Fordham Law Review

Volume 84 | Issue 2 Article 11

2015

Fourth Amendment Fiduciaries

Kiel Brennan-Marquez
New York University School of Law

ARTICLES

FOURTH AMENDMENT FIDUCIARIES

*Kiel Brennan-Marquez**

Fourth Amendment law is sorely in need of reform. To paraphrase Justice Sotomayor's concurrence in United States v. Jones*, the idea that people have no expectation of privacy in information voluntarily shared with third-parties—the foundation of the widely reviled "third-party doctrine"—makes little sense in the digital age.*

In truth, however, it is not just the third-party doctrine that needs retooling today. It is the Fourth Amendment's general approach to the problem of "shared information." Under existing law, if A *shares information with* B*,* A *runs the risk of "misplaced trust"—the risk that* B *will disclose the information to law enforcement. Although the misplaced trust rule makes sense as a default, it comes under strain in cases where* A *and* B *have no relationship of trust and the only reason that* A *shares information with* B *is to obtain a socially valuable (and practically indispensable) service. In such cases, I argue that the doctrine should treat* B *as an "information fiduciary" and analyze* B*'s cooperation with law enforcement—whether voluntary or compelled—as a Fourth Amendment search.*

The argument develops in three parts. Part I demonstrates that the Court has already identified two settings—if only implicitly—where fiduciary-style protections are necessary to safeguard constitutional privacy: medical care and hotels. When A *is a patient and* B *is a doctor, and, likewise, when* A *is a guest and* B *is a hotel manager, the Court has been reluctant to apply the "misplaced trust" rule. Rightly so: the principle is mismatched to the underlying relationship. From there, Part II fleshes out the*

* Postdoctoral Research Fellow, Information Law Institute, New York University School of Law; Visiting Fellow, Information Society Project, Yale Law School. Thanks are due to BJ Ard, Jack Balkin, Jane Bambauer, Bryan Choi, Sherry Colb, Tom Dannenbaum, Jen Daskal, Kevin Frick, Michael Gottesman, David Gray, James Grimmelmann, Woody Hartzog, Stephen Henderson, Shishene Jing, Paul Kahn, Margot Kaminski, Paula Kift, Kara Loewentheil, Vivek Mohan, Helen Nissenbaum, Rachel Schwartz, Andrew Selbst, Chris Slobogin, Priscilla Smith, Kathy Strandburg, Olivier Sylvain, Andrew Todres, Andrew Tutt, and Carly Zubrzycki; to participants at the 2014 Privacy Law Scholars Conference who commented on an early draft of this paper; to NYU's Information Law Institute and Center on Law and Security, which invited me to present the paper at a symposium on law enforcement and big data; and to my friends, co-clerks, and family members, who patiently indulged tireless discussion of the topics addressed here. Errors are mine.

normative argument. Put simply, we do not "trust" information fiduciaries, in the everyday sense, at all. So it makes little sense—normatively, or even semantically—to speak of trust being "misplaced." Rather, the information is held for the benefit of the sharing party, and its use should be constrained by implied duties of care and loyalty. Finally, Part III lays the groundwork for determining who are "Fourth Amendment fiduciaries." The Article concludes by exploring various practical metrics that courts might adopt to answer this question.

INTRODUCTION

Fourth Amendment law has long embraced the proposition that disclosure invites betrayal. If *A* shares information with *B*, and *B* relays the information to the police, *A* can claim no constitutional harm. Beginning with *Katz v. United States*,[1] the watershed case prohibiting warrantless wiretaps, modern doctrine has focused on walling off private relationships from intrusion by law enforcement. But the doctrine has nothing to say—by design—about the possibility that those relationships are built on "misplaced trust."[2] Whatever else the Fourth Amendment protects against,

1. 389 U.S. 347 (1967).

2. *See* United States v. Jacobsen, 466 U.S. 109, 124–26 (1984) (finding no Fourth Amendment violation when a FedEx worker dismantled a customer's package, identified contraband, and reported the results to law enforcement); United States v. Miller, 425 U.S. 435, 443 (1976) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."); Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971) ("Had Mrs. Coolidge, wholly on her own initiative, sought out her husband's guns and clothing and then taken them to the police station to be used as evidence

one thing it does *not* protect against is the risk of another person voluntarily cooperating with the authorities.

This Article scrutinizes the "misplaced trust" rule. In a different age—when far less information was shared with others—this principle may have been sustainable in its strong form. But it is no longer. In today's world, we constantly disclose vast amounts of information to digital intermediaries: email providers, social media sites, and the like. A rote application of the misplaced trust rule would leave these intermediaries categorically free to take up the mantle of law enforcement: to serve as "Big Brother's little helpers,"[3] as long as the decision to do so is neither instigated nor remunerated by the state.[4] This status quo is intolerable, and it will only become more intolerable as time goes on.

My position is not that the misplaced trust rule should be discarded. To the contrary, the rule makes sense—as a default—on both practical and normative grounds. My position is that the misplaced trust rule is *only* a default, and Fourth Amendment doctrine should become more attentive to its exceptions. Analytically, those exceptions are easily summarized. The misplaced trust rule should not apply to information shared with "information fiduciaries."[5] If the nature of *A* and *B*'s relationship is such

---

against him, there can be no doubt under existing law that the articles would later have been admissible in evidence."); United States v. White, 401 U.S. 745, 749 (1971) ("[H]owever strongly a defendant may trust an apparent colleague, his expectations in this respect are not protected by the Fourth Amendment . . . ."); Hoffa v. United States, 385 U.S. 293, 302 (1966) ("[T]he Fourth Amendment [does not protect] a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.").

3. I borrow this phrase from Chris Hoofnagle. *See* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595 (2004) (exploring the ways in which private data companies collaborate with law enforcement).

4. *See Jacobsen*, 466 U.S. at 113 (explaining that the Fourth Amendment is "wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official"). Lower courts, tasked with applying this standard, have focused on the existence of (1) compulsion, and (2) remuneration. *See, e.g.*, Cassidy v. Chertoff, 471 F.3d 67, 74 (2d Cir. 2006) ("Although a wholly private search falls outside the scope of the Fourth Amendment, a search conducted by private individuals at the instigation of a government officer or authority constitutes a governmental search for purposes of the Fourth Amendment." (citation omitted)); United States v. Jarrett, 338 F.3d 339, 341, 344 (4th Cir. 2003) (holding an anonymous hacker's search for child pornography did not violate the Fourth Amendment—despite being a crime—because the Government did not "participate in," but rather "passively accept[ed] . . . a private party's search efforts"); United States v. Hall, 142 F.3d 988, 993 (7th Cir. 1998) (holding that a technician's discovery of files on defendant's computer, "made pursuant to . . . maintenance work" that "[t]he Government had no knowledge" of and "did not instruct" the technician to perform, is not protected by the Fourth Amendment; also noting that one consideration in determining whether a search was private is "whether the Government offered the private party a reward").

5. *See* Jack Balkin, *Information Fiduciaries in the Digital Age*, BALKINIZATION (Mar. 5, 2014, 4:50 PM), http://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html [http://perma.cc/VN5D-JBZP]; *see also* Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out*, NEW REPUBLIC (June 1, 2014), http://www.newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering (exploring, among other things, the idea that Facebook is an information

that *B* is obligated to prioritize *A*'s interests over her own, *B* should not be free to betray information shared by *A*. In those circumstances, the Fourth Amendment should not only constrain the way law enforcement officials gather information, but it should also constrain the way that private actors—information fiduciaries—transmit it.[6]

This Article proceeds in three parts. Part I is exegetical. Notwithstanding the absolute language that judges use—and commentators echo—when describing the misplaced trust rule, in fact there are two settings in which the Court's jurisprudence has already been sensitive to the need for heightened protection due to the types of relationships involved: medical care and hotels. When *A* is a patient and *B* is a doctor, and likewise, when *A* is a guest and *B* is a hotel manager, the Court has been reluctant to apply the misplaced trust rule. And rightly so: in both settings, it seemed apparent to the Court—even if existing doctrine offered no vocabulary to say so explicitly—that the rule would disserve, and perhaps disintegrate, the underlying relationship.

Equipped with these examples, Part II turns to normative analysis. Although there has been no shortage of commentary in recent years about the need to retool Fourth Amendment law for the digital age, the misplaced trust rule survives unscathed. Instead, the reform effort has focused primarily on *Smith v. Maryland*[7] and *United States v. Miller*[8]—progenitors of the so-called "third-party doctrine"—which hold that we have no expectation of privacy in the dialed numbers we share with phone companies[9] or in the financial information we share with banks.[10] In the shadow of *Smith* and *Miller*, scholars (and dissident judges) have been scrambling to explain why digital communication enjoys *any* Fourth Amendment protection, even from intrusion by law enforcement.[11] The

---

fiduciary) [http://perma.cc/TR9M-R29X]. These efforts have much in common, conceptually, with work that Neil Richards has done, along with Dan Solove and Woody Hartzog, on the normative relationship between privacy, confidentiality, and trust. *See* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123 (2007); Neil M. Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law* (Aug. 4, 2015) (unpublished manuscript), http://ssrn.com/abstract=2655719 [http://perma.cc/Z8VD-Y9W2].

6. Although reform efforts have not been entirely insensitive to this issue, they have tended to focus (for obvious reasons, given the doctrinal pedigree) on the law enforcement side of the equation. *See, e.g.*, ABA STANDARDS FOR CRIMINAL JUSTICE: LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS 99–111 (3d ed. 2013) [hereinafter ABA STANDARDS] (outlining the criteria that law enforcement should be required to satisfy before seizing records from institutional third parties). Although this is certainly a step in the right direction, in my view a full account of constitutional privacy today must also interrogate the *other* side of the equation: To what extent should third parties be able to cooperate with law enforcement?

7. 442 U.S. 735 (1979).

8. 425 U.S. 435 (1976).

9. *Smith*, 442 U.S. at 736.

10. *Miller*, 425 U.S. at 436.

11. On the judicial front, see *United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (noting that in "the digital age," it may be "necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties"); *Klayman v. Obama*, 957 F. Supp. 2d 1,

results have been mixed. Although the effort to marginalize *Smith* and *Miller* certainly improves on the status quo, it also leaves unresolved—indeed, *unexamined*—the distinct privacy concerns that arise when intermediaries decide to aid the authorities voluntarily. Many of the practices that rightfully alarm scholars today—for example, the collection of bulk metadata—would still be alarming (perhaps even more so) if they were spearheaded by private actors, not at the behest of law enforcement, but with the purpose of *assisting* law enforcement. In today's world, that possibility is no dormant hypothetical. It is an increasingly prevalent state of affairs.[12]

In short, although existing commentary has focused—understandably—on the pitfalls of the third-party doctrine, the problem actually looms considerably larger. *Smith* and *Miller* stand for the proposition that when information is shared between parties with no preexisting trust relationship, the act of sharing carries no expectation of privacy. Many commentators have lodged their disagreement with this proposition. There is an important sense, however, in which the proposition is not just wrong; it is backward. When information is shared between parties with no preexisting trust relationship, it makes little sense to speak of trust being misplaced, because trust was not "placed" at all. The act of sharing therefore should carry even *more* protection than the misplaced trust rule would afford. In this sense, the abrogation of *Smith* and *Miller*—though certainly a welcome possibility—would not go far enough. To refurbish Fourth Amendment law for the digital age, it is not merely the third-party doctrine, but also the misplaced trust rule, that needs rethinking.

---

32 (D.D.C. 2013) (describing the surveillance ushered in by section 215 of the PATRIOT ACT as "so different from [the] simple pen register [in] *Smith*" and holding that "bulk telephony metadata collection and analysis [violates] a reasonable expectation of privacy"). *But see* ACLU v. Clapper, 959 F. Supp. 2d 724, 749–53 (S.D.N.Y. 2013), *vacated on other grounds*, 785 F.3d 787 (2d Cir. 2015) (holding, under *Smith*, that individuals do not have a reasonable expectation of privacy in telephony metadata). On the scholarly front, see Laura Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757, 865–71 (2014) (arguing that on the facts of *Smith*, reasonable suspicion—at the very least—was essentially established, setting the case entirely apart from applications today that extend its holding to bulk, suspicionless surveillance); 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, 976–77 (2007); Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 40 (2011) [hereinafter Henderson, *Timely Demise*] (describing the doctrine as, among other things, "fundamentally misguided"); Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1117–19 (2006); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 109–15 (2008); Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 619–21 (2011) (suggesting that technological change has rendered the third-party doctrine untenable). Although some of these critiques preexisted the digital age, technological change has only intensified their force. *See, e.g.*, Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 585 (2011) (noting that although "*Smith* and the Third-Party Doctrine were heavily criticized even before the Internet age, the drumbeat of criticism has [only] intensified"); *id.* at 585 n.26 (compiling further sources). *See generally* 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 (2002).

12. *See infra* notes 149–52 and accompanying text.

Against this backdrop, I propose a simple remedy: Fourth Amendment doctrine must abandon the pretense that all private actors are alike. The implication of *A*'s decision to share information with *B* should not be uniform across contexts. Rather, it should depend on what *type* of "third party" *B* is, on *B*'s role in the world vis-à-vis *A*. In many settings, it is perfectly acceptable—indeed, it serves an important public function—for *B* to help investigate *A*'s illicit activity. But there is also an important class of cases in which *B* is not a run-of-the-mill private actor, but rather an information fiduciary, beholden to *A*'s interests first and foremost.

I. THE DOCTRINAL STORY

When it comes to shared information, the familiar story is that Fourth Amendment doctrine toggles between two rules. First, some acts of disclosure simply extinguish one's expectation of privacy outright. I call this the "exposure" rule. If information has been exposed to the world, its investigation does not qualify, in the first instance, as a search, so the Fourth Amendment does not apply. Second, other acts of disclosure, although they do not eliminate one's expectation of privacy, do cause one to run the risk that *another* party—the counterparty to the disclosure—will betray the information to law enforcement. I refer to the latter as the "misplaced trust" rule.[13]

Rule	**By disclosing information to *B*, has *A* lost his expectation of privacy?**	**By disclosing information to *B*, has *A* run the risk that *B* will relay the information to law enforcement?**
Exposure (no protection)	Yes	Yes
Misplaced Trust (default)	No	Yes

13. There is one set of cases that is not easily explained by this scheme—cases in which the Court holds that no expectation of privacy exists in the specific type of evidence being searched for, even if the evidence has not been, in the usual sense, "exposed." The two examples that come to mind are dog sniffs and sting operations designed to uncover illicit activity in the home. *See, e.g.*, United States v. Place, 462 U.S. 696, 707 (1983) (explaining that dog sniffs are "sui generis," insofar as they precisely target contraband); Lewis v. United States, 385 U.S. 206, 211 (1966) ("[W]hen, as here, the home is converted into a commercial center to which outsiders are invited for purposes of transacting unlawful business, that business is entitled to no greater sanctity than if it were carried on in a store, a garage, a car, or on the street."). Because these cases are difficult to rationalize under *any* theory of privacy, I do not take it as a particularly bad sign that they clash with the scheme set forth here.

But the familiar story is incomplete. In fact, there is a third Fourth Amendment rule—a heightened tier of protection. Some acts of disclosure neither extinguish one's expectation of privacy in the shared information *nor* cause one to run the risk of a counterparty betraying the information to law enforcement. I refer to this as the "fiduciary" rule.

Rule	**By disclosing information to *B*, has *A* lost his expectation of privacy?**	**By disclosing information to *B*, has *A* run the risk that *B* will relay the information to law enforcement?**
Exposure (no protection)	Yes	Yes
Misplaced Trust (default)	No	Yes
Fiduciary (more protective)	No	No

To date, the fiduciary rule has surfaced in the Court's jurisprudence in two settings: medical care and hotels. In both settings, the same impetus is discernible—the misplaced trust rule seemed mismatched to the underlying relationship. It seemed wrong to the Court—for good reason—that constitutional privacy would be left to the mercy of doctors and hotel staff. The rest of this part explores each rule, and their interrelationship, at greater length.

A. Exposure

Exposure cases typically focus on the vantage point from which information can be ascertained. As the Court explained in the seminal case of *Katz v. United States*,[14] "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[15] This principle, repeated tirelessly since *Katz*,[16] supplies an intuitive anchor for Fourth Amendment doctrine. At root, the principle depends on the uncontroversial premise that information disclosed to the whole world carries no expectation of privacy—from which it follows that the act of viewing and recording such information does not qualify as a search.[17]

14. 389 U.S. 347 (1967).
15. *Id.* at 351.
16. *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 213 (1986).
17. Sherry Colb has traced the contours of this logic (and its shortcomings) with precision. *See generally* Colb, *supra* note 11.

The key question, of course, is what counts as exposing something "to the public." In response, the Court has offered an elaborate, if sometimes unconvincing, parade of answers. To begin with, something is exposed to the public if it is viewable from a public place.[18] Suppose Mary runs frantically through the town square, yelling about the details of a murder she recently committed. If a police officer, overhearing Mary, acts on the information (decides to follow Mary, to arrest Mary, and so on), plainly no search has occurred. The Fourth Amendment does not constrain the officer's ability to listen, from a public vantage point, to Mary's ravings. The same reasoning applies, moreover, if Mary is raving inside her home, but loudly enough that she can be heard from the sidewalk;[19] likewise, if Mary posts the ravings to her Facebook page (assuming it is a public page);[20] or if she transcribes the ravings in a notebook and then discards the notebook in a trash heap by the side of the road.[21]

What is true of a confession is also true of material evidence. Joe struts through the town square with a kilo of cocaine under his arm, and a police officer, viewing the drugs, arrests him. Clearly, no search has occurred. Nor would it have been a search for the police officer to watch Joe, in public, for many hours *before* Joe came into possession of the cocaine. Indeed, it doesn't matter how long the public surveillance of Joe had been ongoing; absent certain kinds of technological enhancement, the surveillance would never amount to a search.[22] Similarly, if Joe puts a kilo of cocaine on his coffee table and the table is viewable from the street, Joe cannot complain if police officers look through his window, see the drugs, and arrest him. Likewise, if Joe lives on a grand estate and the police enter the grounds—against Joe's wishes—and observe a kilo of cocaine on Joe's living room table while standing in the "fields" surrounding his home, no search has occurred.[23] Nor can Joe complain if he puts the kilo of cocaine in his backyard and the police identify it via aerial surveillance.[24]

---

18. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 31–32 (2001) (explaining that "ordinary visual surveillance of a home"—from a public vantage point—is not a Fourth Amendment search).

19. *See* Florida v. Jardines, 133 S. Ct. 1409, 1415 (2013) ("[L]aw enforcement officers need not 'shield their eyes' when passing by the home 'on public thoroughfares.'" (quoting *Ciraolo*, 476 U.S. at 213)).

20. *See, e.g.*, Chaney v. Fayette Cty. Pub. Sch. Dist., 977 F. Supp. 2d 1308 (N.D. Ga. 2013) (no reasonable expectation of privacy in material posted to a social networking website); United States v. Meregildo, 883 F. Supp. 2d 523 (S.D.N.Y. 2012) (same). For an excellent summary of the intersection of Fourth Amendment doctrine and social media, see Stephen E. Henderson, *Expectations of Privacy in Social Media*, 31 MISS. C. L. REV. 227 (2012).

21. *See* California v. Greenwood, 486 U.S. 35 (1986).

22. *See Kyllo*, 533 U.S. at 33–34 (explaining that "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology," and holding that doctrine must evolve to reflect this reality). Something like this is rather obviously at stake in the Court's recent holdings regarding GPS and smart phones. *See* Riley v. California, 134 S. Ct. 2473 (2014); United States v. Jones, 132 S. Ct. 945 (2012).

23. *See* United States v. Dunn, 480 U.S. 294 (1987); Oliver v. United States, 466 U.S. 170 (1984).

24. *See* Florida v. Riley, 488 U.S. 445 (1989); *Ciraolo*, 476 U.S. 207.

The same logic applies to the tracking of movements through public space—a mainstay of everyday law enforcement. Suppose the police suspect Bill of drug trafficking, so they watch Bill's movements to and from work every day, noting his stops. After a few weeks, the police patch together a pattern of Bill stopping at a known drug den after work, and on that basis, they secure a warrant to search his apartment. Bill would have no grounds to complain about such surveillance; he has no expectation of privacy in his public movements. Nor would Bill have any grounds to complain about the police tailing his movements by car, even if they do so by getting Bill to unwittingly equip his car with a tracking device.[25] To whatever extent technological enhancement would change these outcomes—a doctrinal question currently in flux, being negotiated against the backdrop of *United States v. Jones*[26]—it is clear that in the absence of technological enhancement, no Fourth Amendment claim would lie.

Some of these holdings may seem like unsound applications of the "exposure" principle. Who, after all, would think that activity carried out in a private backyard, shielded from neighbors by a tall fence, is exposed to the whole world simply because someone could, in theory, view it from the sky? And who would think the police, having entered private property in clear disregard of a "no trespassing" sign, have free reign to snoop around, as long as they stay sufficiently far away from the physical perimeter of one's home? The important point, however, is that even putting the virtues of these holdings to one side, their analytic underpinning is clear. The Court's logic focuses on whether the relevant information has been "exposed" to the world. When the answer is yes, no Fourth Amendment protection applies because the observational act does not amount, in the first instance, to a search.

Before moving on, there is a final pair of cases that qualify—rhetorically, at least—as applications of the exposure rule: *Smith* and *Miller*, which hold that sharing a dialed number with a phone company or sharing financial information with a bank eliminates one's expectation of privacy in the relevant information.[27] To reach this result, *Smith* and *Miller* conflate the act of disclosing information with the act of exposing information to public view, a conceptual jump that scholars and sitting judges have long maligned.[28] This is understandable—in the pantheon of modern Fourth

25. *See* United States v. Karo, 468 U.S. 705 (1984); United States v. Knotts, 460 U.S. 276 (1983).

26. 132 S. Ct. 945 (2012).

27. Smith v. Maryland, 442 U.S. 735, 736 (1979) (sharing a dialed number); United States v. Miller, 425 U.S. 435, 436 (1976) (sharing financial information); s*ee also* United States v. Payner, 447 U.S. 727, 732 (1980) (interpreting *Miller* to preclude defendant from challenging the search of his accountant's papers, on the grounds that, inter alia, the search yielded only financial information).

28. In addition to criticizing the Court's conflation of disclosure and exposure as a normative proposition, various commentators have also noted that, in practice, the Court has not had the courage of its own conviction. Like many extreme principles, the third-party doctrine would lead to some very uncomfortable results if extended to its logical limit. Instead of biting the bullet, the Court has continually found ways around applying the third-party doctrine in its strong form. *See, e.g.*, Stephen E. Henderson, *After* United States v.

Amendment law, *Smith* and *Miller* are the *only* times the Court has understood the disclosure of information to a specific counterparty as equivalent to broadcasting the information to the whole world.[29]

B. Misplaced Trust

This brings us to the second rule. Notwithstanding the Court's rather zealous language from *Smith* and *Miller*, it simply is not the case that "individual[s] ha[ve] no reasonable expectation of privacy in information voluntarily disclosed to third parties."[30] In fact, the default rule—famously enshrined in *Katz*, when the Court banned warrantless wiretapping—is just the opposite. Normally, when *A* shares information with *B*, *A does* retain her expectation of privacy in the information.[31] But *A* also runs the risk that *B*, now in possession of the information, will betray it to law enforcement. This is the sense in which, as the Court is fond of repeating, the Fourth Amendment is not a bulwark against misplaced trust; it provides no remedy

---

Jones, *After the Fourth Amendment Third Party Doctrine*, 14 N.C. J.L. & TECH. 431, 438 (2013) (arguing that, in the last twenty-five years, "there have certainly been cases which some of the Justices believed to be governed by the [third-party] doctrine," but "the doctrine has not fared well"); *id.* at 438–43 (exploring how the Court has departed from the third-party doctrine in no fewer than five prominent cases); *cf.* Strandburg, *supra* note 11, at 633–38 (arguing that, notwithstanding the sweeping language of *Smith* and *Miller*, the "aggressive" form of the third-party doctrine has almost never been faithfully applied).

29. This claim requires two caveats. First, the Supreme Court has held that some Fourth Amendment challenges are stillborn for want of "standing," because the police did not search the *defendant's* property; rather, the police searched another person's property, and that search ended up yielding evidence incriminating the defendant. *See, e.g.*, Rawlings v. Kentucky, 448 U.S. 98, 105–06 (1980) (holding that defendant lacked standing to challenge the search of a third-party's handbag). One could read these "Fourth Amendment standing" cases as standing for the proposition that transmitting certain types of material evidence to a third-party—for example, as in *Rawlings*, a bag of drugs for storage in a third-party's purse—is equivalent to exposing evidence to the whole world. But even so, the Fourth Amendment standing cases apply only to material evidence, not shared information. *See* Rakas v. Illinois, 439 U.S. 128 (1978) (stating that passengers lacked standing to challenge the search of a car when they had no possessory interest in either the car or the evidence seized from the car); Minnesota v. Carter, 525 U.S. 83 (1998) (finding defendant lacked standing to challenge the search of a home where he was working as a drug packager). Second, some lower courts have picked up where the Supreme Court left off in *Smith* and *Miller* and *extended* the reach of the third-party doctrine. *See, e.g.*, United States v. Caraballo, 963 F. Supp. 2d 341, 361 (D. Vt. 2013) (holding that cell phone users have no reasonable expectation of privacy in cell-site location data). However, *Smith* and *Miller* (and *Payner*, insofar as it echoes *Miller*) are the only times the Supreme Court has spoken on the issue.

30. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (summarizing the received view of *Smith* and *Miller*); *see Smith*, 442 U.S. at 743–44 ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

31. Traditionally, the wedge dividing *Smith* from *Katz*—or, one could say, keeping *Smith* quarantined—is the distinction between "content" and "noncontent" information. The pitfalls of this distinction, particularly in an age of sophisticated data analytics, are well known. *See infra* note 121 and accompanying text. Similarly well known is Orin Kerr's defense of the distinction on technological neutrality grounds. *See* Orin S. Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561, 581 (2009).

for "a wrongdoer's [mistaken] belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."[32]

Mail correspondence is the paradigm case. In one of its earliest Fourth Amendment holdings, *Ex Parte Jackson*,[33] the Court canonically held that the government may not engage in suspicionless searches of private letters because "[l]etters and sealed packages . . . are as fully guarded from examination and inspection" when sent through the postal service "as if they were retained by the parties forwarding them in their own domiciles."[34] In some sense, *Katz* and its progeny are, at their core, little more than an affirmative extrapolation of the principle in *Ex Parte Jackson*.

The essence of *Katz* (and *Ex Parte Jackson*) is twofold. First, one's expectation of privacy in the contents of a phone call—or, equally, a letter or an email—survive disclosure. Otherwise, corresponding with another person would amount to an ipso facto waiver of all restraints on law enforcement surveillance of private communication. At the same time, however, corresponding with another person *does* expose one to the risk of betrayal. No one would construe *Ex Parte Jackson*—and as far as I know, no one *has* construed *Ex Parte Jackson*—to limit the ability of a letter's recipient to forward its contents to law enforcement, just as no one construes *Katz* to limit the ability of the person on the other line from recording the call or consenting to a wiretap.[35]

Framing the issue this way underscores the analytic harmony between *Katz* and the confidential informant (CI) cases, which hold that *A*, by sharing information with *B*, runs the risk that *B* is an undercover police agent.[36] Although *Katz* is often described as the "lodestar" of Fourth Amendment protection[37] while the CI cases are described as the opposite,[38] a common premise unites them. Namely, by disclosing something to *B*, *A* puts herself at *B*'s mercy, exposed to the danger that *B* may prove to be a "false friend."[39] Even for commentators that decry the CI cases as wrongly decided—and there are plenty[40]—this premise is not in dispute. For critics,

32. Hoffa v. United States, 385 U.S. 293, 302 (1966).

33. 96 U.S. 727 (1877).

34. *Id.* at 733.

35. *See, e.g.*, United States v. Karo, 468 U.S. 705, 726 (1984) (O'Connor, J., concurring) ("[T]wo people who speak face to face in a private place or on a private telephone line both may share an expectation that the conversation will remain private, but either may give effective consent to a wiretap or other electronic surveillance. One might say that the telephone line, or simply the space that separates two persons in conversation, is their jointly owned 'container.' Each has standing to challenge the use as evidence of the fruits of an unauthorized search of that 'container,' but either may also give effective consent to the search." (citations omitted)).

36. *See* United States v. White, 401 U.S. 745 (1971); *Hoffa*, 385 U.S. 293; Lewis v. United States, 385 U.S. 206 (1966).

37. Smith v. Maryland, 442 U.S. 735, 739 (1979).

38. *See supra* note 11.

39. *See, e.g.*, Donald L. Doernberg, *"Can You Hear Me Now?": Expectations of Privacy, False Friends, and the Perils of Speaking Under the Supreme Court's Fourth Amendment Jurisprudence*, 39 IND. L. REV. 253 (2006).

40. *See, e.g.*, Christopher Slobogin, *The World Without a Fourth Amendment*, 39 UCLA L. REV. 1, 103–06 (1991); James J. Tomkovicz, *Beyond Secrecy for Secrecy's Sake: Toward*

the point is simply that the danger of *B turning out* to be a "false friend" does not entail the danger that *B already is* a "false friend."[41] But controversy about the second proposition in no way disturbs the first. Among scholars who would do away with the CI cases, none would do away with "false friend" logic as such—which makes sense because, at some level, the "false friend" logic simply restates the misplaced trust rule.

Finally, the misplaced trust rule also applies to spaces, including homes.[42] By inviting someone into my home, I don't lose my expectation of privacy; I still have the right to exclude law enforcement from entry (absent a warrant or probable cause). But I *do* run the risk that an invited guest—or, likewise, a roommate, spouse, or family member—will open my home to law enforcement. This is true in two senses. First, I run the risk that another person will locate incriminating evidence in my home, physically remove it, and pass it on to the police.[43] Suppose Laura's boyfriend finds cocaine under their mattress and takes it to the local precinct, leading to her arrest. On these facts, Laura has no constitutional recourse.[44] The second sense in which the misplaced trust rule applies to homes is that if *A* and *B* cohabitate, *A* runs the risk of *B* consenting to search by law enforcement (and vice versa). In *United States v. Matlock*,[45] the Court established, in no uncertain terms, that one cotenant may consent to a search on behalf of all cotenants, even if there is evidence that another

an Expanded Vision of the Fourth Amendment Privacy Province, 36 HASTINGS L.J. 645, 728 (1985).

41. In this sense, to bear their conceptual burden, critics of the CI cases must distinguish between (1) *B* receiving information from *A*, and then deciding to tell law enforcement, and (2) *B* deciding, in the first instance, that she wishes to incriminate *A* and then eliciting information from *A* with the goal of assisting law enforcement. Although this distinction is certainly conceivable, it also gives rise to a rather serious line-drawing problem. In practice, there are many sympathetic cases—cases where I suspect most people would want *B* to remain free to assist the police without constitutional hindrance—where *B* will make up her mind to betray *A before* soliciting the incriminating information or material evidence. For example, what if *A* is *B*'s abusive spouse, and *B*, fearing for her own safety, decides to build a case against *A*? To be persuasive, criticism of the CI cases must distinguish a hypothetical like this from the use of police informants—a taller order than it might first appear.

42. That being said, the application of the misplaced trust rule to spaces is not *limited* to homes. Given the hallowed status of the home in Fourth Amendment law, however, other examples follow, as a normative matter, essentially a fortiori. *See, e.g.*, O'Conner v. Ortega, 480 U.S. 709, 717 (1987) (holding that employees have an expectation of privacy in their offices, but that "in many cases offices are continually entered by fellow employees and other visitors during the workday for conferences, consultations, and other work-related visits," which carries certain risks).

43. *See* Coolidge v. New Hampshire, 403 U.S. 443, 487–89 (1971) (holding that it was a private search—outside the bounds of the Fourth Amendment—when a woman retrieved incriminating evidence about her husband from their home and gave the evidence to the police); *see also* United States v. Bowers, 594 F.3d 522, 525–27 (6th Cir. 2010) (holding that it was a purely private search when defendant's roommate and her boyfriend entered defendant's room, removed a photo album, and gave it to the police).

44. Indeed, if Laura peruses the case law, she may be chastened to learn that courts express sympathy not for the party in her position, but for the party in her boyfriend's position—the innocent figure who brings wrongdoing to light. *See Bowers*, 594 F.3d at 525–27.

45. 415 U.S. 164 (1974).

cotenant, absent when the police arrived on the scene, would have objected to the search.[46] Later cases have affirmed this principle numerous times over.[47]

C. Expanding the Horizon of Protection

And so the traditional story ends, with the idea that another private actor's decision to cooperate with law enforcement is, across contexts, the outer bound of constitutional protection and that no matter how robustly the Fourth Amendment might protect us from *police* activity, it protects us not at all from the activity of private persons. Taking the Court's words at face value, one could be forgiven for seeing this idea as an irreducible axiom of Fourth Amendment law. The reality is more complicated. The misplaced trust rule certainly operates as a constitutional default. But ultimately, it is only that. Like any default rule, it comes under strain in exceptional cases. The question is what makes the exceptional cases exceptional. I believe the answer centers on relationships.

1. Doctors

In 1988, doctors at a public hospital in Charleston, South Carolina, instituted a program to screen the urine of pregnant women for drug use and, if drug use was found, to transmit the incriminating samples to law enforcement.[48] One of the women subject to this program was Crystal Ferguson. Along with a group of other similarly situated plaintiffs, she brought a constitutional challenge on the grounds that the collection and testing of the patients' urine violated their Fourth Amendment rights.[49] The Court held, in *Ferguson v. City of Charleston*,[50] that it did because (1) the hospital's program involved suspicionless searches, and (2) unlike other drug testing cases—where the Court had permitted suspicionless searches because of the "special needs" they serve—law enforcement was the

46. *See id.* at 169–72.

47. *See, e.g.*, Illinois v. Rodriguez, 497 U.S. 177, 186–87 (1990) (extending *Matlock* to situations where third party is not actually a cotenant and only has apparent shared authority over the residence). *Compare* Georgia v. Randolph, 547 U.S. 103, 114–23 (2006) (holding that if both cotenants are present, and one invokes his Fourth Amendment rights, that invocation trumps the other's consent), *with* Fernandez v. California, 134 S. Ct. 1126, 1137 (2014) (holding that the consent of cotenant sufficed to justify the search after the other tenant (1) had invoked his *Randolph* rights, but (2) had been removed from the premises). Furthermore, the same logic also works in reverse, as applied to *guests themselves*, rather than people who invite guests into their homes. Just as *A* does not lose all expectation of privacy in his home by inviting *B* over, so, too, *B* does not lose all expectation of privacy by taking *A*'s invitation. Rather, both parties, *A* and *B*, risk "betrayal" (i.e., consent to search by law enforcement or exposure of contraband) by the other. *See, e.g.*, Minnesota v. Olson, 495 U.S. 91, 98–99 (1990).

48. Ferguson v. City of Charleston, 532 U.S. 67, 70 (2001).

49. *See id.* at 72–73.

50. 532 U.S. 67 (2001).

ultimate purpose.[51] Thus, the program did not withstand Fourth Amendment scrutiny.[52]

I regard *Ferguson* as unassailably correct. The interesting question is *why*. The opinion for the Court sweeps past—but, curiously enough, never fully answers—the threshold question in the case: Given the misplaced trust rule, why does the Fourth Amendment even come into play? What aspect of the doctors' decision to betray their patients' trust amounts to a law enforcement "search"? The only explanation offered in Justice Stevens's opinion is that "[b]ecause [the South Carolina hospital] is a state hospital, the members of its staff are government actors, subject to the strictures of the Fourth Amendment."[53] And this explanation has some glancing appeal. After all, the Fourth Amendment certainly embeds some version of the state action requirement; as a general matter, "private searches" meet with no constitutional scrutiny, even if the very same activity, carried out by law enforcement, would undeniably constitute a search.[54]

But the majority's "state hospital" rationale suffers a fundamental defect. Government actors are only "subject to the strictures of the Fourth Amendment," in the way the majority suggests, to the extent their actions are coercive, either because the search in question is compelled by law or because failure to submit to the search incurs legal consequences. This is true of all the special needs cases invoked by Justice Stevens to support the "state hospital" rationale.[55] For example, in *Skinner v. Railway Labor Executives' Ass'n*,[56] train conductors brought a Fourth Amendment challenge to a federal statute requiring drug testing for railway employees.[57] It was undisputed (and indisputable) that the testing constituted a search;[58] it was mandatory,[59] and it was plainly an invasion of privacy. The question

51. *Id.* at 84.

52. *Id.* at 84–85.

53. *Id.* at 76.

54. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 113 (1984) (declaring that the Fourth Amendment is "wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official'" (quoting Walter v. United States, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting))).

55. *Ferguson*, 532 U.S. at 76; *see* Chandler v. Miller, 520 U.S. 305, 309–10 (1997) (urine test required as a condition of running for public office); Verona Sch. Dist. 47J v. Acton, 515 U.S. 646, 648–49 (1995) (student urine testing required by school district); Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 659–63 (1989) (urine testing as a condition of employment); New Jersey v. T.L.O., 469 U.S. 325, 335–37 (1985) (search of student's effects required by schools officials).

56. 489 U.S. 602 (1989). For background on the way the Court reasons through mandatory urine testing—and other mandatory "special needs" searches—see *Chandler*, 520 U.S. 305.

57. *Skinner*, 489 U.S. at 612.

58. *See id.* at 618.

59. This is true even in the case of the noncompulsory drug testing, which the Court held to be a *constructive* law enforcement search. *Id.* at 615–16. Although *Skinner* concerned both mandatory and "optional" drug testing on the part of private companies, the Court explicitly rejected the proposition that the searches were not instigated by the government. *Id.* at 614–15. In other words, it saw the testing as coerced by the state de facto rather than

before the Court was whether the "special need" of public safety—in light of the heightened danger that arises from having railway conductors operating trains under the influence of drugs—*justified* the invasion of privacy.[60] (And the answer was yes.[61])

In *Ferguson*, by contrast, the initial act of disclosure—from patient to doctor—was not mandatory.[62] To be sure, because the disclosure was motivated by a desire for medical care, it would be difficult to call the act purely voluntary. The patients needed prenatal care, and to obtain it, urine testing was necessary. What were the patients to do? Presumably none of them anticipated (or desired) the transmission of incriminating medical evidence to law enforcement.[63] But the fact remains that no law required the patients to entrust urine to their doctors. They chose to do so—and their trust ended up being misplaced. Under existing doctrine, that should be the end of the matter.

To be clear, I regard this result as an argument *against* the misplaced trust rule—hence the motivation for this Article. But there can be little doubt that on a faithful application of the rule, a patient's decision to give her doctor a urine sample should end the inquiry. The doctor should be free—as any party is free—to transmit incriminating evidence to law enforcement.[64] A patient no more can object, on Fourth Amendment grounds, to a doctor furnishing law enforcement with a urine sample than I can object to my sister furnishing law enforcement with information about a crime I committed, in the event that I (mistakenly) confess the details to her. For purposes of the misplaced trust rule, what matters is not whether the entrusted party is a state actor or a private actor; what matters is that

---

de jure—but the subtleties of this distinction are beside the point, because in *Ferguson*, the testing was not coerced by the state in *either* sense. If it was coerced, it was so *by the doctors*, which might be said, of course, to underscore a problem with the private search doctrine. But it does not make *Ferguson* and *Skinner* analogous.

60. *Id.* at 618–20.

61. *Id.* at 621.

62. As it turns out, even if the initial disclosure was *not* voluntary—as the Fourth Circuit concluded on remand—this still cannot rescue the majority's logic. *See* Ferguson v. City of Charleston, 308 F.3d 380, 402–03 (4th Cir. 2002) (explaining the difficulties associated with treating disclosures to doctors as "voluntary"). What makes it a search is its practical involuntariness—an idea I explore in Part II below—not the fact that the counterparty to the (practically involuntary) transmission was a public actor. Put otherwise, it would be just as practically involuntary, and therefore just as much a search, if the doctors were private doctors.

63. In this respect, the Fourth Circuit's opinion on remand confirms what common sense makes inescapable: the patients were not consenting to a law enforcement search when they turned over their urine for medical purposes. *See id.*

64. To be clear, I mean that doctors "should be free" to transmit incriminating evidence to law enforcement under the logic of the private search rule, not that doctors ought to be free, in a normative sense, to transmit incriminating evidence to law enforcement. In fact, in many jurisdictions doctors have obligations of confidentiality that strictly limit what they can do with patient information. *See, e.g.*, Alsip v. Johnson City Med. Ctr., 197 S.W.3d 722, 725–28 (Tenn. 2006) (explaining doctors' confidentiality obligations under Tennessee law and canvassing other jurisdictions with equivalent rules). This is rightly so: expectations of confidence are what facilitate candid interaction with doctors and, ultimately, what allow for optimal medical care.

information has been entrusted *voluntarily*. Once voluntary entrustment occurs, the entrusting party (here, the patient) runs the risk of betrayal by the entrusted party (here, the doctor)—whether or not the entrusted party is a state actor.

An example will shore up the point. Suppose a drug dealer is waiting in line at the DMV with a paper bag full of illicit pills in his coat pocket. After receiving a call from a customer who lives across the street, the drug dealer gets an idea. He thinks: *I bet I could run across the street and make this delivery before my number is called.* Then the drug dealer gets another idea: he will only take a few pills across the street, in case the deal is a setup. So he reaches into the bag, puts some pills in his pocket, and asks the person sitting next to him—another private citizen, for all he knows—to watch the paper bag for him. The neighbor agrees, and the drug dealer goes across the street to make his delivery.

In this example, if the neighbor becomes suspicious and rustles through the bag to discover the pills, there is no dispute that he could turn the pills over to law enforcement (and provide testimony about the incident) without violating—indeed, without even *triggering*—the drug dealer's Fourth Amendment rights. By leaving the bag with his neighbor, not only has the drug dealer run the risk that the neighbor will become curious and decide to betray his trust, but, under *Hoffa v. United States*[65] and *United States v. White*,[66] he has also run the risk that the neighbor is already working as an informant. Indeed, he has even run the risk that (unbeknownst to the drug dealer) the police have orchestrated the entire scene to catch him red-handed when he hands over the bag. All of this would fall clearly within the bounds of Fourth Amendment law.

But now adjust the hypothetical slightly: instead of giving the bag to his neighbor, the drug dealer goes up to the DMV counter and asks a clerk to hold on to the bag. The clerk agrees. Does this version of the hypothetical yield a different result because the DMV clerk, unlike the neighbor, is a state actor? Does the Fourth Amendment prohibit the clerk from helping law enforcement in a manner that it does *not* prohibit the neighbor from doing so? Or, asked the other way around, has the drug dealer run any *less* risk of misplaced trust simply because the clerk happens to work for the state? Hewing to its own logic, the *Ferguson* majority would have to answer all these questions "yes." But that seems amiss. Under existing doctrine, the important variable is the fact of entrustment, not the identity of the entrusted party. If entrustment occurred, the Fourth Amendment has nothing to say when it proves ill-advised, whether or not the entrusted party is a state actor.[67]

---

65. 385 U.S. 293 (1966).

66. 401 U.S. 745 (1971).

67. It may be that if the entrusted party happens to be a *police officer*, the analysis would proceed differently. Query: If a drug dealer walks into a police station and leaves a bag of drugs in the care of the supervising officer, does the Fourth Amendment constrain the officer's ability to open the bag? Perhaps. But even so, what is at stake is not the public-private divide as such; it is the distinction between law enforcement and *all* other actors, public or private. The reasoning in *Ferguson* still falters.

Ultimately, then, the rationale offered by the *Ferguson* majority to justify subjecting the urine screening program to constitutional scrutiny—that the conduct occurred "[at] a state hospital"[68]—cannot shoulder its doctrinal burden. Why, given the misplaced trust rule, should the transmission of incriminating evidence from doctors to law enforcement qualify as a search *at all*, regardless of the "special need" behind it? The opinion for the Court begs this question in lieu of resolving it,[69] which is no doubt why Justice Scalia, dissenting in *Ferguson*, expressed such virulent dismay with Justice Stevens and the majority. In Justice Scalia's words:

> Until today, we have *never* held—or even suggested—that material which a person voluntarily entrusts to someone else cannot be given by that person to the police, and used for whatever evidence it may contain. Without so much as discussing the point, the Court today opens a hole in our Fourth Amendment jurisprudence.[70]

Justice Scalia is right.[71] Normally, once *A* shares incriminating evidence with *B*, *A* can raise no objection if *B* decides to share the evidence with law enforcement.[72] *Ferguson* departs from this principle. And in doing so, it

---

68. Ferguson v. City of Charleston, 532 U.S. 67, 76 (2001).

69. Not surprisingly, this has been replicated in lower court applications of *Ferguson*. *See, e.g.*, Nicholas v. Goord, 430 F.3d 652, 663 (2d Cir. 2005) ("We thus read . . . *Ferguson* to call for the application of the special-needs test *in cases involving suspicionless searches* . . . ." (emphasis added)); Padgett v. Donald, 401 F.3d 1273, 1279 (11th Cir. 2005) ("*Ferguson* . . . struck down suspicionless searches because they vindicated no special need distinguishable from general law enforcement."). Indeed, I was able to locate only *one* dissent in *one* case—combing through all of the federal appellate jurisprudence—that indicates an appreciation for *Ferguson*'s more radical implications. *See* Kerns v. Bader, 663 F.3d 1173, 1200–01 (10th Cir. 2011) (Holloway, J., dissenting) (arguing that *Ferguson* not only vindicates patients' expectations of privacy in personal medical evidence but also reaffirms the "long ago established" proposition that "the police cannot breach one's constitutional rights simply by asking another person to do it for them"—that doctors may not furnish the police with material that the police, absent probable cause, couldn't seize on their own).

70. *Ferguson*, 532 U.S. at 95 (Scalia, J., dissenting).

71. Well, to be picky about it, Scalia's use of the word "never," though technically true, is a bit misleading. He is right that no other Supreme Court case supports the proposition that material evidence voluntarily given to a third party cannot be shared subsequently with law enforcement. But zoom out one click—make the point about incriminating evidence *in general*, not material evidence in particular—and the hotel cases discussed below are similar to *Ferguson*. *See infra* Part I.C.2.

72. United States v. Miller, 425 U.S. 435, 443 (1976); United States v. White, 401 U.S. 745, 749 (1971) ("[H]owever strongly a defendant may trust an apparent colleague, his expectations in this respect are not protected by the Fourth Amendment when it turns out that the colleague is a government agent regularly communicating with the authorities."); Hoffa v. United States, 385 U.S. 293, 302 (1966) ("[T]he Fourth Amendment [does not protect] a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."). As Justice Scalia (correctly) notes, "The *Hoffa* line of cases . . . does not distinguish between operations meant to catch a criminal in the act, and those meant only to gather evidence of prior wrongdoing," as was the case in *Ferguson*, 532 U.S. at 94 (Scalia, J., dissenting). For a deft elaboration of this point, see Colb, *supra* note 11, at 182 (validating Scalia's analytic point the same way I am validating it here—by noting the sense in which *Ferguson* departs from the premise that "police collection of what has been surrendered to a third party . . . is not a Fourth Amendment search"); *id.* at 181–84

runs contrary to what is often described, in other cases, as an immutable first principle of Fourth Amendment law.[73]

Much as I agree, however, with Justice Scalia's *analytic* point, I cannot sign on to his conclusion that no search occurred. The normative intuition underlying the majority opinion in *Ferguson* seems to me undeniably right—so right, in fact, that it verges on self-evident, which may help to explain why Justice Stevens felt no compulsion to fully defend his rationale. Doctors should not be allowed to betray the trust of their patients. Full stop. Which is to say, something about the nature of the relationship between doctors and patients creates an exception to the misplaced trust rule. Under normal circumstances, if *A* shares evidence with *B*, *B* is free to relay the evidence to law enforcement. But if *B* is a doctor, the misplaced trust rule no longer applies.

Because the *Ferguson* majority was able to wave off this problem by invoking the public status of the hospital, it made no effort to reconcile its holding with other instantiations of the misplaced trust rule. The CI cases make one, and only one, appearance in *Ferguson*—in Justice Scalia's dissent.[74] But make no mistake: *Ferguson* runs directly into this line of cases.[75] At some level, in fact, it runs into *Katz* itself. For if the logic of

---

(exploring the radical effect that *Ferguson*'s logic, extended to its limits, has for Fourth Amendment privacy).

73. Although the majority tries to parry this argument, its reasoning withers under scrutiny. According to the majority,

> The dissent . . . mischaracterizes our opinion as holding that "material which a person voluntarily entrusts to someone else cannot be given by that person to the police, and used for whatever evidence it may contain." But, as we have noted elsewhere, given the posture of the case, we must assume for purposes of decision that the patients did *not* consent to the searches, and we leave the question of consent for the Court of Appeals to determine.

Ferguson, 532 U.S. at 85 n.24 (citation omitted). This rejoinder is confused. It conflates consent to search by law enforcement with the entirely distinct question of whether the initial transmission of evidence—to a party *other than* law enforcement—was consensual. The *Ferguson* majority is correct that its opinion makes no pronouncement, one way or the other, on the first question. Justice Scalia's point, however, is not that the patients consented to search by law enforcement (though, of course, he may also believe that). His point is that the patients consensually gave urine samples to their doctors, which means—according to Scalia—that the patients assumed the risk that the doctors would betray their trust. If so, they can raise no Fourth Amendment grievance, *not* because they "consented to the searches," as the majority claims, but because no search occurred.

By analogy, the difference here is between (1) telling a police officer, "You may search my car," which results in the officer finding a bag of cocaine, and (2) having a mechanic stumble on a bag of cocaine in your car, which he takes and gives to the police. In the first example, you consented to search—a search occurred, but it was justified. In the second example, *no* search occurred. As long as the mechanic is not an agent of law enforcement, he may dispose of the incriminating evidence as he sees fit—the Fourth Amendment does not even enter the equation.

74. *See id.* at 94–95 (Scalia, J., dissenting).

75. That *Ferguson* did not formally reach the "search" question is sometimes invoked to explain the case away. These efforts find themselves in the analytically unfortunate position of citing the fact that *Ferguson* does not address the threshold search issue as evidence that a search did not occur. This is manifestly backward. *See, e.g.*, *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things, No. BR 14-01, 2014 WL 5463097, at *7 n.9 (FISA Ct. Mar. 20, 2014).

Ferguson applied to phone calls, the result would be that not only are police prohibited from tapping phones, but also that the party on the other line—the party in the position analogous to a doctor—is prohibited from disclosing the contents of the call *to* the police. But that, of course, is not the constitutional rule we have; nor, for reasons explained more fully below, is it the constitutional rule we want.

Ultimately, the point is not that *Ferguson* upends *Katz*. On the contrary, *Ferguson* and *Katz* coexist—and should continue to coexist—happily. The point is that their coexistence lodges a challenge to the familiar doctrinal story. Either (1) *Ferguson* is wrongly decided, or (2) the axiom that the Fourth Amendment does not protect misplaced trust is, in fact, no axiom at all—it is simply a default rule, subject to exceptions. And one of those exceptions is the doctor-patient relationship.

2. Hotels

Now for the second exception—hotels. In two cases, the Court has held definitively that hotel managers may not grant police access to a guest's premises, even if the hotel manager *himself* has permission to enter those premises.[76] The first case is *United States v. Jeffers*.[77] There, police acquired a key to a hotel guest's room from the assistant manager and proceeded to enter the room without obtaining consent from anyone; neither the defendant nor his aunt (who was renting the room and with whom the defendant was staying at the time) was present when the police entered.[78] Inside the room, the police found a bevy of narcotics evidence.[79] When the search was challenged, the Government conceded that their actions were unlawful as against the defendant's aunt.[80] But the Government argued, nevertheless, that its actions were not unlawful as to the defendant because

76. There is a third case in this constellation, *Chapman v. United States*, 365 U.S. 610 (1961), presenting the identical issue except with regard to a landlord, not a hotel manager. Because hotel managers offer a closer analogy to doctors—and because, for the purposes of constitutional privacy, what is true of a temporary residence like a hotel room is surely true, a fortiori, of a permanent residence like an apartment—I will summarize *Chapman* only briefly here. The police obtained permission from a tenant's landlord to enter the tenant's apartment. *Id.* at 612. When the tenant moved to suppress evidence procured during the apartment's search, the Government argued that the landlord had consented to it, effectively waiving the tenant's Fourth Amendment rights. *See id.* at 616.

The Court rejected this argument, citing two rationales. First, the Court could find no case under the property laws and landlord-tenant laws of the relevant jurisdiction (in this case, Georgia) authorizing landlords to enter a tenant's premises merely because they suspect that criminal activity might be going on. *Id.* What a landlord was not authorized to do himself, the Court reasoned, surely he could not authorize *another* person to do. *Id.*

Second, the Court concluded that in fashioning the "procedural protections accorded to those charged with crime," constitutional law "ought not to bow" to "the body of private property law which, more than almost any other branch of law, has been shaped by distinctions whose validity is largely historical." *Id.* at 617 (quoting Jones v. United States, 362 U.S. 257, 266–67 (1960)).

77. 342 U.S. 48 (1951).

78. *Id.* at 50.

79. *Id.*

80. *Id.* at 51.

he was not the one formally renting the room.[81] The Court disagreed. It reasoned that what was unlawful (by the Government's own admission) as applied to one occupant was also unlawful as applied to the other,[82] so the evidence was tossed.[83]

The second case—a more lucrative doctrinal resource—is *Stoner v. California*.[84] There, as in *Jeffers*, police obtained consent (and a key) from a hotel manager to search an occupant's room, where they located evidence of criminal activity.[85] The question presented was whether, as in *Jeffers*, it was unconstitutional for the police to enter the defendant's hotel room simply on the basis of another party's consent.[86] The Court agreed, describing the constitutional right in question as one that

> only the petitioner could waive by word or deed, either directly or through an agent . . . [and] there is nothing in the record to indicate that the police had any basis whatsoever to believe that the night clerk had been authorized by the petitioner to permit the police to search [his] room.[87]

In other words, the defendant's acquiescence to the hotel's policy requiring him to "place[] [his key] in the mail box each time [he] left the hotel"[88]—thereby exposing potentially sensitive information to the hotel staff—did not expose him to the risk of the staff's cooperation with law enforcement.

It may seem odd to invoke these cases alongside *Ferguson*. Where the latter seems to pick out a socially distinctive relationship for elevated protection, the hotel cases—one might argue—achieve nothing so luminous; they seem like humdrum applications of agency law, transplanted to the Fourth Amendment setting. By granting someone else access to your temporary dwelling space, you do not necessarily run the risk that he, in turn, will grant *someone else* access to that space. What great triumph is there in that?

There are two responses to this question, and they interpenetrate. The first response is that the "agency principles" on exhibit in *Jeffers* and *Stoner* are not as humdrum as initial appearances might imply. After all, the Court sees the agency question quite differently when it is not a hotel manager, but instead a cotenant or a guest, who authorizes the police to enter a residence. In *United States v. Matlock*, the Court made clear that when someone with shared authority over the premises invites the police in, no Fourth Amendment violation occurs.[89] And in *Illinois v. Rodriguez*,[90] the

81. *Id.* at 52.
82. *Id.* at 52–53.
83. *Id.* at 54.
84. 376 U.S. 483 (1964).
85. *Id.* at 485–86.
86. *Id.* at 484.
87. *Id.* at 489.
88. *Id.* at 485.
89. United States v. Matlock, 415 U.S. 164, 168–69 (1974) (finding consent by cotenant to enter apartment justified law enforcement search). *Compare* Georgia v. Randolph, 547 U.S. 103, 115 (2006) (holding that if both cotenants are present, and one invokes his Fourth Amendment rights, that invocation trumps the other's consent), *with* Fernandez v. California, 134 S. Ct. 1126, 1130 (2014) (holding that consent of cotenant sufficed to justify search after

Court extended this core principle—and outcome—to situations where someone only *appears* to have shared authority.[91] Whether someone else's authority over my premises is actual or merely apparent, I run the risk that he or she will consent to entry by law enforcement.

The scope of the latter principle bears emphasizing. In light of the "misplaced trust" principle, it is of little surprise that someone with actual shared authority over premises may consent to entry by law enforcement. For the reasons set forth above, space, like information, is something that can be entrusted: if *A* invites *B* into her home, and all the more so if *A* decides to cohabitate with *B*, *A* runs the risk of *B* betraying their residence (so to speak) to the police.

But what about apparent authority? It is hard to see why the "misplaced trust" principle would authorize someone with the mere *appearance* of authority to consent to entry by law enforcement. No actual "entrustment" occurred. So it strains plausibility to say that the tenant's trust, which had not been "placed" in the first instance, had been *mis*placed. Furthermore, the "consent by apparent authority" rule is difficult to square with *Stoner*, which—as the defendant in *Rodriguez* pointed out—explicitly held that "the rights protected by the Fourth Amendment are not to be eroded . . . by unrealistic doctrines of 'apparent authority.'"[92]

Appreciating this difficulty, Justice Scalia's opinion in *Rodriguez* addressed the case's seeming tension with *Stoner* head on. In Justice Scalia's view, the *Stoner* opinion—with its high-flying rhetoric about apparent authority—was ambiguous between two views.[93] First, the *Stoner* Court might have meant that it would *always* be unrealistic to let apparent authority "erode" Fourth Amendment protection; it might have been drawing a categorical line.[94] Second, the *Stoner* Court might have been saying that it was unrealistic, on the specific facts of *Stoner*, to conclude that the hotel manager actually *had* apparent authority.[95] Justice Scalia—and a majority of the Court—favored the latter interpretation.

On the *Rodriguez* Court's reading of *Stoner*, then, the latter stands for the proposition that "the police could not rely upon the obtained consent because they knew it came from a hotel clerk, knew that the room was rented and exclusively occupied by the defendant, and could not reasonably have believed that the [hotel manager] had general access to or control over the [room]."[96] In this light, even if *Jeffers* and *Stoner* are about applying agency law principles to the Fourth Amendment setting, the *way* they do so still sheds light on the conceptual architecture of constitutional privacy. They underscore the importance of relationships, the difference between

---

the other tenant (1) had invoked his *Randolph* rights, but (2) had been removed from the premises).

90. 497 U.S. 177 (1990).
91. *See id.* at 186.
92. *Stoner*, 376 U.S. at 488.
93. *See Rodriguez*, 497 U.S. at 187–89.
94. *See id.* at 187.
95. *See id.* at 186–88.
96. *Id.* at 188.

granting an intimate (a spouse, a friend, or a family member) access to one's private space, as opposed to granting a hotel manager the same.

But *Jeffers* and *Stoner* also invite a more expansive reading. Suppose that, in *Stoner*, the hotel manager did not simply show the police to the door and (literally) turn the key. Instead, when the police arrived, the hotel manager said: "I'll tell you what—how about, instead of having me let you into the room, *I'll* go in, see what I can find, and bring it out for you."[97] Would the result be different? One could, of course, argue that the police in this hypothetical instigated the hotel manager's activity, rendering him a de facto agent of law enforcement and bringing the search back into the Fourth Amendment's sweep. But this route, in addition to straining existing case law,[98] also sells short the larger point. Namely, it seems odd, given the *Stoner* Court's clear determination that the hotel manager could not let the police in, to conclude that the hotel manager would be permitted to simply go in to the room and, say, empty all of its contents into the hall. Suppose, for example, that the manager, having seen a report on the local news about a recent robbery, took it upon himself to search through every hotel room for evidence of the crime, and when the police arrive, the hotel manager already has the incriminating evidence waiting for them. Would *that* be permissible?

To be sure, there is no logical contradiction between (1) the idea that the police may not enter a hotel room on consent of the hotel manager, and (2) the idea that the hotel manager may enter a hotel room *himself*, and relay whatever he finds there to law enforcement. The absence of a logical contradiction is what makes the reading "expansive." But the more expansive reading also strikes me as the far more persuasive one—for it seems quite implausible that *Stoner* would come down, ultimately, to the *way* the hotel manager betrayed the confidence of his guest, as opposed to the fact of betrayal.[99]

---

97. For fun, we can imagine even more fanciful versions of the hypothetical. Suppose the hotel manager says, "I'm worried that if I let you into the room, whatever evidence you find will ultimately be tossed. But I've read the *Jacobsen* case"—which, without a time machine or great prescience, the hotel manager in *Stoner* could not have done; but the point still stands—"so I know that if *I* perform the search, and I bring the evidence back out to you, there's no Fourth Amendment problem. So sit tight."

98. *See infra* notes 103–10 and accompanying text.

99. *See* United States v. Spicer, 432 F. App'x 522 (6th Cir. 2011) (holding that the private search rule—allowing law enforcement to retrace the steps of private actors who have already performed a search—does not apply to hotel rooms because they are, in essence, residences); United States v. Young, 573 F.3d 711, 720–21 (9th Cir. 2009) (drawing on *Stoner* to hold that it was a Fourth Amendment violation when security personnel at a hotel—private employees—engaged in a search of defendant's hotel room, opened suitcases to locate contraband, and gave the contraband to the police); *see also* Georgia v. Randolph, 547 U.S. 103, 112 (2006) ("[A] hotel manager calls up no customary understanding of authority to admit guests without the consent of the current occupant . . . and a hotel guest customarily has no reason to expect the manager to allow anyone but his own employees into his room."). *But see* United States v. Veatch, 674 F.2d 1217, 1219–21 (9th Cir. 1981) (finding no violation for hotel manager to turn over to law enforcement contraband that defendant had abandoned in his room, despite the fact that defendant had instructed the hotel manager to convey the contraband to his lawyer); State v. Weekley, 27 P.3d 325, 329–30 (Ariz. Ct. App. 2001) (concluding it was private action outside the Fourth Amendment's

In my view, *Stoner* vindicates the grander of these principles. It stands for the proposition that hotel managers, because they are hotel managers, are not permitted to betray guests to law enforcement—even when they do so voluntarily, even when it is they, not police officers, who perform the searches in question.[100] Here, as in *Ferguson*, something about the underlying relationship makes it normatively inappropriate to speak of trust being "misplaced." Just as it would misconstrue the act of giving a urine sample to a doctor to conclude that a patient has "assumed the risk" of betrayal by her doctor, it also misunderstands the act of leaving room keys at the front desk of a hotel to conclude that a hotel guest has "assumed the risk" of betrayal by hotel staff. In both settings, widespread expectations are to the contrary.

D. An Objection: State Agency

Very well—but even supposing these heterodox interpretations succeed, and the Court truly *has* picked out relationships with doctors and hotel managers for heightened protection, there is still an elephant in the room. What does it mean to say that private actors, cooperating with law enforcement of their own volition, are bound by the Fourth Amendment? The first principle of nearly all constitutional law is that the Constitution constrains *state* action, not private action. Taking this principle seriously, how can the fiduciary rule get off the ground? If *Ferguson* and *Stoner* stand for the proposition that certain types of private actors are bound by the strictures of the Constitution, perhaps the proper inference is simply that *Ferguson* and *Stoner* are wrong.

Although other, more overtly normative responses are conceivable,[101] the simplest response is that Fourth Amendment law has long contained a "state

---

reach when hotel staff searched a guest's room); Glass v. State, 696 S.E.2d 140, 144 (Ga. Ct. App. 2010) (holding no Fourth Amendment violation for maid to report contraband witnessed in hotel room).

100. *See Young*, 573 F.3d at 720–21; United States v. Allen, 106 F.3d 695, 698–700 (6th Cir. 1997). In *Allen*, the court held that the defendant lacked an expectation of privacy in his hotel room because he had been locked out of the room when management learned that he was using it to store contraband. But in so holding, the court also suggested that a search carried out by hotel management, *before* locking defendant out of the room, would have been subject to Fourth Amendment scrutiny notwithstanding *Jacobsen*. *Id.* at 699 ("Unlike the package in *Jacobsen*, however, which 'contained nothing but contraband,' Allen's motel room was a temporary abode containing personal possessions. Allen had a legitimate and significant privacy interest in the contents of his motel room . . . . [T]his Court is unwilling to extend the holding in *Jacobsen* to cases involving private searches of residences." (quoting United States v. Jacobsen, 466 U.S. 109, 120 n.17 (1984))); *see also* United States v. Paige, 136 F.3d 1012, 1020–21 n.11 (5th Cir. 1998) (applying the same reasoning—and refusing to extend *Jacobsen* on the same grounds—in the context of a home, when the owner let a handyman in to perform repairs on the roof).

101. It is possible, for example, to answer the state action challenge by severing duties from remedies and arguing that even if "Fourth Amendment fiduciaries" are not bound by the Constitution (due to their private status), the exclusionary remedy (and perhaps also civil remedies) should be available to defendants whose incrimination was built on cooperation between fiduciaries and law enforcement. Normally, we think of constitutional right violations (and resulting remedies) in one-to-one correspondence with constitutional duties. If *A* claims that *B* violated his constitutional rights, the meaning of *A*'s grievance is that *B*

agency" principle—an appreciation of the fact that private actors sometimes become extensions of law enforcement and that, when they do, the Fourth Amendment's protections come back into play. In this light, the fiduciary rule does not undermine the state action requirement. It merely provides a more realistic—and normatively appealing—gloss on what it means for private actors to operate as "state agents."[102]

As it stands, the case law about when private actors operate as state agents is checkered at best. The Supreme Court has been virtually silent on the matter,[103] and appellate courts have yet to converge on clear standards. Everyone seems to agree that if a private actor is legally *required* to assist

---

had a duty (to *A*) that *B* failed to discharge. But this relationship between rights, remedies, and duties is contingent, not necessary. In fact, there are times when constitutional rights are violated, and remedies are available, despite the fact that the party initially responsible for the violation, in light of her status as a private actor, has no corresponding constitutional *duty*.

One clear example is ineffective assistance of counsel. The Sixth Amendment has long been understood to ensure that criminal defendants receive adequate legal representation. One implication of this guarantee is that states must fund representation for indigent defendants. *See* Padilla v. Kentucky, 559 U.S. 356, 364–65 (2010); Gideon v. Wainwright, 372 U.S. 335, 340–41 (1963). But another implication is that when a defendant—*any* defendant—does not receive effective assistance from competent counsel, she has constitutional recourse: under some circumstances, she can demand a new trial; under other circumstances, she can revive expired plea deals; and so forth. *See, e.g.*, Missouri v. Frye, 132 S. Ct. 1399, 1410 (2012) (holding that a defendant who was never informed of a favorable plea deal should be allowed to reconsider the deal and have it reinstated *nunc pro tunc*); Hill v. Lockhart, 474 U.S. 52, 62 (1985) (clarifying that the Sixth Amendment applies to plea bargains); Hughes v. United States, 258 F.3d 453, 460 (6th Cir. 2001) (granting a new trial due to ineffective assistance when counsel failed to strike a juror who admitted bias). Crucially, these constitutional remedies are available whether the attorney is in private practice or employed by the government. No one believes—nor would it make normative sense to suggest—that Sixth Amendment remedies should hinge on that distinction or that, by choosing to hire private counsel rather than work with a public defender, a criminal defendant waives her right to constitutional remedies in the event of ineffective assistance. Who signs the lawyer's paycheck is irrelevant. The Constitution forbids the state from subjecting an inadequately represented defendant to (certain forms of) criminal liability, whether or not a state actor provided the representation. Likewise, perhaps in the Fourth Amendment setting, although information fiduciaries are not bound by the Fourth Amendment (just as private attorneys are not bound by the Sixth), law enforcement is prohibited from relying on—and prosecutors, from introducing—evidence procured by particularly intrusive means, whether or not a state actor was initially responsible for the intrusion.

102. *See Jacobsen*, 466 U.S. at 113 (explaining that the Fourth Amendment is "inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual *not acting as an agent of the Government or with the participation or knowledge of any governmental official*'" (emphasis added) (quoting Walter v. United States, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting))).

103. *Jacobsen* is one of the few cases on point, and because it held that the FedEx workers were *not* government agents, it ultimately sheds little light on what such agency consists of. The only other major Supreme Court case is *Skinner*, which held that a private railway was a state agent when it screened its employees for drug use, due to the extensive regulations related to such screening. *See supra* notes 56–61 and accompanying text. For a possible explanation as to *why* the private search doctrine has received comparatively little elaboration, see Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 643, 662 (2013) (arguing that the private search rule has fused together with the plain view rule, such that "private searches" are really just a subset of cases in which a law enforcement official becomes alerted to something incriminating through no action of her own).

the police, the private actor becomes a state agent.[104] Likewise, there appears to be consensus that when private actors receive monetary compensation (or other quid pro quo consideration) for assisting the police, they should be treated as state agents.[105] Less clear are cases where assistance is neither instigated nor compensated by the state but nonetheless reflects an endogenous desire on the part of a private actor to aid law enforcement. Some courts express support for the view that "law enforcement motivation" can suffice, on its own, to transform otherwise-private activity into a Fourth Amendment search.[106] Other courts disagree.[107] And some opt for a split-the-difference approach, one that

104. *See* Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 614 (1989) (holding that it constituted a "search" when a private railroad company performed urine tests on its employees pursuant to a federal statute). The principle reaches beyond formal compulsion. It also encompasses situations where law enforcement provides substantial support to an otherwise-private search. *See id.* at 614–15 (applying Fourth Amendment scrutiny to drug testing carried out by private railway companies, due to the existence of federal regulations that facilitated the testing); United States v. Stevenson, 727 F.3d 826, 829 (8th Cir. 2013) (holding private investigative activity can qualify as a Fourth Amendment search, even if not formally compelled, insofar as the government "demonstrate[s] a strong . . . preference for [it]"); Cassidy v. Chertoff, 471 F.3d 67, 74 (2d Cir. 2006) ("Although a wholly private search falls outside the scope of the Fourth Amendment, a search conducted by private individuals at the instigation of a government officer or authority constitutes a governmental search for purposes of the Fourth Amendment.").

105. *See, e.g.*, United States v. Jarrett, 338 F.3d 339, 344 (4th Cir. 2003) (holding that an anonymous hacker's search for child pornography did not violate the Fourth Amendment, despite being a crime, because the government did not "participate[]" in the search, but noting that the analysis would be different in the event that the government compensated the hacker); United States v. Hall, 142 F.3d 988, 993 (7th Cir. 1998) (holding that a technician's discovery of files on defendant's computer, "made pursuant to . . . maintenance work" that "[t]he Government had no knowledge [of]" and for which it paid the technician no "reward," is not protected by the Fourth Amendment); United States v. Koenig, 856 F.2d 843, 848 (7th Cir. 1988) (holding that a FedEx employee with a predilection for searching customers' packages was not operating as a state agent because, inter alia, the employee had "never worked as an informant for the DEA, ha[d] *never been rewarded by the DEA for his aid*, nor even discussed with law enforcement authorities what to look for" (emphasis added)).

106. *See, e.g.*, United States v. Bowers, 594 F.3d 522, 526 (6th Cir. 2010) (holding that for a search to be private, "*the intent of the private party* conducting the search [must be] *entirely independent* of the government's intent to collect evidence for use in a criminal prosecution" (quoting United States v. Hardin, 539 F.3d 404, 418 (6th Cir. 2008))); United States v. Pervaz, 118 F.3d 1, 6 (1st Cir. 1997) (citing, as one variable in determining whether a search is truly private, "the extent to which the private party aims primarily to help the government or to serve its own interests"); United States v. Attson, 900 F.2d 1427, 1431 (9th Cir. 1990) (an otherwise-private search meets with Fourth Amendment scrutiny if "its purpose [is] to elicit a benefit for the government in either its investigative or administrative capacities"); *see also* Joshuah Lisk, Comment, *Is Batman a State Actor?: The Dark Knight's Relationship with the Gotham City Police Department and the Fourth Amendment Implications*, 64 CASE W. RES. L. REV. 1419, 1431–32 nn.65–72 (2014) (discussing the applicability of the private search doctrine to searches carried out exclusively for a law enforcement purpose).

107. *See, e.g.*, United States v. Huber, 404 F.3d 1047, 1053–54 (8th Cir. 2005) (holding that even if a bookkeeper was "motivated, to some extent, by an urge to help the government, either as a means of protecting herself through the prospect of immunity or by the 'simple but often powerful convention of openness and honesty,'" that "is not enough to make her a government agent" in the absence of instigation by law enforcement (quoting Coolidge v. New Hampshire, 403 U.S. 443, 488 (1971))); United States v. Smythe, 84 F.3d 1240, 1243 (10th Cir. 1996) (for a private search to constitute state action, "the

regards "law enforcement motivation" as one *potentially*—but not necessarily—dispositive variable in the analysis.[108]

Against this backdrop, the fiduciary rule can be understood as a way of designating a particular type of private activity—the voluntary assistance of law enforcement by information fiduciaries—as de facto state action. So understood, the fiduciary rule overlaps analytically with the idea of "entwinement" that the Court has developed in other settings that pose difficult issues of state action. In the bankruptcy context, for example, the Court has construed the wrongful attachment of property (in anticipation of bankruptcy) as state action for the purpose of bringing due process claims.[109] Accordingly, it has allowed § 1983 actions to proceed not only against the judicial officers who wrongfully issue writs of attachment but also against a private actor who wrongfully *requests* a writ of attachment. In essence, the Court's reasoning was that because the request for a writ is what puts the wheels of attachment in motion, the request qualifies, by itself, as state action—even if not instigated by the government.[110]

---

government . . . *must* . . . *affirmatively encourage, initiate or instigate* the private action," or put otherwise, the question turns on whether "the government coerces, dominates or directs the actions of a private person" (emphasis added) (quoting Pleasant v. Lovell, 876 F.2d 787, 796 (10th Cir. 1989))).

108. *See, e.g.*, United States v. Momoh, 427 F.3d 137, 140–41 (1st Cir. 2005) (enumerating the following factors as relevant in distinguishing private and government action for Fourth Amendment purposes: "the extent of the government's role in instigating or participating in the search, its intent and the degree of control it exercises over the search and the private party, and the extent to which the private party aims primarily to help the government or to serve its own interests" (quoting *Pervaz*, 118 F.3d at 6)); United States v. Ellyson, 326 F.3d 522, 527 (4th Cir. 2003) (describing the state agency test as a "fact-intensive inquiry" that asks "whether the government knew of and acquiesced in the intrusive conduct and whether the private party's purpose for conducting the search was to assist law enforcement efforts or to further her own ends" (quoting United States v. Feffer, 831 F.2d 734, 739 (7th Cir. 1987))).

109. *See* Sniadach v. Family Fin. Corp. of Bay View, 395 U.S. 337, 341–42 (1969).

110. *See* Lugar v. Edmondson Oil Co., 457 U.S. 922, 933 (1982) (explaining that, in the typical case involving the attachment of property by a creditor, although "state agents aid[] the creditor in securing the disputed property[,] . . . the federal [due process challenge] ar[ises] in litigation between creditor and debtor in the state courts and no state official [i]s named as a party," but that this fact does not frustrate the federal court's ability to "entertain[] and adjudicate[] the defendant-debtor's claim that the procedure under which the private creditor secured the disputed property violated federal constitutional standards of due process"); *id.* at 941 ("[W]e have consistently held that a private party's joint participation with state officials in the seizure of disputed property is sufficient to characterize that party as a 'state actor' for purposes of the Fourteenth Amendment."); *id.* at 927 n.6 ("Joint action with a state official to accomplish a prejudgment deprivation of a constitutionally protected property interest will support a § 1983 claim against a private party."). For other cases along these lines, see *Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass'n*, 531 U.S. 288, 296 (2001) (stating that a private actor is subject to the Constitution "when a private actor operates as a 'willful participant in joint activity with the State or its agents'" (quoting *Lugar*, 457 U.S. at 941)); *Blum v. Yaretsky*, 457 U.S. 991, 1004 (1982) ("[The] State . . . can be held responsible for a private decision . . . when it has exercised coercive power or has provided such significant encouragement, either overt or covert . . . ."); *Evans v. Newton*, 382 U.S. 296, 299 (1966) (explaining that "[c]onduct that is formally 'private' may become so entwined with governmental policies or so impregnated with a governmental character as to become subject to the constitutional limitations placed upon state action," and applying the principle to a municipality's acting as trustee to a private estate). For further background

So, too, in the law enforcement setting: a private actor that assists the police voluntarily is no less "entwined" with an inherently public function than she would be if the police were compelling her cooperation. It is unclear in principle, and the Court has offered no convincing explanation in practice, why chronology—who *initiates* the entwinement—should drive the analysis. If the concern is about private actors using the machinery of state power to imperil the interests of other private actors, it would seem more natural to focus on the presence (or absence) of entwinement as such, not on its origin. That is, it would seem more natural to focus on whether the private actor in question *actually was* entwined with law enforcement, instead of how the entwinement came about.[111] Indeed, this is exactly what some appellate courts have done by applying Fourth Amendment scrutiny to private action simply because it stemmed, in the first instance, from a desire to aid law enforcement.

For reasons explained more fully below, I believe these courts go too far. There are both normative and pragmatic reasons to leave private actors free, as a general matter, to assist the authorities, which is exactly why the misplaced trust rule makes sense as a default.[112] But even if the entwinement principle should not apply to *all* voluntary cooperation with law enforcement, it should certainly apply—as I argue below—to voluntary cooperation by information fiduciaries. When information fiduciaries step into the shoes of law enforcement, they have the capacity, because of their

---

on the "entwinement" principle, see Benjamin F. Jackson, *Censorship and Freedom of Expression in the Age of Facebook*, 44 N.M. L. REV. 121, 152–53 (2014).

111. Another way to put this point would be that limiting the ability of information fiduciaries to share information with law enforcement is, in practice, really just a way of constraining the way law enforcement officials *gather* information. In other words, constitutional protection actually attaches to the *receipt* of evidence, not to its transmission; the rule prohibits law enforcement from, for example, capitalizing on a doctor's decision to betray her patient. Or, more exactly put, the rule requires that law enforcement, in order *to* capitalize on a doctor's decision to betray her patient, must ensure that the overall process of collection and disclosure complies with the Fourth Amendment's "reasonableness" requirement. Among other things, this framing helps to sow the beginnings of a distinction between dragnet surveillance programs—like the one described in *Ferguson*—and garden variety mandated reporter laws, which obligate doctors (among other actors) to report certain kinds of dangerous or harmful activity. In those circumstances, the presence of dangerous behavior acts as an ipso facto Fourth Amendment safeguard, rendering an otherwise-protected disclosure inherently reasonable. In other words, one way to think about mandated reporter laws, within the confines of the fiduciary rule, is to say that reporting does amount to a search, but the search complies with the Fourth Amendment. *See* Ferguson v. City of Charleston, 532 U.S. 67, 86–91 (2001) (Kennedy, J., concurring) (explaining why, in his view, *Ferguson* does not reach mandated reporter laws).

112. Limiting the ability of private actors to assist law enforcement across the board—that is, discarding the misplaced trust rule in its entirety—would lead to both normative and doctrinal problems. *See, e.g.*, Georgia v. Randolph, 547 U.S. 103, 115–16 (2006) (noting a person's "interest as a citizen in bringing criminal activity to light"); Coolidge v. New Hampshire, 403 U.S. 443, 488–89 (1971) (safeguarding the ability of one spouse to intentionally transmit to law enforcement incriminating evidence about the other); *cf.* On Lee v. United States, 343 U.S. 747, 756 (1952) ("Society can ill afford to throw away the evidence produced by the falling out, jealousies, and quarrels of those who live by outwitting the law. Certainly no one would foreclose the turning of state's evidence by denizens of the underworld.").

role, to violate expectations of privacy in a different way than other private actors. The sense in which that is true—and what it means for the conceptual structure of Fourth Amendment law—are the topics addressed in the rest of this Article.

II. THE NORMATIVE PUZZLE

The proposition that the law of searches consists of two—and only two—tiers has hobbled efforts to retool Fourth Amendment doctrine for the digital age. Beginning from the premise that sharing information results either in (1) exposure, or (2) misplaced trust, scholars have focused on dialing protection upward, on explaining why certain cases currently analyzed under the exposure rule should, instead, be analyzed under the misplaced trust rule.

As a result, criticism of existing doctrine, for all its fervency, ends up having limited bite. Although scholars and judges have spared no effort putting the lash to *Smith* and *Miller*, they have left unanswered—indeed, unasked—how the Fourth Amendment bears on voluntary private action. The urgency of this question, already on the rise, will only increase with time. In today's world, it is not just the occasional service provider—like a doctor or a hotel manager—who possesses sensitive information about us. A large (and growing) number of private entities currently have access to vast (and growing) stores of voluntarily conveyed information about all of us. If these intermediaries are categorically free to cooperate with law enforcement—if their use of our information falls totally outside the bounds of Fourth Amendment scrutiny, as the traditional story would imply—the erosion of privacy will be unforgiving and swift.

In response, this part draws on the foregoing doctrinal analysis to develop a tiered account of constitutional privacy, centered on relationships. To do so, I draw on the law of fiduciary duties and, in particular, on Jack Balkin's concept of "information fiduciaries."[113] The common thread uniting the two examples from Part I—doctors and hotel managers—is that both hold sensitive information for the benefit of the would-be suspect or defendant. For them to share sensitive information with law enforcement would, therefore, flout an implied limitation on its use.

Ultimately, the question becomes, how can information fiduciaries be distinguished from other parties—friends, family members, colleagues, and so forth—with whom we routinely share sensitive information, expecting it to be kept in (some degree of) confidence? The answer, I suggest, is twofold. First, we share information with fiduciaries despite the fact that we have no reason, in the everyday sense of the term, to *trust* them. Second, because of the social functions that information fiduciaries serve, the decision to share sensitive information with them is, practically speaking, involuntary. In my view, these considerations render informal systems of social regulation insufficient to ensure integrity, and they make it necessary for implied legal duties to fill the gap. Before building out this

113. Balkin, *supra* note 5.

answer, however, it will be useful to examine where the existing criticism of Fourth Amendment law stands—and what it has missed.

A. Existing Commentary

To date, the Fourth Amendment reform effort, among both scholars and lower court judges, has focused on explaining why fact patterns traditionally analyzed as "exposure" cases should be analyzed, instead, as "misplaced trust" cases. The effort begins from two conceptually distinct (though often overlapping) starting points. The first focuses on the *type* of information at stake; the second, on the *amount* of such information.

1. Type of Information

The first approach to reform—primarily aimed at the third-party doctrine—has been to emphasize the sensitive nature of the information we share with counterparties today. 1979 is gone. Today, it is not just dialed numbers being disclosed to telephone companies; it is all manner of highly personal information being disclosed to internet service providers, social media sites, and the like—often by virtue of arcane user agreements that garner our consent only in the thinnest sense of the phrase.[114]

In response to this reality, scholars have long been clamoring for the abolition of *Smith* and *Miller* and the ill-formed theory of "exposure" on which they rest.[115] Stephen Henderson, for example, regards the third-party doctrine as "fundamentally misguided,"[116] among other reasons because it fails to distinguish between *recipients* of sensitive information (such as friends and loved ones) and *conduits* of sensitive information (such as Google).[117] In a similar vein, Jed Rubenfeld has argued that the third-party doctrine, if followed to its logical end, would render "the Fourth Amendment . . . a hollow shell, because in an increasingly digitized, networked world with ever-expanding privacy-invading technologies, virtually all information is exposed to third parties."[118] Indeed, according to Rubenfeld, even *Katz* is not safe from the doctrine's ruinous touch, because "[e]ven Katz had exposed the seized information to a third

---

114. *See* David A. Anderson, *Privacy and Fictitious Contracts*, 87 TEX. L. REV. *SEE ALSO* 11, 13–14 (2009) (explaining the "preposterous[]" way that "law treats our acquiescence [to form contracts] as if we had bargained with the entity and reached a mutually agreeable solution").

115. *See generally* Colb, *supra* note 11 (demonstrating how both steps of the logic of the third-party doctrine—equating risk with invitation and equating large intrusions with small ones—fall off the bone conceptually). *See also* Jane Bambauer, *Other People's Papers*, 94 TEX. L. REV. (forthcoming 2015) (manuscript at 4), http://ssrn.com/abstract=2572448 (noting that "[t]he third party doctrine may be dismantled soon, and for good reason [as] [i]t always strained the logic and common sense of search and seizure law") [http://perma.cc/C6CE-KNKL]; Selbst, *supra* note 103, at 668 (describing the third-party doctrine originating in *Smith* and *Miller* as the "favorite villain" of Fourth Amendment scholars).

116. Henderson, *Timely Demise*, *supra* note 11, at 40.

117. *See id.* at 40 & nn.6–8; *see also* Stephen E. Henderson, *Nothing New Under the Sun?: A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 524–28 (2005).

118. Rubenfeld, *supra* note 11, at 115.

party,"[119] which means, on a strict reading of *Smith* and *Miller*, that Katz lost his expectation of privacy the minute he picked up the phone.[120] Furthermore, even if the distinction between "content" and "noncontent" information successfully distinguished *Smith* from *Katz* when the former came down, the coherence of that distinction has long since fallen to ash. For in the digital age, "noncontent information may reveal"—and increasingly *does* reveal—"as much, if not more, intimate [knowledge] about users than the content of communications do."[121]

Other scholars have focused on drawing analogies outside of Fourth Amendment law. Susan Brenner, for example, has likened digital service providers to servants at common law.[122] Because the common law recognized "a concept of 'shared privacy,'" it understood servants as an extension of the household; interrogating them—or compelling their testimony—was equivalent to interrogating or compelling testimony from other members of the family.[123] In a similar vein, Monu Bedi has invoked the idea of "inter-personal privacy"—an idea that he ties back to fundamental rights cases, such as *Lawrence v. Texas*[124]—to explain why the aggressive variant of the third-party doctrine offered in *Smith* and *Miller* should not apply to communication over Facebook.[125] Bedi argues, in essence, that because Facebook is a forum in which we *exercise* our privacy rights, to exempt information shared with Facebook from privacy protection would drain those rights of practical meaning.[126]

Kathy Strandburg has coined a phrase that aptly summarizes the sensibility underlying these positions: "technosocial continuity."[127] Just as "the special solicitude for the home and office" in Fourth Amendment law

119. *Id.*

120. *See id.* Of course, the Court has not been inclined to construe *Smith* and *Miller* this way—a fact that to some scholars suggests the third-party doctrine is not the sturdy foundation that appearances imply. *See supra* note 28.

121. Olivier Sylvain, *Failing Expectations: Fourth Amendment Doctrine in the Era of Total Surveillance*, 49 WAKE FOREST L. REV. 485, 488 (2014); *see also* Simon Stern, *The Third-Party Doctrine and the Third Person*, 16 NEW CRIM. L. REV. 364, 391–92 (2013) (exploring ways in which "no content" data in fact can embed far more—and richer—*information* than "content" data); Katherine J. Strandburg, *Membership Lists, Metadata, and Freedom of Association's Specificity Requirement*, 10 J.L. & POL'Y FOR INFO. SOC'Y 327 (2014) (exploring the breathtaking sweep of metadata collection efforts today and the "associational information" they reveal); Jane Mayer, *What's the Matter with Metadata?*, NEW YORKER (June 6, 2013), http://www.newyorker.com/news/news-desk/whats-the-matter-with-metadata [http://perma.cc/84PK-VL5W]. Nita Farahany has come up with a particularly clever example of where the distinction between content and noncontent information breaks down: situations where it is necessary to dial numbers in order to navigate a menu. *See* Nita A. Farahany, *Searching Secrets*, 160 U. PA. L. REV. 1239, 1252 (2012).

122. Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1, 76 (2005).

123. *Id.* at 80–81.

124. 539 U.S. 558 (2003).

125. Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1, 2–5, 15–36 (2013).

126. *Id.* at 29–32.

127. Strandburg, *supra* note 11, at 619.

stems from the "social functions [those] places perform,"[128] new practices like "social media and cloud computing" should *also* be recognized for the social functions they perform and for the "social changes [they have] occasioned."[129] To safeguard privacy in the digital age, therefore, we must update the rules that govern shared information, so as to recognize that sensitive information is shared today with many more entities, and many different *kinds* of entities, than ever before. Applying the wooden rule from *Smith* and *Miller* to all such sharing would not only yield undesirable results, but would also disavow reality. Instead, constitutional rules should be crafted "in a technosocially continuous manner,"[130] which means, in practice, that they should "build upon" the forms of protection traditionally associated with the home.[131] Put simply, the Fourth Amendment should be sensitive to social practice and should evolve, accordingly, as social practice evolves.[132]

2. Amount of Information

The second approach to reform—which focuses more on traditional "exposure" cases than the third-party doctrine—has been to highlight the sheer amount of information we share with counterparties today. The most prominent advocates of this approach are Danielle Citron and David Gray, who argue that the digital age is distinctive, as far as privacy is concerned,

128. *Id.* at 659.

129. *Id.* at 650.

130. *Id.* at 658.

131. *Id.* Similar trends can be ascertained from recent judicial opinions. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2491 (2014) ("A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is."); United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (musing that, in the digital age, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties" due to the fact that "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks").

132. This view is widely shared in *all* privacy scholarship, not just commentary on the Fourth Amendment. Indeed, one of the benefits of the fiduciary rule, in my view, is that it incorporates—and packages in doctrinally operational form—the insights of various privacy theorists that have emphasized the importance of contextual variance in privacy norms. *See, e.g.*, JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE (2012); HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 129–31 (2010) (arguing for an approach to privacy policy that focuses on "contextual integrity" and attention to the actuality of social practice); Anita L. Allen, *Privacy-As-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861, 866 (2000); Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1093, 1128 (2002) (arguing that "privacy" is a porous concept and that its meaning and normative salience differs depending on the context). I am not the first to relate these "context-based" accounts of privacy—which are pitched at a high level of abstraction and tend to be explicitly normative in character—to Fourth Amendment doctrine. For perhaps the most ambitious effort along these lines, see Selbst, *supra* note 103 (drawing on Helen Nissenbaum's work on "contextual integrity" and seeking to make expectations about "information flow" the touchstone of constitutional privacy); *see also* Laurent Sacharoff, *The Relational Nature of Privacy*, 16 LEWIS & CLARK L. REV. 1249 (2012).

because of the *means* of data collection available today.[133] In a way that has never been true before, it is now possible (for law enforcement and private parties alike) to cheaply amass and archive enormous volumes of information. From this observation, Citron and Gray conclude that the Fourth Amendment's scope—the threshold doctrinal question of which activities qualify, in the first place, as searches—must become responsive to the "how," rather than the "what," of surveillance.[134] According to Citron and Gray, data collected by ordinary means poses no Fourth Amendment problem. But data collected by *enhanced* means—means that were previously unavailable—does pose such a problem. In their words:

> There is . . . no Fourth Amendment issue just because investigators collect a detailed mosaic of personal information on a suspect. Rather, it is the means that matter. Thus, the Fourth Amendment would not be implicated if a third party used pen registers or similar technology to gather evidence for the government because these technologies are too limited to facilitate the sort of broad and indiscriminate surveillance characteristic of a surveillance state. By contrast, the data aggregation technologies deployed by Verizon and other telecommunications companies to provide the FBI and the NSA with "telephony metadata" for all calls "between the United States and abroad" and all calls "wholly within the United States, including local telephone calls" implicate "different constitutional principles." By virtue of their scale and scope, these data aggregation capacities . . . should . . . be subject to Fourth Amendment regulation.[135]

Other commentators agree. Elizabeth Joh, for example, has made similar arguments in favor of rethinking the Court's "abandoned DNA" jurisprudence.[136] In a world where technological advancement has made it so that "nearly any 'body particle' can reveal entirely our genetic information," limits should be placed on law enforcement's ability to procure such "particles."[137] The upshot of Joh's view is the same as Citron and Gray's: law enforcement is increasingly equipped with means of easily and cheaply collecting vast amounts of information about citizens—and in response, the Fourth Amendment must evolve.[138]

---

133. *See* Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. F. 262 (2013).

134. *Id.* at 267.

135. David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 143 (2013) (footnotes omitted); *see also* Joel R. Reidenberg, *Privacy in Public*, 69 U. MIAMI L. REV. 141, 147–52 (2014) (exploring the way that technological advances have rapidly intensified the amount of "public" information that can be seized and stored, putting normative strain on the "exposure" principle at the heart of much Fourth Amendment law).

136. *See* Elizabeth E. Joh, Essay, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857 (2006). *See generally* Erin Murphy, *License, Registration, Cheek Swab: DNA Testing and the Divided Court*, 127 HARV. L. REV. 161 (2013) (discussing the Fourth Amendment status of DNA collection and the specifically quantitative concerns that it inspires).

137. Joh, *supra* note 136, at 859–60.

138. *See* Elizabeth E. Joh, *Policing By Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35 (2014). *But see* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012) (arguing that the mosaic theory leads to

The quantitative approach, alternatively called the "mosaic theory," also appears to be gaining traction in the courts.[139] Although *United States v. Jones* was resolved (famously or infamously, depending on one's view) on trespass grounds, five Justices seemed poised to resolve the case on quantitative grounds.[140] Furthermore, a unanimous Court recently expressed support for the "quantitative privacy" view in *Riley v. California*,[141] which held that, incident to an arrest, the police may not engage in the suspicionless search of a smart phone's contents.[142]

Indeed, *Riley* offers a good example of a setting in which the quantitative and qualitative approaches coalesce, as they often do. The problem with allowing law enforcement to examine the contents of smart phones could be stated in two different, if overlapping, ways.[143] To begin with, smart phones contain all sorts of sensitive information; by perusing someone's phone for just a handful of minutes, I can learn many intimate details of their life. Secondly, smart phones contain an enormous volume of information; in a different era, amassing the amount of data currently stored on smart phones today would have required invasive and prolonged investigation.

---

considerable line-drawing problems and fails to capture the stakes of Fourth Amendment protection).

139. *See* United States v. Jones, 132 S. Ct. 945, 954–57 (2012) (Sotomayor, J., concurring) (suggesting that constitutional privacy doctrine should change in response to law enforcement-empowering technologies); ACLU v. Clapper, 785 F.3d 787, 822–23 (2d Cir. 2015) ("[R]ules that permit the government to obtain records and other information that consumers have shared with businesses without a warrant seem much more threatening as the extent of such information grows."); Transcript of Oral Argument at 16, *Jones*, 132 S. Ct. 945 (No. 10-1259) (Chief Justice Roberts describing the distinction between following a car around for a few days and tracking the movements via GPS as "the difference between seeing a little tile and seeing a mosaic"). It also has some support among state supreme courts (which are, of course, free to fashion *greater* parameters of protection than those fashioned by the U.S. Supreme Court). *See, e.g.*, People v. Sporleder, 666 P.2d 135, 142 (Colo. 1983) ("[A] pen register record holds out the prospect of an even greater intrusion in privacy when the record itself is acquired by the government, which has a technological capacity to convert basic data into a virtual mosaic of a person's life.").

140. *See Jones*, 132 S. Ct. at 955–57 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring) (joined by Justices Ginsburg, Breyer, and Kagan).

141. 134 S. Ct. 2473 (2014).

142. *Id.* at 2493. The rhetoric in *Riley* is noticeably sweeping. As Chief Justice Roberts put it:

> A cell phone collects in one place many distinct types of information . . . that reveal much more in combination than any isolated record. [And] a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions.

Id. at 2489.

143. As Chief Justice Roberts aptly summarized the point, "[C]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person." *Id.* And then, once again, emphasizing the confluence:

> Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.

Id. at 2490.

The same confluence is discernible in other Fourth Amendment settings as well.[144] In *Kyllo v. United States*,[145] for example, the Court held that a search occurred when law enforcement used an infrared scanner to detect heat emanating from a home.[146] Although the majority opinion focused on the sensitive information that such scanning might yield, given its proximity to the home—with Justice Scalia waxing somber at the idea of capturing data about "the lady of the house tak[ing] her daily sauna and bath"[147]—the practice is also troubling on quantitative grounds. Imagine if the scanner were left running for hours or days (or, as in *Jones*, months) on end. Even if the scanner picked up nothing particularly sensitive—even if there was nothing particularly sensitive *to* pick up—law enforcement might nevertheless come away with a detailed mosaic of activity in the home.[148]

B. "Misplaced Trust" Presupposes Trust

Ultimately, whether the fulcrum of reform is qualitative or quantitative, the goal is the same. The point of the reform effort is to truck cases from the "exposure" tier to the "misplaced trust" tier. In other words, the point is to explain why settings in which the Court has found that suspects have *no* expectation of privacy should, instead, be treated as settings in which suspects' expectation of privacy remains intact, but the expectation can be violated (with constitutional impunity) by any counterparty to whom the information has been disclosed. In other words, the point of the reform effort has been to equilibrate Fourth Amendment protection to the level of *Katz*, the Fourth Amendment's traditional "lodestar."[149] And this makes sense. In a doctrinal landscape haunted by *Smith* and *Miller*, the promise of *Katz*—that information voluntarily shared with another person might not lose all constitutional protection—is a significant promise indeed.

But there is a problem. For all that *Katz* protects against, the one thing it avowedly does *not* protect against is misplaced trust. This leads to major difficulties in the digital age, when information is "entrusted" to third parties *constantly*, at a pace and quantity never before imagined. Today, most interaction with other human beings, not to mention a ballooning number of everyday tasks, requires one to share information with countless third parties whose role—and profit source—is the intermediation of data. Email providers, social media sites, optimization companies like FitBit and

144. Indeed, in its way, DNA collection is another example of a practice that sounds alarm on both dimensions. Beyond the quantitative concerns explored above, DNA collection also raises qualitative concerns, in light of the inherently sensitive nature of genetic information. Though at some level, this would depend more than other examples on the particular *use* to which the captured data was being put.

145. 533 U.S. 27 (2001).

146. *Id.* at 40.

147. *Id.* at 38.

148. Scalia offers a hypothetical along these lines, in a startling prefiguration of Google Earth—"a satellite capable of scanning from many miles away [that] pick[s] up only visible light emanating from a house," allowing law enforcement to theoretically record everything visible from outside of a home (e.g., comings and goings) with impunity. *Id.* at 35.

149. Smith v. Maryland, 442 U.S. 735, 739 (1979).

Nest Labs, GPS navigation systems—the list is long and growing. The point is not that these entities are iniquitous. They perform important services and improve the world. But their presence in our lives—a less and less optional state of affairs—also makes it necessary to reconsider the role of the "misplaced trust" rule in Fourth Amendment doctrine.

Consider Gmail. I send an email to my sister, confessing that I stole a car. In so doing, I have shared information—the same information—with both my sister and Google. Each now possesses evidence that I stole a car. After sharing the information, what expectation of privacy, if any, do I retain? The qualitative and quantitative approaches both supply the same to this question. By sharing the information with Google, I have not—contra *Smith* and *Miller*—lost all ability to claim a privacy interest in it. Put simply, it should not be the case that I waive my expectation of privacy in information simply by disclosing it to Google—just as it is not the case, under *Katz*, that I waive my expectation of privacy in information simply by disclosing it to my sister.

The next question, however, becomes more complicated: How, if at all, does the Fourth Amendment regulate voluntary transmission of the information—by my sister or by Google—to law enforcement? In the case of my sister, the answer is clear: under existing doctrine, she is free to betray my trust. By telling her that I stole a car, I ran the risk that she would ultimately prove untrustworthy—that I was unwise to confide in her. Does the same analysis apply to Google? Under a strict construction of the misplaced trust rule—which, for reasons explored above, is not only consistent with *Katz* but, in some sense, *derived* from *Katz*—the answer would certainly be "yes." Google is a private actor with whom I have voluntarily shared information; therefore, it is free to betray me. Along these lines, consider how Patricia Bellia and Susan Freiwald analyze the issue in the course of arguing that *Smith* and *Miller* should not extend to stored email. Although they argue that using an email storage client should not extinguish one's expectation of privacy in the content of email outright, Bellia and Freiwald go on to conclude that

> if [an email provider] *chooses* to disclose the [content of a user's email] to the government without requiring a warrant, the user cannot complain. When the user assumed the risk that the intermediary would discover incriminating information or property in the course of its business, she also assumed the risk that the intermediary would choose to turn that information over to the government. If the user mistakenly trusted the intermediary to protect its incriminating information, there is no reason for the Fourth Amendment to protect that misplaced trust.[150]

150. Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121, 167 (2008). Resolving the question this way, Bellia and Freiwald made explicit what is, in other scholars' accounts, only latent. *See* Tokson, *supra* note 11, at 585 n.26 (compiling sources to this effect). In passing, it bears noting that Bellia and Freiwald's account has an interesting wrinkle. Analytically, the core proposition on which their view rests is the following: when people use services run by "third party intermediaries," they retain an expectation of privacy against the state, but they "lack a reasonable expectation of privacy with regard *to those third party intermediaries* who

This analysis certainly scores points for candor. But I want to suggest that it is both (1) normatively uncomfortable, and (2) in tension with the reasoning of *Ferguson* and *Stoner*. First, the normative point is not difficult to see. Under Bellia and Friewald's analysis—which flows from *Katz* and tracks the misplaced trust rule—it would be constitutional for Google (or an entity like it) to archive and mine all user data, running sophisticated analytics designed to unearth criminal behavior, and to submit the results to law enforcement (which could then sustain search warrants). Indeed, not only would this be constitutional; it would *not even trigger constitutional scrutiny*, because, under the misplaced trust rule, no Fourth Amendment search would have occurred. Making matters worse, the hypothetical is not genuinely hypothetical. Today, many intermediaries *do* assist law enforcement in ways like this. The assistance most commonly takes the form of ferreting out child pornography,[151] but there is little reason, in principle or in practice, to think that "data vigilantism" will remain circumscribed to that particular domain.[152] Furthermore, even among intermediaries that have not taken up the law enforcement mantle voluntarily, virtually all seem to be facing pressure in that direction.[153]

The bigger issue, however, is that the misplaced trust rule leaves Google (and other entities like it) free to use customer information this way despite the fact that, practically speaking, the information was never actually "entrusted" to Google in the manner the rule has in mind. When a user shares information with Google—like when a patient shares information with a doctor or a guest shares information with a hotel manager—she is engaged in what I will call "arm's length entrustment." Unlike, say,

---

discover information in the course of exercising their rightful access to[,] [for example,] the users' packages, storage lockers, rental properties, or stored e-mail accounts." Bellia & Freiwald, *supra*, at 166. Curiously, the only authority cited for this proposition are cases in which someone loses his expectation of privacy because the fiduciary relationship has expired, which would seem at least ambiguous—if not actively counterproductive—to their position. *Id.* at 166 n.184.

151. *See, e.g.*, United States v. Stevenson, 727 F.3d 826, 830 (8th Cir. 2013) (holding that AOL was not operating as an agent of law enforcement when it voluntarily monitored user email for the purpose of assisting with criminal investigation); United States v. Cameron, 699 F.3d 621, 637–38 (1st Cir. 2012) (holding likewise with respect to Yahoo!); United States v. Richardson, 607 F.3d 357, 367 (4th Cir. 2010) (holding same as to AOL); *see also* Hoofnagle, *supra* note 3, at 600–07 (discussing the data technology available to mainstream companies today).

152. Perhaps the best—and most chilling—argument along these lines comes from fiction. *See* DAVE EGGERS, THE CIRCLE (2013) (imagining a world in which a Google-like entity turns its sights toward, among other things, predictive analytics about criminal behavior).

153. For obvious reasons, this is difficult to quantify—the whole point of many of these programs is secrecy. But if recent revelations about the ubiquity of national security letters and so forth are any indication, pressure from law enforcement is incredibly widespread. *See, e.g.*, Rebecca Wexler, *Warrant Canaries and Disclosure by Design: The Real Threat to National Security Letter Gag Orders*, 124 YALE L.J. F. 158 (2014). To be clear, compliance with, for example, national security letters falls beyond the scope of my concern here because it is clearly instigated by law enforcement and, therefore, even under *existing* doctrine, not purely private action. The point is simply that, given the reality of pressure today, it is easy to imagine a climate tomorrow in which cooperation is voluntary (rather than compliant), but the upshot for privacy is the same.

siblings, Google and its users have no preexisting trust relationship. The reason a user shares information with Google has nothing to do with their relationship; rather, it is the precondition of using Gmail, just as sharing information with a doctor is the precondition of obtaining medical care, and sharing information with hotel staff is the precondition of renting a room. Furthermore, all three actors serve social functions that make sharing information with them practically involuntary. If I need medical care, I have no choice but to consult a doctor. If I need lodging, I have no choice but to find a hotel. Likewise, with email, if I wish to participate fully in the digital world—an increasingly unavoidable decision given the realities of social and professional life—I must engage with Internet Service Providers (ISPs).

This segues to the second difficulty with applying the misplaced trust rule to an entity like Google: it runs directly into *Ferguson* and *Stoner*. Consider Bellia and Friewald's final sentence—"[i]f [a] user mistakenly trusted the [ISP] to protect its incriminating information, there is no reason for the Fourth Amendment to protect that misplaced trust"[154]—as a template. On this logic, the proper analysis in *Ferguson* would have been as follows: "[I]f [a pregnant woman] mistakenly trusted [her doctor] to protect [the] incriminating information [contained in her urine], there is no reason for the Fourth Amendment to protect that misplaced trust." And similarly, in *Stoner*: "[I]f [a hotel guest] mistakenly trusted [hotel employees] to protect incriminating information [in his room], there is no reason for the Fourth Amendment to protect that misplaced trust." For the reasons explained at length in Part I, neither of these formulations is faithful to the logic of *Ferguson* and *Stoner*. In both cases, the upshot was that the defendant did *not* run the risk of misplaced trust. Rather, the third party's decision to voluntarily assist law enforcement fell within the bounds of Fourth Amendment protection because the Court recognized that "trust," in the everyday sense, was not present in these relationships at all. Instead, sensitive information had been "entrusted" at arm's length, and the decision to engage in arm's length entrustment was, in a practical sense, involuntary.[155]

Distinguishing between (1) the presence of genuine trust, and (2) the act of practically involuntary, arm's length entrustment not only helps to draw out the commonalities among doctors, hotel staff, and ISPs, but it also helps to pinpoint exactly what went wrong in *Smith* and *Miller*. Although these cases have inspired no shortage of vitriol, the foregoing analysis of arm's length entrustment makes clear that commentators have actually been too forgiving of the cases' common flaw. If, as *Ferguson* and *Stoner* (and

154. *See supra* text accompanying note 150.

155. Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting) ("Implicit in the concept of assumption of risk is some notion of choice. At least in the third-party consensual surveillance cases, which first incorporated risk analysis into Fourth Amendment doctrine, the defendant presumably had exercised some discretion in deciding who should enjoy his confidential communications. By contrast here, 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." (citations omitted)).

normative intuition) suggest, arm's length entrustment generates more Fourth Amendment protection than disclosure to a genuinely trusted party, *Smith* and *Miller* are not just wrong but backward; they regard arm's length entrustment—precisely because it is arm's length—as deserving of *less* Fourth Amendment protection. Therein lies the crucial error.

This element of backwardness came explicitly to the fore in *Smith*. In his opinion for the Court, Justice Blackmun distinguished *Smith* from *Katz* on the grounds that people have much less reason to trust a phone company than they have to trust a person on the other line of a call.[156] As Justice Blackman put it, "it is too much to believe that telephone subscribers . . . harbor any general expectation that the numbers they dial will remain secret,"[157] in implicit contrast to the expectation—codified in *Katz*—that telephone subscribers' actual conversations *will* remain secret. Viewed in this light, Justice Blackmun's logic is appealingly straightforward: because phone companies are less trusted than listeners, disclosures to phone companies (dialed numbers) should carry a lesser expectation of privacy than disclosures to listeners on the other line. In other words, there is a clear, linear relationship—according to Justice Blackmun—between trust and privacy protection.

Many commentators find Justice Blackmun's analysis in *Smith* unconvincing, to put it mildly. I am among them. But it is important to be precise about *why* Blackmun's analysis fails. The problem is not that Justice Blackmun (and the rest of the Court) hallucinated a distinction between sharing information with another person and sharing a dialed number with the phone company. That distinction is a real one; I *do* have less reason, generally speaking, to trust my phone company than I have (again, generally speaking) to trust people to whom I elect to talk on the phone. The problem is the next step in Justice Blackmun's reasoning. From the observation that people trust phone companies less than they trust other human beings, Justice Blackmun drew the wrong inference. In fact, he drew the *diametrically* wrong inference. Our lack of trust in phone companies, far from eroding constitutional protection, should have increased it. In short, what Justice Blackmun failed to appreciate—and what *Ferguson* and *Stoner* make clear—is that, for Fourth Amendment purposes, protection does not always correlate positively to trust. At times, the correlation inverts, and relationships predicated on arm's length entrustment of information carry greater protection than relationships predicated on genuine trust.

156. *Id.* at 743 (majority opinion).

157. *Id.* For the reasons explored in Part I, Justice Blackmun could not have meant "remain secret" to mean "not disclosed to another party"—the whole point was that both pieces of information (the contents of the call and number dialed) had already been disclosed to another party. Furthermore, the question was how to think about the significance of the disclosure.

III. WHO ARE FOURTH AMENDMENT FIDUCIARIES?

Ultimately, the claim is quite straightforward. Under conditions of practically involuntary, arm's length entrustment, one should be able to expect that shared information will be used only for limited purposes and certainly not to expose one to criminal liability. Indeed, in areas of "private privacy" law—as opposed to constitutional privacy law—regulators have already begun to recognize the need for implied, fiduciary-style duties to govern arm's length entrustment.[158] The same is true, I will argue, for Fourth Amendment doctrine as well.

Jack Balkin has fashioned a term—"information fiduciaries"—to describe the set of counterparties with whom we have relationships built on arm's length entrustment.[159] Although Balkin's analysis has focused specifically on ISPs, the logic extends beyond that realm.[160] In fact, it reaches all manner of counterparty to whom we entrust "personal [or] sensitive information" today, and who, because they occupy a status "analogous to . . . traditional . . . fiduciaries,"[161] are obligated to use that information in ways that benefit us (or at least, that don't work to our detriment). Whereas traditional fiduciaries often manage financial assets, and their duties tend to concern financial transactions, information fiduciaries manage the "asset" of information, and their duties primarily concern security and confidentiality. But putting to one side this difference in the *content* of duties owed by information fiduciaries as compared to traditional fiduciaries, their essential *nature* is the same. The duties operate, in practice, to constrain information fiduciaries from pursuing their unbounded self-interest, when doing so would collide with the interests of beneficiaries—that is, with our interests.[162]

To appreciate the force of Balkin's claim, particularly in the somewhat idiosyncratic setting of Fourth Amendment law, an overview of fiduciary norms will be useful. In general, fiduciary duties come in two forms: care

158. *See, e.g.*, Woodrow Hartzog & Daniel J. Solove, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 638–42 (2014) (exploring how the FTC uses "unfairness" as a doctrinal mechanism for enforcing widespread expectations and substantive privacy norms, notwithstanding the explicit language of privacy policies); Margot Kaminski, *Robots in the Home: What Will We Have Agreed to?*, 51 IDAHO L. REV. 661, 674 (2015) (noting that unlike the Fourth Amendment setting, where courts tend to interpret voluntary sharing of information with a third party as a *waiver* of privacy interests, "in the private actor context, they may consider substantive privacy norms even where consent has technically been granted"); *id.* at 674–75 & nn.73–77.

159. Balkin, *supra* note 5.

160. *See generally id.*

161. *Id.*

162. *See* Lynn A. Stout, *On the Export of U.S.-Style Corporate Fiduciary Duties to Other Cultures: Can a Transplant Take?*, *in* GLOBAL MARKETS, DOMESTIC INSTITUTIONS 46, 55 (Curtis J. Milhaupt ed., 2003) ("The keystone . . . legal obligation [is] that the fiduciary use her powers not for her own benefit but for the exclusive benefit of her beneficiary."); *see also* RESTATEMENT (SECOND) OF AGENCY LAW § 387 (AM. LAW INST. 1958) (explaining that a fiduciary is obligated "to act solely for the benefit of the principal in all matters connected with his agency").

and loyalty.[163] A duty of care is an obligation, in essence, to exercise diligence when making decisions on behalf of a beneficiary.[164] A duty of loyalty, by contrast, is an obligation to resolve conflicts of interest in favor of the beneficiary.[165] These two obligations are conceptually harmonious but also, in important respects, distinct. For example, suppose that *A* manages money for *B*—a role that carries both a duty of care and duty of loyalty. Pursuant to her duty of care, *A* has an obligation to ensure that investments are not riskier than *B* desires. To do so, *A* must be attuned to *B*'s appetite for risk (which, in practice, will likely be set by contract), and she must exercise diligence when reviewing possible investments. Pursuant to her duty of loyalty, on the other hand, *A* has an obligation to refrain from making investments on *B*'s behalf simply because *A* stands to benefit from those investments. For example, suppose that *A*, in addition to being a money manager, also owns Company *X*. If Company *X* is trying to attract a new round of funding, *A* may not pledge *B*'s assets—to which *A* only has access because of their fiduciary relationship—to help capitalize Company *X*. Doing so would subordinate *B*'s interests, which *A* is supposed to be safeguarding, to *A*'s *own* interests. It would be a form of "self-dealing."[166]

Ultimately, both duties respond to the same underlying problem. Fiduciaries, by virtue of their status, have access to the resources of their beneficiaries—a position naturally ripe for abuse, rendering informal mechanisms of accountability insufficient to ensure good behavior.[167]

---

163. There is some variance across legal settings, but all formulations seem to conceptually come back to care and loyalty. *See* Iman Anabtawi & Lynn Stout, *Fiduciary Duties for Activist Shareholders*, 60 STAN. L. REV. 1255, 1262 (2008) (explaining that corporate fiduciary duties "fall into two broad categories: the duty of loyalty and the duty of care"); Ethan Leib, *Friends As Fiduciaries*, 86 WASH. L. REV. 665, 675 (2009) (describing care and loyalty as the "two central fiduciary duties").

164. *See, e.g.*, Robert Cooter & Bradley J. Freedman, *The Fiduciary Relationship: Its Economic Character and Legal Consequences*, 66 N.Y.U. L. REV. 1045, 1047–49 (1991) (explaining that the duty of care is not merely a nonharm principle—unlike the duty of loyalty, it sometimes requires affirmative action on the fiduciary's part); Elizabeth S. Scott & Robert E. Scott, *Parents As Fiduciaries*, 81 VA. L. REV. 2401, 2420–21 (1995) (outlining the contours of the duty of care).

165. *See* Anabtawi & Stout, *supra* note 163, at 1263 (sketching the contours of the duty of loyalty in broad strokes); Cooter & Freedman, *supra* note 164, at 1045–55 (examining the scope of the duty of loyalty, and explaining when and why fiduciaries are permitted to engage in self-regarding behavior). Naturally, however, the duty of loyalty does not eliminate the room for self-serving behavior *outright*. *See, e.g.*, Eileen Scallen, *Promises Broken Vs. Promises Betrayed: Metaphor, Analogy, and the New Fiduciary Principle*, 1993 U. ILL. L. REV. 897, 908 ("[C]lassic fiduciary relationships are by no means divorced from self-serving considerations.").

166. *See* Cooter & Freedman, *supra* note 164, at 1054–55 (outlining the general prohibition on self-dealing, and explaining the limited circumstances in which fiduciaries are permitted to engage in it).

167. *See* Leib, *supra* note 163, at 683 (explaining that fiduciaries "ha[ve] easy access to important resources of [their] beneficiar[ies]," and that the purpose of fiduciary duties is to "deter misuse" of those resources); D. Gordon Smith, *The Critical Resource Theory of Fiduciary Duty*, 55 VAND. L. REV. 1399, 1402 (2002) ("[F]iduciary relationships form when one party (the 'fiduciary') acts on behalf of another party (the 'beneficiary') while exercising discretion with respect to a critical resource belonging to the beneficiary." (emphasis omitted)).

Fiduciary relationships also tend to be "especially difficult to monitor," making them particularly "susceptible to abuse."[168] And this, in turn, is why contract remedies are not enough, standing alone, to vindicate the normative purpose of fiduciary duties. The point of enforcing fiduciary duties is not only to make injured parties whole ex post, but it is *also* to deter "opportunism" and encourage "bonding" in ways that "facilitate a beneficiary's reliance on the trustworthiness of her fiduciary."[169] Put simply, legal structures are necessary to ensure that fiduciaries refrain from exploiting the considerable power that flows from their status vis-à-vis beneficiaries.

These rationales map straightforwardly onto the actors discussed so far in this Article. Not only are ISPs, for example, privy to large amounts of sensitive information, but monitoring what they do with that information is also difficult and costly, especially in the context of metadata and other "noncontent" information, which users often do not even *realize* they are transmitting.[170] This is not to say, of course, that users couldn't be made to shoulder the costs of monitoring. They certainly could. There is no reason, in principle, why service providers currently bound by fiduciary obligations—trustees, for example, or money managers—couldn't be bound, instead, exclusively by contractual obligations.[171] But that possibility misses the normative point. The whole purpose of imposing duties of care and loyalty on (traditional) fiduciaries is that market forces—as reflected in the outcomes of bargaining—do not lead, on their own, to a desirable allocation of cost and risk.[172]

---

168. Leib, *supra* note 163, at 683.

169. *Id.* at 683–84; *see also* Tamar Frankel, *Fiduciary Law*, 71 CAL. L. REV. 795, 824–25 (1983) (explaining that a key doctrinal feature of fiduciary law is burden-shifting: beneficiaries are "entitle[d] . . . to rely on the fiduciary's trustworthiness," meaning that in the event of a lawsuit, a beneficiary "is . . . not required to show that he *actually* relied on the fiduciary," but rather "the fiduciary has the burden of justifying self-dealing transactions").

170. *See, e.g.*, *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317 (3d Cir. 2013) (noting that, in the context of cell site data, "it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information").

171. *See, e.g.*, Frank H. Easterbrook & Daniel R. Fischel, *Contract and Fiduciary Duty*, 36 J.L. & ECON. 425, 427 (1993) ("Fiduciary duties are not special duties; they have no moral footing; they are the same sort of obligations, derived and enforced in the same way, as other contractual undertakings."); John Langbein, *The Contractarian Basis of the Law of Trusts*, 105 YALE L.J. 625, 629 (1995) (describing fiduciary obligations as "unambiguously contractarian" in nature). *But see* Deborah A. DeMott, *Beyond Metaphor: An Analysis of Fiduciary Obligation*, 1988 DUKE L.J. 879, 880 (1988) (concluding that in spite of the "elusive nature" of fiduciary duties, "descriptions drawn exclusively from contract principles are surely mistaken"); Scott Fitzgibbon, *Fiduciary Relationships Are Not Contracts*, 82 MARQ. L. REV. 303, 341–43 (1999) (exploring the shortcomings of the "contractualist" approach to fiduciary duties).

172. *See, e.g.*, Fitzgibbon, *supra* note 171, at 341 (exploring the ways in which "fiduciary affiliations serve different purposes than those known to [market-based] utilitarianism"); Selbst, *supra* note 103, at 681 (noting that there is a tendency in debates about privacy to conflate "the descriptive claim that the market [could] solve the problem" with "the normative claim that it should [do so]"); *see also* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK 158 (2007) (explaining why the "privacy market" tends not to operate efficiently—among other reasons, because "[w]e rarely have any real 'relationship' with the third-party entities

In other words, even if beneficiaries are theoretically *capable* of shouldering the costs necessary to monitor fiduciaries, the point is that they should not have to. Beneficiaries should be able to rely on the sturdiness of background legal rules designed to safeguard their interests; this is what enables beneficiaries to act *as though* they trust fiduciaries, even though, in the absence of legal rules, such "trust" would be unwarranted. This sort of "virtual trust" serves a variety of functions. Perhaps most importantly, it facilitates candid interaction, which, in the context of something like medical care or legal assistance, can be paramount to successful outcomes and, in the context of digital correspondence, allows social life to proceed organically, without constant fear of disruption. In short, fiduciary duties relieve us of the burden of determining who, among a particular class of counterparties, is actually trustworthy; in doing so, they help preserve the integrity of social life.[173]

There are, to be sure, some conceptual difficulties that arise in trying to import fiduciary principles to the Fourth Amendment setting. But those difficulties are no greater than—and indeed, they ultimately reflect—the internal tensions of fiduciary law. As Ethan Leib has shown, many, if not all, of the justifications behind traditional fiduciary duties apply just as readily (perhaps even more readily) to intimate relationships. Although we are accustomed to thinking about fiduciary duties in the context of arm's length transactions, there is no reason in principle why the same logic—justifying the use of state power to enforce implied obligations—should not apply, for example, to promises made by friends. For Leib, then, the proper doctrinal test for assessing duties of care, loyalty, and confidentiality would be functional, not formal, in nature. It would ask whether a given relationship "trade[s] upon high levels of trust and leave[s] one party in a position of domination, inferiority, or vulnerability."[174] If so, that relationship should enjoy special solicitude.[175] Indeed, in certain domains, the doctrine already takes this sort of functionalist approach to fiduciary-style obligations—for example, when it ascribes implied duties of confidentiality to parties that hold themselves out as promising to keep sensitive information in confidence[176] or implied duties of loyalty to parties that maintain an ongoing course of dealing.[177]

---

that acquire our information, possess virtually no bargaining power over them, are often ignorant of or confused about the third party's privacy 'offer,' and in any event frequently have no way to opt out of or fine-tune the 'contract'"); Anderson, *supra* note 114, at 13–14 (explaining the "preposterous[]" way that "law treats our acquiescence [to form contracts] as if we had bargained with the entity and reached a mutually agreeable solution").

173. *See supra* note 132.

174. Leib, *supra* note 163, at 672.

175. *See id.* at 700–20 (especially pages 707–10).

176. *See, e.g.*, Woodrow Hartzog, *Reviving Implied Confidentiality*, 89 IND. L.J. 763, 777–80 (2014) (documenting the salience of (1) underlying trust between the parties, and (2) social custom in the jurisprudence of implied confidentiality).

177. *See* 68 C.J.S. *Partnership* § 11 (2009) ("A partnership arises from express or implied agreement among parties . . . ."). For an example of what this standard means in practice, see *Chenault v. Jamison*, 578 So. 2d 1059, 1060 (Ala. 1991) (explaining that, if one party to

Leib's insight is an important one. And the problem he highlights—a problem for the law of fiduciary duties writ large—is particularly pronounced in the Fourth Amendment context. After all, many of the variables that counsel in favor of treating doctors, hotel staff, or ISPs as information fiduciaries also counsel in favor of treating friends, family members, and other intimates the same way. By way of explaining why my doctor occupies a fiduciary status, for example, I might invoke the experience (which most of us undoubtedly share) that when I entrust sensitive information to a doctor, I do not expect that she will betray me. I *feel* as though I am telling my doctor something in confidence. But of course the same is likely to hold true when I tell my friend, sibling, spouse, or colleague something sensitive. Indeed, it will be the rare case of disclosure—to any counterparty—when I expect the person to disseminate the relevant information to others behind my back.

Yet there would be something seriously wrong with a Fourth Amendment rule that disallowed, for example, supervisors or coworkers from reporting illegal activity at work. And there would be something even *more* seriously wrong with a rule that stopped coconspirators from deciding to withdraw from inchoate criminal activity[178] or that prohibited friends and family members, for example, from cooperating with law enforcement in circumstances where they felt impelled—for reasons of conscience or out of concern for their own safety—to do so.

Adopting rules like this—rules that effectively extend Fourth Amendment protection to all voluntary cooperation with law enforcement—would devastate the criminal justice system. Defendants would always be able to assert an interest in, and potentially forestall or suppress, the (incriminating) testimony of other parties. All evidence procured from common areas—homes, cars, offices, computers, and so on—would arouse Fourth Amendment scrutiny.[179] Consider the

---

a putative partnership is "led to believe . . . that [the other party] intended to be a partner," that can be sufficient for the partnership to form).

178. *See* United States v. Huber, 404 F.3d 1047, 1054 (8th Cir. 2005) (declining to apply Fourth Amendment scrutiny to a bookkeeper's decision to testify for the prosecution on the grounds, inter alia, that the bookkeeper should be free to "protect[] herself" from prosecution). This commitment is also reflected in, among other places, the "withdrawal" defense in conspiracy law—which allows a coconspirator to escape liability if he can show that he took material steps to withdraw from the effort before the commission of the offense—and the "coconspirator" exception to the rule against hearsay. *See* FED. R. EVID. 801(d)(2)(E) (a statement is not hearsay if it "is offered against an opposing party and . . . was made by the party's coconspirator during and in furtherance of the conspiracy"); *see also* Neal Kumar Katyal, *Conspiracy Theory*, 112 YALE L.J. 1307, 1330–31 (2003) (explaining that the legal system's facilitation of betrayal among coconspirators originated in common law immunity doctrine and was designed to ensure that "so long as the . . . witness made a good faith effort to assist the prosecution he would go free"); *id.* at 1331–32 (explaining, in a similar vein, that "the law of contracts . . . rightly refuses to enforce agreements that prevent conspirators from defecting").

179. *See* Coolidge v. New Hampshire, 403 U.S. 443 (1971); United States v. Bowers, 594 F.3d 522, 525–27 (6th Cir. 2010) (holding that it was a purely private search when defendant's roommate and her boyfriend entered defendant's room, removed a photo album, and gave it to the police). Naturally, many fact patterns that involve searches by roommates,

implications of such a world! Uncertainty would loom over every investigation. The history of virtually *all evidence* introduced against a given defendant would be cast into doubt and amenable (theoretically, at least) to a Fourth Amendment challenge. Criminal investigations would grind to a halt. In short, there are good reasons to leave private actors free, in general, to betray one another to law enforcement on pragmatic grounds certainly, but even on normative grounds. People in possession of incriminating information about others should have autonomy to use the information as they see fit.[180]

The notion of "counterparty autonomy" is important here because it circles back to the issue of practically involuntary, arm's length entrustment discussed above. What distinguishes Fourth Amendment fiduciaries (to whom the misplaced trust rule does not apply) from everyday counterparties (to whom it does) is not expectations of confidence; it is relative power. When it comes to doctors, hotel staff, and ISPs—to name but a few examples of counterparties that fall into the fiduciary category—the decision to share information, though not formally mandatory, is practically inescapable. As such, the same anxieties about "opportunism" and "suscepti[bility] [to] abuse" that define traditional fiduciary relationships apply in this setting as well.[181] If anything, they apply even more urgently, given the severe consequences that can flow from law enforcement investigation (whether or not one is ultimately convicted). In light of these concerns, the answer, just as in traditional fiduciary relationships, is to limit the autonomy of certain parties to direct the flow of information—to law enforcement, in particular—as they see fit.

Beyond shoring up the distinction between Fourth Amendment fiduciaries and other counterparties, the emphasis on counterparty autonomy also serves another important goal: it helps explain the origin, in the first instance, of the misplaced trust rule in Fourth Amendment law. Although the principle has long been a fixture of doctrine (hence the discussion in Part I), its rationale has gone oddly unelaborated. Indeed, it would hardly be an exaggeration to say that the "expectations of privacy" framework, standing alone, provides *no* rationale for the misplaced trust rule. Normally, when *A* shares information with *B*, *A* does not expect—and sometimes, *A precisely* does not expect—that the information will travel further.[182] Yet the Fourth Amendment allows *B* (at least as a default rule)

---

spouses, and houseguests never even rise to the level of Fourth Amendment scrutiny because they are so clearly outside the bounds of constitutional protection.

180. *See supra* note 112 (discussing Supreme Court language to this effect); *see also* ABA STANDARDS, *supra* note 6, at 39 (explaining that, as a matter of presumption, "an individual"—that is, a counterparty—"has an autonomy and free speech interest in choosing to share information that will often trump any privacy interest" on the part of the sharing party).

181. *See supra* notes 167–69 and accompanying text.

182. Sherry Colb has documented this issue eloquently and at greater length. *See* Colb, *supra* note 11, at 127–44 (documenting the fallacy that runs through much of the Supreme Court case law of "equating risk [with] invitation"). Indeed, not only does *A*, when disclosing information to *B*, not typically expect that disclosures will travel further than *B*, but there are also likely to be likely to be circumstances in which the opposite inference is

to transmit the information as *B* sees fit, notwithstanding *A*'s expectations. Why? Counterparty autonomy supplies a full answer to this question. Generally speaking, *B* should be able to cooperate with law enforcement because *B* has an interest in doing so. Unless *B* has a specific obligation *not* to transmit *A*'s information—that is, unless *B* is an information fiduciary—*B* should be able to direct the flow of information in her possession.[183]

At last, then, the big question is, which counterparties *are* Fourth Amendment fiduciaries? So far, the Article has offered three examples: doctors, hotel staff, and ISPs that facilitate digital correspondence. Who else belongs in the category? First, following Chris Slobogin and others, I would draw a categorical line—at least for the purpose of establishing default rules—between individuals and institutions.[184] When it comes to individuals, autonomy over information—the ability to dispose of information as one pleases—is central to "personhood."[185] In Slobogin's words, "the autonomy interest of a putative witness trumps the privacy interest of a . . . target [of investigation]," because "no person should be able to prevent another from providing information to the government."[186] Crucially, however, "that analysis"—emphasizing the relationship between informational autonomy and personhood—"makes sense only when the third party *is a person*," not an institution.[187] Why? Because "[a] bank,

more plausible—that *A*, by disclosing information exclusively to *B*, expected the disclosure to *limit* the ultimate flow of information. Suppose, for example, that *A* has committed adultery and his wife is starting to get suspicious. *A* tells his best friend, *B*, about the adultery and asks for *B*'s help in brainstorming a way to ensure that their other friends—and most especially, *A*'s wife—don't find out. Under circumstances like this, it would be ludicrous to conclude that because *A* confided in *B*, *A* can no longer expect that his adultery will stay under wraps: that is *precisely* what *A* expects.

183. A similar point can be made about the private search doctrine. One reason we might protect *B*'s ability to investigate *A*—and, if desired, to relay the results of the investigation to law enforcement—is that *B* has an interest in doing so. In fact, the private search doctrine is almost impossible to rationalize on expectation of privacy grounds. Who expects that a package sent via FedEx will be dismantled by an employee (purposefully or not) and its contents brought to the attention of law enforcement? Who expects that his computer will be hacked—itself an illegal act—by an anonymous vigilante keen on unearthing child pornography? Under an "expectations of privacy" metric, these holdings are scandalous. But reconceived in terms of counterparty autonomy, they make sense (whether they are rightly decided is quite another matter).

184. *See* SLOBOGIN, *supra* note 172, at 157–60; Bryan H. Choi, *For Whom the Data Tolls*, 37 CARDOZO L. REV. (forthcoming 2015), http://ssrn.com/abstract=2576948 [http://perma.cc/6SK7-FVRR]; Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 CAL. L. REV. 1593, 1643 (1987) (arguing that people have "an autonomy-based right to choose to cooperate with the authorities"); *see also* ABA STANDARDS, *supra* note 6, at 39 (distinguishing, in broad strokes, between the autonomy interests of persons and the attenuated autonomy interests of "[i]nstitutional third parties").

185. SLOBOGIN, *supra* note 172, at 159; *see also* Coombs, *supra* note 184, at 1642–44 (identifying personhood as the normative rationale for "betrayal" in Fourth Amendment law).

186. SLOBOGIN, *supra* note 172, at 159.

187. *Id.* (emphasis added).

hospital, or ISP is not denied 'personhood' when its ability to turn information over to the government is restricted."[188]

Of course, to say that institutions, generally speaking, have no autonomy interest in the information entrusted to them does not mean (1) that *only* institutions are in this position, or (2) that institutions *never* have an interest—of a normatively relevant sort—in cooperating with law enforcement. Neither proposition is true. To begin with, it is certainly not the case that all information fiduciaries are institutions. Many flesh-and-blood individuals—with whom we transact at arm's length, usually for particular services—play that role as well. Whether they do so depends on the nature of the particular relationship, but the familiar criteria govern. Doctors, lawyers, repairmen, financial advisors—all of these actors (and this is certainly not an exhaustive list) are information fiduciaries to the extent that we entrust information to them for reasons that have nothing to do with "trust," in the everyday sense. Rather, we entrust information to these counterparties because doing so has instrumental value—in spite of, not because of, the fact that we have no basis to assume they will safeguard our information. For the reasons discussed above, there are good reasons to conclude that practically involuntary, arm's length entrustment carries an implicit limitation on use: specifically, an implied covenant to avoid using sensitive information in ways that harm the sharing party.

Moreover, even if institutions—and individuals that play a fiduciary role—lack an *autonomy* interest in sharing information with law enforcement, it does not follow that they have *no* interest in sharing information with law enforcement. Interests take many forms. It seems uncontroversial, for example, that companies should be able to share information with law enforcement (even companies that otherwise operate as information fiduciaries) if they reasonably fear that adverse consequences will flow from not doing so.

For example, if a company can show that the persistence of a customer's (or a user's) criminal activity poses a risk of legal liability for the company, it should be able to cooperate with law enforcement. For instance, a case like *Stoner* would presumably be different—and I think it *should* be different—if the hotel room in question were being used to operate a criminal enterprise, rather than storing nonhazardous contraband.[189] Under those circumstances, the hotel manager might able to convincingly argue that the criminal enterprise was exposing *the hotel* to potential liability, in which case cooperation with law enforcement would certainly be warranted. The Fourth Amendment does not require businesses to subordinate their own legal standing to the privacy interests of their customers.[190] The same

188. *Id.*

189. *See* Lewis v. United States, 385 U.S. 206, 211 (1963) (holding that a homeowner relinquished his reasonable expectation of privacy when he used his home to run an illegal venture). Presumably, what is true of expectations of privacy in one's home would also be true, a fortiori, of expectations of privacy in one's hotel room.

190. *Cf.* Couch v. United States, 409 U.S. 322, 335 (1973) (holding that it does not violate a defendant's self-incrimination rights for the government to subpoena records from the defendant's accountant, because, among other reasons, an accountant's "own need for

reasoning also applies to economic concerns. If a company can show that a customer's (or a user's) criminal activity poses a detrimental risk to business, this, too, might justify cooperation with law enforcement—though probably subject to a more stringent evidentiary burden than claims of imminent criminal or civil liability.[191]

By the same token, it does *not* qualify as an objectively reasonable concern about adverse legal or economic consequences for an institution (or individual) to claim an overarching interest in "aiding . . . in the apprehension of criminals."[192] That interest is shared by everyone, equally, whether or not they operate in a fiduciary capacity. At some level, in fact, the public's general interest in "aiding . . . the apprehension of criminals" is indistinguishable from the autonomy interest that nonfiduciaries have in disposing of information as they see fit. One of the reasons we safeguard the ability of private actors to betray one another—apart from the practical mayhem that the opposite rule would create—is that individuals, as members of the public, have an interest in seeing wrongdoing redressed.[193] The same is not true of information fiduciaries. Crucially, this is *not* because it is impossible (or even unlikely) that information fiduciaries wish to see wrongdoing redressed. It is because information fiduciaries are not empowered to act on that wish. Surely there are many doctors—and hotel managers, and ISPs, and so forth—who, when left to their own devices, would very much prefer to cooperate with law enforcement. The point is that their preferences are not the salient variable. Our privacy is.[194]

---

self-protection [against criminal prosecution] . . . often require[s] the right to disclose the information given him").

191. Something of this has already surfaced in the doctrine—though in an under-theorized way—when courts ask if private searches were motivated by legitimate business interests. *See, e.g.*, United States v. Bowers, 594 F.3d 522, 526 (6th Cir. 2010) (holding that a search, to be private, must serve a purpose "*entirely independent* of the . . . collect[ion] [of] evidence for use in a criminal prosecution" (quoting United States v. Hardin, 539 F.3d 404, 418 (6th Cir. 2008))); United States v. Attson, 900 F.2d 1427, 1431 (9th Cir. 1990) (holding that private searches are only private if their purpose is related to business activity, *not* "to elicit a benefit for the government in either its investigative or administrative capacities"). Doctrinally, the standard is fuzzy partly because of its sheer logical indeterminacy. Courts have not been clear as to whether the absence of a legitimate business *condemns* a search, or, instead, whether the presence of a legitimate business interest *justifies* a search (or something in between). In any event, it seems safe to conclude that courts should look on claims of "business interests" with some degree of skepticism, given how easy it is to speculate about economic loss.

192. Georgia v. Randolph, 547 U.S. 103, 116 (2006) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 488 (1971)).

193. Though in particular cases, of course, there may well be other considerations, such as personal safety, that contribute to an individual's autonomy interest. This concern is front and center in the cotenancy cases. *Compare id.* at 121–22 (holding that if both cotenants are present, and one invokes his Fourth Amendment rights, that invocation trumps the other's consent), *with* Fernandez v. California, 134 S. Ct. 1126, 1134–35 (2014) (holding that the consent of a cotenant sufficed to justify a search after the other tenant (1) had invoked his *Randolph* rights, but (2) had been removed from the premises). With respect to the latter, in particular, Justice Alito's opinion for the Court includes numerous rhetorical flourishes about the importance of leaving law enforcement free to aid victims of domestic violence.

194. Under the framework set forth here (with its emphasis on the institution-individual divide), the hardest cases are likely to be those that involve *agents* of information

CONCLUSION

In the digital age, reforming Fourth Amendment law requires more than just pruning back an isolated site of doctrinal overgrowth from the late 1970s—overgrowth so extreme that even its enthusiasts do not seem to take *Smith* and *Miller* at face value.[195] How could they? The notion that people "[have] no reasonable expectation of privacy in information voluntarily disclosed to third parties"[196] runs directly into *Katz*, and the conceptual edifice devised to explain this tension away—the distinction between "content" and "noncontent" information—has been exposed as a house of cards. Jurisprudentially, *Jones* and *Riley* portend the end of the so-called "third-party doctrine." And conceptually, the doctrine has been something of a mirage all along.

Good riddance—for there are larger monsters to slay. Data is quickly becoming the main currency of law enforcement, and in a world of substantial—and growing—intermediation, our data is less and less our own. To keep clip with these developments, Fourth Amendment law must begin to think differently about collaboration between law enforcement and

---

fiduciaries—like employees—who, as individuals, do not have fiduciary obligations to the sharing party, but who nonetheless operate under the auspices of a fiduciary bond. Hotel managers and doctors pose few, if any, difficulties in this respect, because these actors, despite being individuals, *do* have independent fiduciary obligations to primary parties. The same considerations that would make it troubling for a hospital to maintain a blanket policy of cooperating with law enforcement also make it troubling for a doctor to cooperate with law enforcement in a less systematic way (and likewise, the same considerations that make it troubling for a hotel, as an institution, to betray guest information to law enforcement also make it troubling for a hotel manager to do the same).

But consider the following hypothetical. *B*, a Google engineer, is performing run-of-the-mill maintenance when he notices strange traffic patterns through *A*'s Gmail account. His curiosity piqued, *B* decides to investigate—and lo and behold, *A* has been transmitting child pornography. Under the fiduciary model, *Google's* cooperation with law enforcement certainly triggers (some degree of) Fourth Amendment scrutiny. But what about *B*'s cooperation with law enforcement? There are three possible answers. First, *B*'s cooperation might *always* trigger Fourth Amendment scrutiny—because *B*-the-individual is, in effect, an extension of Google-the-institution. Second, *B*'s cooperation might *never* trigger Fourth Amendment scrutiny—if we think about *B* as an individual with autonomy interests intact. Third, *B*'s cooperation might *sometimes* trigger Fourth Amendment protections, depending on whether *B* was acting in a formal or informal capacity, on Google's behalf or not.

Normatively, this last answer is probably the most attractive (as middle positions often are), but its doctrinal plausibility remains to be seen. *See* United States v. Jacobsen, 466 U.S. 109, 126 (1984) (holding that no Fourth Amendment scrutiny is triggered by a FedEx worker's decision to search the contents of a package broken while in transit and to turn discovered contraband over to law enforcement). The "Google engineer" hypothetical provides an exact analogy to *Jacobsen* in the digital age. Without purporting to resolve the puzzle here, suffice it to note that the result in *Jacobsen* may well have come out differently—and it almost certainly would have been *analyzed* differently—if the "private search" had been pursuant to a FedEx-wide policy to scan and, if necessary, dismantle all packages that flow through the FedEx system. *See* Kiel Brennan-Marquez, *Vigilantes and Good Samaritans*, 18 U. PA. J. CONST. L. (forthcoming 2015), http://ssrn.com/abstract=2657789 [http://perma.cc/G7SE-BAY5].

195. *See supra* note 28.

196. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (summarizing the third-party doctrine, as traditionally understood); Smith v. Maryland, 442 U.S. 735, 742–43 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).

the private sector. Traditionally, the rule has been that sharing information, no matter with whom, invites the danger of misplaced trust. But looking forward, that rule no longer makes normative sense. Nor, looking backward, has the rule given rise to consistent application. When the chips are down, the Supreme Court has refused to extend the misplaced trust rule to settings where it clashes with social reality. Digital communication is the most recent—and in today's world, the most practically pressing—example of such a setting.

The point of this Article is ultimately quite simple. In settings where private actors operate as information fiduciaries, law enforcement should not have carte blanche to demand their cooperation; nor should private actors that serve as information fiduciaries be free—without bound—to assist law enforcement voluntarily. Today, we live alongside sprawling organizations whose purpose, and profit, is fundamentally tied to their use of information. *Our* information. Doctrine must adapt to this reality. It must learn to distinguish between sharing at arm's length—which occurs as the precondition of obtaining a socially valuable service—and sharing with counterparties who are genuinely *trusted* and whose involvement thereby gives rise to a risk of misplaced trust. This distinction, like so many that law confronts in the face of technological change, is at once conceptually lucid and doctrinally precarious. Is Fourth Amendment law up to the task? Let us hope so. The future of constitutional privacy depends on it.