 323, 330 (2009).
321. *See* Minnesota v. Dickerson, 508 U.S. 366, 373 (1993).
322. Terry v. Ohio, 392 U.S. 1, 27 (1968).
323. 18 U.S.C. § 2703(d) (2012) ("Requirements for Court Order.—A court

which adopts the *Terry* standard.[324] In *United States v. Perrine*, for example, the Tenth Circuit evaluated whether a request for the defendant's IP address and name was based on "specific and articulable facts" that supported "a reasonable suspicion that [the defendant] was involved in child pornography."[325] Pointing to the police officer's affidavit, in which he described conversing with a witness and viewing the witness's chat logs, the court found that the search was reasonable under the SCA standard.[326]

2. Reasonable Scope

The second inquiry for the courts would be whether a third party search is reasonable in scope. In *Terry*, the Court made clear that protective frisks "must be limited to that which is necessary for the discovery of weapons which might be used to harm the officer or others nearby."[327] Application of this standard to third party searches poses some difficulty; while the purpose of a *Terry* frisk is officer protection, the purpose of a third party search is acquisition of information. *Terry*'s language, however, provides guidance. Third party searches can be limited to "that which is necessary" to the investigation.[328] Therefore, an indiscriminate dredging of third party information unrelated to the object of the investigation, or clearly exceeding the bounds necessary to acquire the sought-after information, would go beyond the permissible scope of the search.

In the third party context, courts would have to examine the nexus between the method used and the information sought. Take, for example, *Smith*, where the Court focused entirely on the question of whether the pen register installed on the suspect's phone constituted a search. The Court could instead have examined the specific and articulable facts that led the police to believe that this limited quantity of information—

---

order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.").

324. *See, e.g.*, United States v. Perrine, 518 F.3d 1196, 1202 (10th Cir. 2008) ("[T]he 'specific and articulable facts' standard derives from the Supreme Court's decision in *Terry*. Thus, we are familiar with the standard imposed.").

325. *Id.* at 1203.

326. *Id.* at 1204–05.

327. *Terry*, 392 U.S. at 26.

328. *Id.*

a mere single day of pen register data[329]—would provide information relevant to the investigation. Such evidence was legion: the victim of a robbery had provided police with a description of a pattern of harassing phone calls associated with a man in a vehicle driving by her house, and on this basis the police observed the vehicle's license plate, traced it to the defendant's address, and requested the pen register.[330] Yet in other circumstances, an equally limited search via pen register could fail this test, if the police had no specific and articulable basis for thinking that the pen register would produce relevant information.

D. EVALUATING THE TEST

The proposed test has four major advantages over its rivals: first, it provides standing for defendants to challenge searches, and in doing so enables judicial oversight over police surveillance and investigation tactics; second, it does not overly disrupt current police practice; third, it is easily administrable; and fourth, it preserves the advantages of the current third party doctrine.

1. Judicial Oversight Through Standing

Having tied our proposed test to the reasonable suspicion standard, we acknowledge its susceptibility to the myriad criticisms levied against *Terry*. Numerous voices in the academy rail against *Terry*'s test, which they criticize as a paltry restraint on police misbehavior, as well as its metastasis from narrow exception to presumptive default.[331] Yet even partially

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

330. *Id.*

331. Attempting to catalogue the criticisms of the *Terry* doctrine would be unwise, but even a small collection demonstrates scholars' general dissatisfaction. *See, e.g.*, Thomas Gerry Bufkin, Terry *and* Miranda*: The Conflict Between the Fourth and Fifth Amendments to the United States Constitution*, 18 MISS. C. L. REV. 199, 204 (1997) ("[T]he lower federal courts have proceeded on their path to expanding the permissible scope of police action in a *Terry* stop."); Mark A. Godsey, *When* Terry *Met* Miranda*: Two Constitutional Doctrines Collide*, 63 FORDHAM L. REV. 715, 747 (1994) (arguing that courts have not remained true to *Terry*'s premises); Daniel C. Isaacs, Miranda*'s Application to the Expanding* Terry *Stop*, 18 J.L. & POL'Y 383, 387 (2009) ("The permissible degree of intrusion during a 'stop and frisk' has significantly expanded since 1968."); Rachel Karen Laser, *Unreasonable Suspicion: Relying on Refusals To Support* Terry *Stops*, 62 U. CHI. L. REV. 1161, 1169 (1995) ("[C]ourts have interpreted the 'totality of the circumstances' broadly, thus expanding the scope of what constitutes an acceptable *Terry* stop."); Michael J. Roth, Berkemer *Revisited: Uncovering the Middle Ground Between* Miranda *and the New* Terry, 77 FORDHAM L. REV. 2779, 2779 (2009) ("[A]ppellate courts

accepting this critique, the reasonable suspicion test for third party information provides valuable protection, striking the proper balance between privacy and law enforcement interests. We believe this to be true for two reasons, one doctrinal and the other practical.

First, the reasonable suspicion test provides persons the right to challenge the collection of their personal information held by third parties. Under current Fourth Amendment jurisprudence, individuals who provide their information to third parties cannot dispute the collection of their information based on a lack of standing under the Fourth Amendment.[332] Fourth Amendment standing requires that a person challenging the introduction of evidence show a recognized expectation of privacy in the evidence seized before suppression will be entertained.[333] Thus, the third party doctrine all but prevents litigants from challenging third party seizures because the Court refuses to recognize *any* expectation of privacy on the part of the defendant. Instead, standing attaches to the possessor of the information at the time of the government's search.[334] The reasonable suspicion test would correct this deficiency by recognizing an expectation of privacy, even if diminished, sufficient to bestow standing to challenge the introduction of evidence.

Consider the effect of the reasonable suspicion test on an early third party case. In *United States v. Payner*,[335] the Court refused to suppress bank records obtained from a bank execu-

---

have significantly expanded the scope of police authority to stop and frisk potential suspects without probable cause . . . ."). At times, the judiciary has echoed the scholarly frustration. *See* United States v. Perdue, 8 F.3d 1455, 1464 (10th Cir. 1993) ("The last decade . . . has witnessed a multifaceted expansion of *Terry*."); United States v. Chaidez, 919 F.2d 1193, 1198 (7th Cir. 1990) ("[The doctrine has] expanded beyond [its] original contours, in order to permit reasonable police action when probable cause is arguably lacking.").

332. *See generally* Stephen P. Jones, *Reasonable Expectations of Privacy: Searches, Seizures, and the Concept of Fourth Amendment Standing*, 27 U. MEM. L. REV. 907, 909–12 (1997) (describing Fourth Amendment standing). While courts no longer evaluate standing as an explicit factor in their analyses, standing has become part of the examination of reasonable expectation of privacy. *See* DeFilippis, *supra* note 314, at 1102 & n.62.

333. *See* Rakas v. Illinois, 439 U.S. 128, 134 (1978) ("A person who is aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by a search of a third person's premises or property has not had any of his Fourth Amendment rights infringed.").

334. *See* DeFilippis, *supra* note 314, at 1102 ("The third-party doctrine has effectively denied standing to defendants who allege illegal government seizure of personal data held [by others].").

335. 447 U.S. 727 (1980).

tive. Though the case seemed to fall squarely under *Miller*, which also involved bank records,[336] the method through which police obtained the records raised questions. The government agents illegally entered into the apartment of a bank's vice president, stole his briefcase, and copied the contents of documents containing the financial information of one of the bank's clients.[337] When the government attempted to introduce the evidence in prosecuting the bank's client, the trial court suppressed the evidence, with the court of appeals affirming.[338] The Supreme Court, however, reversed; although the Court recognized that "no court should condone the unconstitutional and possibly criminal behavior of those who planned and executed this 'briefcase caper,'" the Court refused to suppress the admission of the evidence against the defendant on the grounds that it was only the vice president's privacy interest that had been intruded upon.[339] Under the reasonable suspicion test, by contrast, recognition of Payner's privacy interest in the documents—even if diminished—would eliminate the bar to consideration of the illegality of the search. As the Court recognized in *Rakas v. Illinois*,[340] a defendant in Payner's situation could "contest the lawfulness of the seizure of evidence or the search if [his] own property were seized during the search."[341] And of course, a defendant's ability to challenge a search allows a court the ability to weigh in on the investigatory techniques at issue, rather than being forced to impotently condone the conduct based on the party at the defense table.

2. Administrability

The proposed reasonable suspicion standard should be administrable both by law enforcement agencies and the courts. The standard and procedure associated with the test is familiar to the police, the defense bar, and the courts alike. Defense attorneys are experienced in probing claims of reasonable suspicion and judges practiced at adjudicating disputes under the standard.

336. United States v. Miller, 425 U.S. 435, 437–38 (1976).

337. *Payner*, 447 U.S. at 729–30.

338. *Id.* at 730–31.

339. *Id.* at 733–35 ("[T]he supervisory power does not authorize a federal court to suppress otherwise admissible evidence on the ground that it was seized unlawfully from a third party not before the court.").

340. 439 U.S. 128 (1978).

341. *Id.* at 142 n.11.

Most importantly, the standard is easily applied by law enforcement. Discussing the warrantless searches of vehicles incident to arrest, the Court stated that

> Fourth Amendment doctrine . . . is primarily intended to regulate the police in their day-to-day activities and thus ought to be expressed in terms that are readily applicable by the police. . . . A highly sophisticated set of rules, qualified by all sorts of ifs, ands, and buts . . . may be the sort of heady stuff upon which the facile minds of lawyers and judges eagerly feed, but they may be literally impossible of application by the officer in the field.[342]

In another context, the Court has noted that "law enforcement officers need to know, with certainty and beforehand, when renewed interrogation is lawful."[343] Certainly the existing standard—all third party searches are constitutionally unregulated—provides that certainty.

But assuming the need for some regulation, a standard based upon reasonableness should not fall prey to the seduction of sophistication. Unlike mosaic theory, which requires law enforcement officers to constantly survey the entirety quantity of gathered information from an abstract perch, the reasonable suspicion test requires evaluation of only one piece of information at a time. Furthermore, it is evaluated objectively from the perspective of a reasonable officer, rather than from the perspective of the target or society at large.

Viewed from the perspective of courts, meanwhile, the *Terry* standard—through its incorporation into the Stored Communication Act—has already proven an applicable standard for courts. In *United States v. Perrine*,[344] the Tenth Circuit noted its familiarity with the *Terry* standard and applied the "specific and articulable facts" requirement to the affidavit the United States had submitted in support of its request for electronic subscriber information.[345] The Tenth Circuit went on to note that the greater protections of the Fourth Amendment did not apply to such information,[346] but it is apparent that were the constitutional framework raised to the standard required under the statutory framework, it would not overly tax courts.

Similarly, state supreme courts have applied the *Terry* framework under their state constitutions to at least some cat-

342. New York v. Belton, 453 U.S. 454, 458 (1981) (internal quotation marks omitted) (quoting LaFave, *supra* note 152, at 141–42), *abrogated by* Arizona v. Gant, 556 U.S. 332, 348 (2009).

343. Maryland v. Shatzer, 559 U.S. 98, 110 (2010).

344. 518 F.3d 1196 (10th Cir. 2008).

345. *Id.* at 1202–04.

346. *Id.* at 1204–05.

egories of searches that currently go unprotected under the Fourth Amendment. In *Litchfield v. State*,[347] the Indiana Supreme Court rejected the rule of *California v. Greenwood*[348] and imposed upon the police, before searching garbage, "a requirement of articulable individualized suspicion, essentially the same as is required for a 'Terry stop' of an automobile."[349] The Alaska Supreme Court followed suit, applying to searches of garbage "[t]he reasonable suspicion standard . . . most often applied in the context of investigatory stop-and-frisks."[350] Professor Stephen E. Henderson has endorsed the departure of states from the Supreme Court's third party doctrine; though he expresses concern over the difficulty of application of complex, multilayered standards, he has noted the comparative simplicity of a single standard of suspicion laid out beforehand:

> One saving grace may be that such decisions can be made without requiring discretion and hard work on the part of police officers in the field. Once a court requires a given quantum of suspicion and/or a given procedure to obtain a certain type of information, officers (and attorneys) will have clear guidance.[351]

We agree, and are optimistic that the reasonable suspicion standard, built for administrability by police in the *Terry* stop context, can be transferred to the collection of third party information without unduly taxing officers of the court or the law.

3. Maintaining Doctrinal Advantages

Kerr identifies two vital attributes of the Fourth Amendment as currently constituted that would be eviscerated under the many critics' alternative schemes: technological neutrality and *ex ante* clarity.[352] The third party doctrine ensures that the Fourth Amendment remains technologically neutral by extending preexisting protections to communicative or storage *functions* without regard to the *form* used.[353] By focusing on the technology used, Kerr argues, proposed alternatives might allow criminals to purposefully refrain from using third party services lacking protection and instead choose to funnel com-

347. 824 N.E.2d 356 (Ind. 2005).

348. 486 U.S. 35, 39–45 (1988) (finding no reasonable expectation of privacy in garbage placed on the street).

349. *Litchfield*, 824 N.E.2d at 364.

350. Beltz v. State, 221 P.3d 328, 336 (Alaska 2009).

351. Henderson, *supra* note 69, at 423.

352. *See* Kerr, *supra* note 2, at 579–81 (technological neutrality); *id.* at 581–83 (*ex ante* clarity).

353. *See id.* at 579–81.

munication through channels receiving Fourth Amendment protection.[354] Whereas the third party doctrine does not differentiate between toll records and social media posts, another regime recognizing special protection for social media would funnel insidious communications through Facebook. He argues that proposals lacking such neutrality allow criminals to shield their malfeasance through a "substitution effect."[355] Instead of passing messages through unprotected mediums, criminals will opt to communicate only on technologies that the Fourth Amendment protects.[356]

Kerr also notes that the current third party doctrine provides the Fourth Amendment with *ex ante* clarity. The doctrine ensures that, upon reaching its destination, information sheds any prior status for whatever protections it receives in its current location.[357] Providing protection based on where the information originated would only cause confusion for law enforcement.[358] The alternative, asking officers to know from where the data they request originated, would tremendously complicate police procedures for subpoena and seizure, leading to significantly more suppressions at trial.[359]

The reasonable suspicion test would maintain both technological neutrality and *ex ante* clarity. Applying a uniform standard for all third party information ensures technological neutrality.[360] Whether police wish to use written bank records or e-mail metadata, they must use the same faculties of reason buttressed by specific, articulable facts, and the courts will engage in the same reasonable suspicion analysis. In fact, the reasonable suspicion approach might be *more* technologically neutral than current doctrine. Kerr has acknowledged, in response to Epstein's similar suggestion to create an intermediate zone of reasonable suspicion, that a more flexible approach would ease the cliff effect between full-blown warrant-and-

354. *Id.* at 580 ("Those who have the most to hide have the most incentive to take advantage of how third-party services can hide their activity.").

355. *Id.* at 574–76; *see also* Reid, *supra* note 244, at 615–17.

356. *See* Kerr, *supra* note 2, at 574–76.

357. *Id.* at 582 ("[The doctrine] guarantees that once information is present in a location it is treated just like everything else located there.").

358. *Id.* ("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.").

359. *Id.* at 581–82.

360. *See id.* at 579–81 (describing the *Katz* test as technologically neutral because it could be applied uniformly).

probable-cause protection and no protection at all; accordingly, it would reduce the incentive to substitute forms of communication.[361]

Similarly, the reasonable suspicion standard provides *ex ante* clarity, with a single standard of reasonable suspicion applicable across types of information. Admittedly, the current doctrine's blanket lack of protection is even clearer, but Kerr's concerns regarding the burden on police to determine where information originated is unfounded under the reasonable suspicion test. If, as Kerr contends, clarity is intended to ensure the police understand the rules,[362] a test relying on the perspective of a reasonable officer fulfills that requirement.

By contrast, most substitutes for the third party doctrine cannot satisfy Kerr's criteria. The mosaic theory, for example, would drastically reduce clarity for law enforcement officers who will be faced with the difficult question of how much data is too much.[363] Justice Alito recognized the difficulty of determining exactly how much GPS data would constitute an unreasonable search;[364] imagine an officer trying to determine how many Facebook posts, cellphone location requests, and phone numbers dialed she could examine before running afoul of the Fourth Amendment. Similarly, a pure reasonableness balancing approach would destroy any semblance of clarity for officers. Amar's reliance on the wisdom of the community, expressed through jury verdicts, to dictate reasonableness would prove impossible to predict.[365] Meanwhile categorization, though clear *ex ante*, would violate the precept of technological neutrality either through protecting certain technologies over others—as social media proponents suggest[366]—or by broadly blanketing practically all digital third party information with protection—as Solove's system of records would.[367]

---

361. *See* Kerr, *supra* note 74.

362. *Id.* at 1236 ("The police need certain answers about what rules they must follow.").

363. Kerr, *supra* note 101, at 341 ("[O]fficers may understandably cross the line without personal culpability.").

364. United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in the judgment).

365. *See supra* Part II.C (arguing that pure balancing is unworkable for officers in the field).

366. *See supra* Part II.B (describing arguments in favor of exempting social media information from the third party doctrine).

367. *See supra* Part II.B (criticizing Professor Solove's critique as overbroad).

V. LIMITATIONS AND IMPLICATIONS

As noted above, an important advantage of the reasonable suspicion test is that it eases the cliff effect between the full protections of the Warrant Clause and the absence of Fourth Amendment protections altogether. Subjecting third party searches to the Reasonableness Clause, however, does create its own new line-drawing problem: When does an investigatory tactic become a third party search, subjecting it to the reasonable suspicion test? Further, the reasonable suspicion test does not resolve some of the difficult questions currently confronting courts about the boundary between the third party doctrine and a "full blown search" requiring warrant and probable cause. And finally, the reasonable suspicion framework only applies to third party searches based on individualized suspicion. While this Article's test does not incorporate the data mining programs currently before the courts, it provides a path for courts and future scholars to follow in addressing them.

A. THIRD PARTY SEARCHES AND NONSEARCHES

Defining the limit between third party searches and nonsearches would be a novel task for courts, one that had previously been unnecessary due to *Smith* and *Miller*. Courts would confront such questions as: whether the use of secret agents and informants—identified by Kerr as a key progenitor of the third party doctrine's concentration on business records[368]—constitutes a third party search; whether government agents must probe the source of anonymous tips to determine whether they compromise third party information;[369] and when information is exposed to the public at large as opposed to being entrusted to specific third parties.[370] Yet such questions should not prove overly vexing to either officers or courts. Officers do not need to prove the extent of the privacy interest on the other side of the ledger before acting in these circumstances. They simply need to be able to point to specific, articulable facts supporting a reasonable suspicion that evidence is to be found within a search of reasonable scope. It is true that such a limitation would engender more self-reflection than complete

368. Kerr, *supra* note 2, at 567–69.

369. Kerr offers the example of police receiving an anonymous tip alleging a politician's corruption, and posits five potential sources that could implicate the third party doctrine to varying degrees. *See id.* at 584–85.

370. *Cf., e.g.*, Strandburg, *supra* note 105, at 671–75 (offering the examples of Facebook messages, Facebook profile information, and posts in a public chatroom).

freedom from Fourth Amendment scrutiny, but the resulting behavior should emulate best practices of investigation—focused inquiry rather than blind casting about—or prove a welcome correction.

For courts, meanwhile, hard cases at the boundary could often be dispatched by looking first to the behavior of the police: if the police acted upon reasonable suspicion and confined to a reasonable scope, there would be no need to ask whether the information acquired fell within the third party doctrine or outside the Fourth Amendment altogether. It is only where the police had no reasonable suspicion or the scope of their search was unreasonable that it would be necessary to ask whether a search had taken place.

B. THIRD PARTY SEARCHES AND FULL BLOWN SEARCHES

The reasonable suspicion test tells courts how they are to evaluate third party searches, rather than what constitutes a third party search. In other words, the difficult line already confronted by courts between third party searches and "full blown searches" would still need to be drawn. For example, the traditional content/noncontent distinction has held that the outside of a package or envelope is publicly viewable and contains no content carrying significant privacy interests, while its inner contents are protected; courts have begun to encounter the question of how this distinction translates to digital information such as e-mails and detailed browsing history.[371] Other questions that may arise including whether use of a computerized automated remote backup system—such as Dropbox—constitutes entrusting one's information to a third party in the absence of any expectation that the remote server will actually access that information.[372] While our test cannot solve these problems, by creating an alternative between no protection and probable cause it reduces the "incredible pressure on the courts to reduce the scope of the Fourth Amendment by narrowly defining 'search' and 'seizure.'"[373]

371. *See, e.g.*, United States v. Forrester, 512 F.3d 500, 510–11 & n.6 (9th Cir. 2008).

372. In *Smith v. Maryland*, 442 U.S. 735 (1979), the Court relied heavily upon an extended discussion of the uses to which phone companies put records of calls sent and received, and users' expectations thereof. *Id.* at 742–43.

373. Slobogin, *supra* note 117, at 1067.

C. DATA MINING

Perhaps the most immediate debate around the Fourth Amendment surrounds data mining.[374] Data mining takes two primary forms: "target-driven data mining," which is "a search of records to obtain information about an identified target"; and "[e]vent-driven data mining, also called pattern-based surveillance," which "does not start with an identified suspect."[375] Target-driven data mining, as the name suggests, is driven by individualized suspicion about the target, thus rendering it sussusceptible to the reasonable suspicion test. Pattern-based data mining, by contrast, does not operate on individualized suspicion. For this pattern-based variety, while the reasonable suspicion framework does not apply, the Reasonableness Clause of the Fourth Amendment may provide an alternative path forward.

When the government seeks to access[376] a set of third party records—whether in the hands of third parties or the government itself[377]—about a specific individual, this Article's framework can help courts evaluate the reasonableness of that access

374. *See* ACLU v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013) (permitting the NSA's mass collection of telephonic metadata), *vacated*, 785 F.3d 787 (2d Cir. 2015); Klayman v. Obama, 957 F. Supp. 2d 1, 30–37 (D.D.C. 2013) (opposite), *vacated*, 800 F.3d 559 (D.C. Cir. 2015).

375. Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 322–23 (2008). Slobogin also provides a third category, "match-driven data mining," which seeks to ascertain whether a suspect is, for example, already in a fingerprint, facial-recognition, or DNA database. *Id.*

376. A further question, outside the scope of this Article, is whether the *collection* of such data—as opposed to its *analysis*—implicates privacy concerns (and, by extension, the Fourth Amendment). *Compare, e.g.*, Richard A. Posner, *Our Domestic Intelligence Crisis*, WASH. POST (Dec. 21, 2005), http://www.washingtonpost.com/wp-dyn/content/article/2005/12/20/AR2005122001053.html ("But machine collection and processing of data cannot, as such, invade privacy."), *and* William J. Stuntz, *Against Privacy and Transparency*, NEW REPUBLIC (Apr. 17, 2006), http://www.newrepublic.com/article/against-privacy-and-transparency ("The best way to stop the nightmare from happening is to limit not what information officials can gather, but what they can do with the information they find."), *with* Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343, 356 (2008) ("It is certainly true that disclosure and use of information can create significant privacy problems. But collection can create problems as well.").

377. Whether mass databases of third party information, such as telephonic and internet metadata, should be held by the government or by third parties is a live controversy as of this Article's writing. *See* Jack Goldsmith, *Bruce Schneier on NSA v. Private Meta-Data Storage*, LAWFARE (Feb. 14, 2014, 4:18 PM), https://www.lawfareblog.com/2014/02/bruce-schneier-on-nsa-v-private-meta-data-storage (describing an ongoing debate on who should warehouse NSA data).

as a matter of Fourth Amendment law. Take, for example, the facts of *Smith*, where the government was seeking to confirm the identity of a stalker and possible robber based upon descriptions of phone calls received by the victim.[378] If the government had potentially available to it all of Smith's phone calls, bank records, internet domains visited, Facebook activity, e-mails sent and received, etc., what of this information could it reasonably access? This Article's test would demand that the government demonstrate reasonable suspicion that a given set of records would produce evidence relevant to the investigation, and that the scope of the search not exceed that which is necessary. Given the witness's description of several days of harassing phone calls, the government would be entitled to access Smith's phone records over that time period. Bank records would be a closer question, but the government could reasonably suspect that Smith might have received and deposited a significant amount of money following the robbery, depending on what was taken. However, his browser history, e-mail contacts, and Facebook activity would all be too unlikely to yield evidence of the crimes,[379] and thus would fall outside the reasonable scope of the search.

For pattern-based data mining, the reasonable suspicion framework would not provide a workable solution, any more than one could stop and frisk an entire street full of people because one suspects that one of them might have a gun. However, courts could follow the doctrinal framework set out in Part III to evaluate the mass analysis of third party data through the lens of the Reasonableness Clause. Under this analysis, pattern-based data mining would constitute a suspicionless programmatic search akin to those that have been analyzed under the Court's special needs doctrine, where courts balance intrusiveness against government need.[380] Under such a framework, for example, the Second Circuit upheld suspicionless bag searches in the New York City subway in the wake of the London tube bombings.[381] In the context of data

378. *See* Smith v. Maryland, 442 U.S. 735, 737 (1979).

379. It is obviously possible to imagine that such records *could* turn up evidence of a crime, but from the facts of *Smith* there would be no specific, articulable facts to so suggest.

380. *See supra* Part III.A.2 (discussing Ferguson v. City of Charleston, 532 U.S. 67, 76–86 (2001); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 654–66 (1995); Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 624 (1989); Griffin v. Wisconsin, 483 U.S. 868, 873 (1987); New York v. Burger, 482 U.S. 691, 693 (1987)).

381. *See* MacWade v. Kelly, 460 F.3d 260, 275 (2d Cir. 2006).

mining, courts would have to weigh the privacy intrusion of the mass analysis of third party information against the government's interest. This evaluation is far beyond the scope of this Article—and would depend heavily upon the details of a particular program—but the relocation of third party searches from outside the Fourth Amendment to within its Reasonableness Clause offers a doctrinal path forward for future analyses.

CONCLUSION

Controversy surrounding the third party doctrine will not abide any time soon. On one side are those who believe that the protections of warrant and probable cause requirements long afforded to private information need to be extended onto the platforms where such information now resides. On the other side are those who believe that, in an era when commercial actors can assemble stunningly detailed portraits of one's relationships, habits, and proclivities, such requirements would hamstring the government in the service of providing no more than an illusory fig leaf of privacy. The middle ground outlined in this Article will likely satisfy neither camp. Yet as a matter of Fourth Amendment law, the third party doctrine fits naturally within the warrant exceptions subject to a rule of reasonableness. And, as a practical matter, such a move will allow courts to impose a uniform standard that will provide necessary oversight to curb the worst abuses of privacy while affording discretion and clarity to law enforcement.