The Constitutional Limits of Private Surveillance

Kiel Brennan-Marquez[*]

[*] Associate Professor, University Connecticut School of Law (appointment to begin August 2018). For indispensable feedback on earlier drafts, I would like to thank Caroline Alewarts, BJ Ard, Jane Bambauer, Bethany Berger, Thomas Brennan-Marquez, Sarah Carroll, Julie Cohen, Andrew Ferguson, Barry Friedman, David Gray, Greg Klass, Will Havemann, Stephen Henderson, Shelly Layser, Yafit Lev-Aretz, Jonathan Manes, Helen Nissenbaum, Paul Ohm, Ira Rubinstein, Andrew Selbst, Mike Shih, Chris Slobogin, Kathy Strandburg, Andrew Tutt, Robin West, and Carly Zubrzycki. Special thanks are due to Will Kukin—without whom, this project may not have gotten off the ground—and to the students in the Spring 2017 Advanced Topics in Privacy seminar at NYU Law School, who indulged me in working out some of these ideas through the course material. I presented drafts of this article at the University of Connecticut, Georgetown, Kentucky, New York Law School, NYU, and Yale; all of these opportunities contributed to the article's ultimate form. Finally, my gratitude to the editors of the *Kansas Law Review*, who provided tremendous substantive edits and helped get the piece into publishable shape. Remaining errors are my own.

I. INTRODUCTION

As law enforcement becomes more data-driven,[1] its efficacy depends increasingly on private surveillance power.[2] Consider two recent examples. In 2013, *The New York Times* reported that in the early 2000's, AT&T built—in secret—a drug-focused communication surveillance system called Hemisphere.[3] The size of Hemisphere is staggering. By some estimates, AT&T adds four billion call records to the system *per day*, making it one of "the largest known reservoirs of communications metadata" in existence, and one of the state's most potent law enforcement tools.[4] Similarly, in 2016, it came to light that Geofeedia, a private "Location-based Analytics Platform,"[5] had been (consensually) siphoning data from Twitter, Facebook, and Instagram—and repackaging it to help police departments around the country keep tabs on protestors and activists.[6]

These are hardly isolated examples. Others include: internet service providers ("ISPs") screening email, en masse, for contraband;[7] financial firms analyzing transaction patterns for signs of fraud;[8] data brokers

---

1. For background, *see* Andrew Ferguson, *Policing Predictive Policing*, 94 WASH. U. L. REV. 1115, 1115–18 (2017); Elizabeth Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 35–39 (2014).

2. *See generally* Alan Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99 (2018) (analyzing the rise of "surveillance intermediaries," i.e., the large technology companies responsible for amassing the data eventually used for government surveillance today).

3. *See* Colin Moynihan & Scott Shane, *Drug Agents Use Vast Phone Trove Eclipsing N.S.A.'s*, N.Y. TIMES (Sept. 1, 2013), http://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html.

4. Adam Schwartz, *AT&T Requires Police to Hide Hemisphere Phone Spying*, EFF BLOG (Oct. 27, 2016), https://www.eff.org/deeplinks/2016/10/att-requires-police-hide-hemisphere-phone-spying.

5. This is Geofeedia's own description of its service. *See* GEOFEEDIA, www.geofeedia.com (last accessed on Jan. 21, 2018).

6. *See, e.g.*, Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, ACLU BLOG (Oct. 11, 2016), https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.

7. *See* Robyn Burrows, *Judicial Confusion and the Digital Drug Dog Sniff: Pragmatic Solutions Permitting Warrantless Hashing of Known Illegal Files*, 19 GEO. MASON L. REV. 255, 261 (2011); Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 39 (2005).

8. One prominent example is private companies that assist the government in detecting healthcare fraud, an industry that has ballooned in recent years, given the explicit mandate within the Affordable Care Act to expand the digitization, collection, and storage of healthcare data. *See* David Gray et al., *Fighting Cybercrime After* United States v. Jones, 103 J. CRIM. L. & CRIMINOLOGY 745, 766–67 (2013). *See also* CTRS. FOR MEDICARE AND MEDICAID SERVS., DEP'T OF HEALTH & HUMAN SERVS., REPORT TO CONGRESS: FRAUD PREVENTION SYSTEM—FIRST IMPLEMENTATION YEAR 4 (2012), https://www.cms.gov/About-CMS/Components/CPI/Widgets/Fraud_Prevention_System_

compiling vast dossiers of "publicly available" information for sale to law enforcement agencies;[9] and computer technicians hunting for child pornography in the course of performing repairs.[10] Going forward, furthermore, practices like these are only likely to intensify.[11] As data analysis subsumes an ever-greater share of traditional police work, the boundary dividing the private intermediaries that collect, store, and curate data from the law enforcement institutions that "insource" data for investigative purposes is liable, if anything, to blur further.[12]

The fusion of private surveillance and public law enforcement is not necessarily lamentable. Indeed, it has many benefits. But from a Fourth Amendment perspective, the fusion raises two related puzzles. The first, which has inspired copious scholarship,[13] and will be addressed by the

---

Report_toCongress-1stYear.pdf ("CMS partnered with industry-leading private-sector contractor teams to adapt existing telecommunications and banking industry anti-fraud technology to the unique requirements of fighting Medicare fraud."). Overall, the upshot is that under federal law, Medicare carriers (typically private insurance companies) are permitted to audit Medicare providers' records, with the assistance of private contractors, to uncover fraudulent billing. *See, e.g.*, Anghel v. Sebelius, 912 F. Supp. 2d 4, 9 (E.D.N.Y. 2012). And while this practice clearly has social value, it also implicates privacy interests.

9. *See generally* 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). For a trenchant critique of the concept of "publicly available information," *see* Woodrow Harzog, *The Public Information Fallacy* (Ne. Univ. Sch. of Law Research Paper No. 309-2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3084102.

10. *See, e.g.*, Tom Jackman, *If a Best Buy Technician Is a Paid FBI Informant, Are His Computer Searches Legal?*, WASH. POST (Jan. 9, 2017) (exposing the fact that certain members of Best Buy's "Geek Squad" — its team of in-house computer technicians — had decided, of their own accord, to run searches for child pornography, and to shuttle their findings along to the FBI), https://www.washingtonpost.com/local/public-safety/if-a-best-buy-technician-is-a-paid-fbi-informant-are-his-computer-searches-legal/2017/01/09/f56028b4-d442-11e6-9cb0-54ab630851e8_story.html. The scope of Geek-Squad-vigilantism is currently unknown (and the subject of at least one Freedom of Information Act lawsuit), but preliminary evidence suggests that it has been ongoing for many years. *See also* Tom Jackman, *Records Show Deep Ties Between FBI and Best Buy Computer Technicians Looking for Child Porn*, WASH. POST (Apr. 3, 2017), https://www.washingtonpost.com/news/true-crime/wp/2017/04/03/records-show-deep-ties-between-fbi-and-best-buy-computer-technicians-looking-for-child-porn/; Aaron Mackey & Stephanie Lacambra, *Why We're Suing the FBI for Records About Best Buy Geek Squad Informants*, EFF BLOG (May 31, 2017), https://www.eff.org/deeplinks/2017/02/FBI-tries-to-bypass-Fourth-Amendment-Safeguards-by-using-Geek-Squad.

11. *See* ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT 2–19 (2017).

12. *See* Kimberly N. Brown, *Outsourcing, Data Insourcing, and the Irrelevant Constitution*, 49 GA. L. REV. 607, 609–15 (2015) (exploring the ways in which outsourcing of government functions, paired with "data insourcing" by state agencies, permits the circumvention of various regulatory mechanisms, including constitutional rules).

13. *See* Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 639–44 (2015) (compiling sources). Another issue that deserves further attention — but differs slightly from the use of warrants to obtain data — is the government's conscription of help from private companies in carrying out investigations. A recent example of this was the widely publicized

Supreme Court this term in *Carpenter v. United States*,[14] is the compulsory seizure of data. When must state officials show probable cause (and presumptively, obtain a warrant) before obtaining "third-party records"? The second puzzle, which has received remarkably little attention,[15] is voluntary data-sharing between and law enforcement and the private sector. How should the Constitution respond when, as in the examples above, private companies decide—free of any legal obligation—to collect user data and funnel the results to the state?

In response to the problem of voluntary data-sharing, current doctrine focuses on the degree of governmental influence over initial collection. The Fourth Amendment reaches private surveillance, the logic goes, only insofar as the surveillance was deputized by state officials ex ante.[16] If not, the surveillance is not a "search," so no Fourth Amendment scrutiny applies; full stop. In other words, *regardless* of whether a private surveillance practice runs afoul of reasonable expectations of privacy—even assuming, arguendo, that it does—the Fourth Amendment imposes no limits of any kind.[17] The practice is exempt from any analysis regarding "reasonableness," no matter how totalizing, pervasive, or far-reaching it becomes.

My claim here is simple: the deputization framework is unresponsive to the realities of data-sharing today. In an age of "handshake agreements" between law enforcement agencies and information companies,[18]

---

tug-of-war between Apple and the FBI, over the unlocking of a smartphone that was suspected to contain evidence related to the San Bernardino terror attacks in 2015. For further background on the question of unwarranted-but-compulsory assistance, see Ian Samuel, *The New Writs of Assistance*, FORDHAM L. REV. (forthcoming) (manuscript on file with author).

14. For excellent background on the issues presented in *Carpenter*, *see* Stephen E. Henderson, *Carpenter v. United States and the Fourth Amendment: The Best Way Forward*, 26 WM. & MARY BILL RTS. J. (forthcoming 2018), https://ssrn.com/abstract=2994369.

15. There are a few exceptions. *See e.g.*, Kiel Brennan-Marquez, *Outsourced Law Enforcement*, 18 U. PA. J. CONST. L. 797 (2016); Eugene L. Shapiro, *Governmental Acquiescence in Private Party Searches: the State Action Inquiry and Lessons from the Federal Circuits,* 104 KY. L. J. 287 (2016); Elizabeth E. Joh, *The Paradox of Private Policing*, 95 J. CRIM. L. & CRIMINOLOGY 49 (2004); David A. Sklansky, *The Private Police*, 46 UCLA L. REV. 1165 (1999).

16. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 115 (1984) (explaining that private searches do not trigger the Fourth Amendment unless the private actor was operating as an agent or instrument of law enforcement at the time of the disputed conduct); Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971) (same). For a fuller discussion of the facts and holdings in these—and other—private search cases, *see infra* Part II.A.

17. *See, e.g.*, Jacobsen, 466 U.S. at 115 (Because "the initial invasions of respondents' package were occasioned by private action. . . . [*w*]*hether those invasions were accidental or deliberate, and whether they were reasonable or unreasonable*, they did not violate the Fourth Amendment because of their private character" (emphasis added)).

18. Rozenshtein, *supra* note 2, at 2–5. *See also* Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1338 (2012) [hereinafter Ohm, *The Fourth Amendment*] (envisioning a "coming world" in which "police outsource [almost all] surveillance to private third

privately-collected data often finds its way into governmental hands through informal channels of cooperation: initiatives either spearheaded, in the first instance, by the companies themselves, or developed in tandem with state officials but absent any legal compulsion.[19] When this happens—when companies serve, in effect, as the "first line of offense" for policing and counterterrorism[20] —the question should not be whether the state has directed private surveillance. Instead, what matters in practice, and what should guide the doctrine, is whether private surveillance *effects an extension of law enforcement infrastructure into the private sphere*. When the answer is yes, Fourth Amendment protection should extend likewise.[21]

Refocusing the inquiry on infrastructure—on how the surveillance ecosystem, with its combination of public and private elements, actually operates—offers a host of benefits over the status quo. I identify four.

First, the infrastructural view explains existing law better than existing law explains itself. The Supreme Court's focus on deputization is not entirely misguided. But the Court has drawn the wrong lesson. Deputization matters because it *produces* an extension of infrastructure, not because it exhaustively captures the harm of private surveillance. The deputization framework, in other words, confuses a sufficient condition for a necessary one; private surveillance practices directed by the state are a subset, but not the entirety, of those that demand Fourth Amendment scrutiny. In fact, the Court came close to acknowledging this point in *Skinner v. Railway Labor Executives' Association*, a case about urine testing of employees by private railway companies.[22] Superficially, *Skinner* presents as a cut-and-dry application of the deputization framework. Probe a little deeper, however, and this rationale unravels. *Skinner* cannot plausibly rest on deputization principles. Rather, it is the Court's first, albeit sub silentio, "extended infrastructure" case.

---

parties," and the Constitution "cast[s] much more scrutiny than it does today on how the private choices of private actors can disrupt this balance of power."); Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 904 (2008) (documenting the rise of informal private surveillance).

19. As for the former, examples include email-hashing by ISPs or analysis of social media data to monitor protest activity—and as for the latter, examples include AT&T's construction of Hemisphere (in tandem with drug enforcement authorities) and private health insurers' development of fraud-detection technology and protocols (in tandem with HHS). *See supra* notes 3–11 and accompanying text.

20. *See generally* Brennan-Marquez, *supra* note 15.

21. This does not mean, of course, that private actors should be forbidden from extending law enforcement infrastructure. It simply means that there are limits—rooted in the Fourth Amendment's requirement of "reasonableness"—to what forms the extensions may take. *See infra* Part III.

22. Skinner v. Ry. Labor Exec. Ass'n, 489 U.S. 602, 614–15 (1989).

Second, the infrastructural view connects the Court's private search cases, including *Skinner*, to broader patterns of state action jurisprudence. To date, there have been two settings—elections and property-attachments—in which the Court has recognized that voluntary private actors can significantly alter public infrastructure, calling for constitutional limits on private conduct. The same concerns, we will see, apply to law enforcement.

Third, the infrastructural view is normatively desirable; it captures the actual stakes of private data surveillance today. The reason we worry about unconstrained surveillance power—just as the Founders worried about unconstrained surveillance power, in the guise of general warrants[23]—is that a polity subject to constant monitoring cannot engage in effective self-governance. The danger of indiscriminate surveillance, in other words, is the erosion of individual autonomy and, ultimately, democracy itself.[24] In light of this, it matters little—often, not at all—if the genesis of indiscriminate surveillance is (1) direct state action, (2) private action directed by the state, or (3) voluntary private action that yields an expansion of state surveillance power. All three, when left unchecked, threaten the integrity of social life. The infrastructural view speaks to this reality in a way that current doctrine, focused solely on deputization, cannot.

---

23. For a fuller discussion of this point, see *infra* Part I. *See also* Maryland v. King, 133 S. Ct. 1958, 1980–82 (2013) (Scalia, J., dissenting) (documenting copious authority for the proposition that general warrants were the Fourth Amendment's specific target during the Founding Era); Messerschmidt v. Millender, 132 S. Ct. 1235, 1253 (2013) (Sotomayor, J., dissenting) (arguing that the paradigmatic deprivation of security—against which the warrant requirement and the ban on unreasonableness searches and seizures strove to protect—was the "Crown's practice of using general warrants and writs of assistance to search 'suspected places'"); Andresen v. Maryland, 427 U.S. 463 (1976) (explaining that "[g]eneral warrants are especially prohibited by the Fourth Amendment[,]" and that "the problem to be avoided is 'not that of intrusion [p]er se, but of a general, exploratory rummaging in a person's belongings.'"); Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. IN BRIEF 1, 10 (2011) [hereinafter Ohm, *Massive Hard Drives*] ("The Supreme Court has repeatedly explained that the Fourth Amendment's particularity requirement arose, at least in part, from the founders' concerns about British writs of assistance, general warrants issued by the king permitting soldiers to look in homes and places of business with few restrictions."); *id*. n. 37 (compiling sources); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 123–24 (2008) ("The Fourth Amendment was enacted above all to forbid 'general warrants.'"); Christopher Slobogin, *Government Dragnets*, 73 LAW & CONT. PROBS. 107, 107 (2010) ("The Fourth Amendment to the United States Constitution (and perhaps even the United States itself) exists because the American colonists abhorred the suspicionless house-to-house searches visited upon them by government officials armed with so-called 'general warrants.' . . . They were so despised by some segments of the colonies that they are said to have been a major cause of the Revolutionary War."); Scott E. Sundby, *Protecting the Citizen "Whilst He is Quiet": Suspicionless Searches, "Special Needs" and General Warrants*, 74 MISS. L. J. 501, 509 (2004) (suggesting that the "concern over general warrants . . . suppl[ies] a theoretical and historical underpinning" for Fourth Amendment law).

24. *See infra* Part I.

Finally, and most importantly, the infrastructural view underscores the connection between compulsory data seizures—whereby the state, using instruments like Section 2703 orders,[25] extracts from private companies data it would have difficulty collecting itself—and informal data-sharing, which requires no such extraction but can easily lead, in practice, to the same result. Scholars and advocates have long criticized the way that warrantless data extraction, enabled by the so-called "third party doctrine," tears a hole in the Fourth Amendment's fabric.[26] But the flip-side of extraction is *cooperation*. And unless both dynamics are addressed in tandem—unless they are recognized as substitute mechanisms, one formal, the other informal, for extending state surveillance infrastructure—the risk of partial victory looms large. Even if *Carpenter v. United States* delivers long-overdue reform of the third-party doctrine (an issue about which I am hesitantly optimistic[27]), it will mean rather little if the state is able to collect the same data through informal means. Indeed, the victory may be not only partial but Pyrrhic. A privacy-protective ruling in *Carpenter* could encourage state officials to rely even *more* on informal data-sharing than they currently do, leaving data privacy—and the democratic values it serves—in a position roughly as precarious as the

---

25. *See* 18 U.S.C. § 2703(a) (2012) (outlining the criteria whereby "[a] governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less . . . ."). The Fourth Amendment implications of Section 2703 orders (and similar instruments), understood through the prism of the third-party doctrine, is the central issue in *Carpenter v. United States*. For useful background, *see* Jennifer Lynch, *Symposium: Will the Fourth Amendment Protect 21st-century Data? The Court Confronts the Third-Party Doctrine*, SCOTUSBLOG (Aug. 2, 2017, 12:21 PM), http://www.scotusblog.com/2017/08/symposium-will-fourth-amendment-protect-21st-century-data-court-confronts-third-party-doctrine/.

26. *See, e.g.*, Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 40 (2011) (describing the doctrine as, among other things, "fundamentally misguided"); Neil Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1117–19 (2006) (explaining that a constitutional right to "decisional privacy" would resolve problems created by the third-party doctrine); Rubenfeld, *supra* note 23 at 109–115 (criticizing the notion, which Rubenfeld terms the "perfect stranger" principle, that all disclosures to a third-party are equivalent to exposing information to the entire world); Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 619–21 (2009) (suggesting that technological change has rendered the third-party doctrine untenable). *See also* Brennan-Marquez, *supra* note 13, at 639–44 (compiling other sources to the same effect). *See also* AM. BAR. ASS'N, STANDARDS FOR CRIMINAL JUSTICE: LAW ENFORCEMENT ACCESS TO THIRD-PARTY RECORDS 41–44 (3d ed. 2013), https://www.americanbar.org/content/dam/aba/publications/criminal_justice_standards/third_party_access.authcheckdam.pdf (drawing a sharp distinction between compelled v. voluntary private assistance of law enforcement, on the grounds that "purely private conduct" is beyond the Standards' purview).

27. I am not alone. On the scholarly front, see Henderson, *supra* note 14 (manuscript at 1) (expressing optimism about the likelihood of a protective—if somewhat narrow—ruling in *Carpenter*). And on the popular media front, see, for example, Jeffrey Rosen, *A Liberal-Conservative Alliance on the Supreme Court Against Digital Surveillance*, ATLANTIC (Nov. 30, 2017), https://www.theatlantic.com/politics/archive/2017/11/bipartisanship-supreme-court/547124/.

one created by the third-party doctrine itself.

Ultimately, then, the normative payoff of focusing on infrastructure is not limited to the Fourth Amendment's state action rules; though that is certainly my doctrinal focus here. The payoff of the infrastructural view is that it highlights, and would enable courts to respond to, a central feature of data-driven law enforcement. Namely, as long as data is collected and stored in the private sector, state officials will endeavor to capitalize on private surveillance infrastructure. Whether this happens by compulsion or, instead, by more informal means, the Fourth Amendment should—for the same reasons in both instances—have a constraining role to play.

II. THE HARMS OF (PRIVATE) SURVEILLANCE

To appreciate the importance of conceptualizing surveillance in infrastructural terms, first we must clarify the Fourth Amendment's purpose. What is wrong with unconstrained law enforcement power? By limiting such power, what types of harm does the Fourth Amendment strive to protect us against?

The question invites multiple, overlapping answers. For one thing, the Fourth Amendment shields us from undue disruption in everyday life. When the police perform *Terry* stops, or they pull people over on the road, or they enter private residences, or they examine the contents of luggage—and so on—the result is, at the very least, inconvenience, and often significantly more.[28] Stops can escalate.[29] Searches of the home, like burglaries, can feel profoundly intrusive. Without the Fourth Amendment in place to limit such practices, they risk becoming routine. Indeed, that

---

28. *See* Jane Bambauer, *Hassle*, 113 MICH. L. REV. 461, 487–90 (2014) (presenting "hassle"—that is, everyday forms of practical disruption and intrusion—as the focal point of Fourth Amendment harm, and compiling relevant sources). *See also* Paul Butler, *Stop and Frisk and Torture-Lite: Police Terror of Minority Communities*, 12 OHIO ST. J. CRIM. L. 57, 69 (2014) (arguing that much police activity is about detaining and harassing people—frequently, men of color—in public, to effect an ongoing a reminder of "who is in charge, and the violent consequences of dissent").

29. Dismayingly, the Supreme Court has actually *blessed* this dynamic, at least in the context of traffic stops. *See* Atwater v. City of Lago Vista, 532 U.S. 318, 354 (2001) (holding that an officer may perform an arrest, impound a vehicle, take a suspect into custody—and subject the suspect to all the accoutrement of being in custody, including compulsory DNA sampling and, depending on the context, strip-searches—as long as the "officer has probable cause to believe that an individual has committed even a very minor criminal offense[,]" including failing to properly use a seatbelt); Josh Bowers, *Probable Cause, Constitutional Reasonableness, and the Unrecognized Point of a "Pointless Indignity"*, 66 STAN. L. REV. 987, 995–1004 (2014) (exploring various normative rationales behind the *Atwater* rule). *See also* Kiel Brennan-Marquez & Andrew Tutt, *Offensive Searches: Toward A Two-Tier Theory of Fourth Amendment Protection*, 52 HARV. C.R.-C.L. L. REV. 103, 104–08 (2016) (criticizing the *Atwater* rule—and similar rules—on the grounds that the Fourth Amendment embeds baseline dignity norms).

is part of the recent pushback against programmatic stop-and-frisk tactics.[30] For the populations targeted by such tactics, disruption—coupled with an ever-present threat of escalation—becomes a normalized condition of life.[31]

For another thing, the Fourth Amendment requires law enforcement officials to give reasons for their actions.[32] This has many benefits. First, it helps ensure that state officials are targeting the "right" persons, places, and effects for investigation: those that are likely, relative to the general population, to be linked to wrongdoing.[33] Second, reason-giving facilitates governance. If officials did not have to explain their targeting decisions—if there were no particularized suspicion requirement—law enforcement would be a black-box, frustrating efforts by elected officials, citizen groups, and departmental higher-ups to address troubling practices.[34] Third, and most fundamentally, reason-giving respects the autonomy and dignity of suspects; it requires justifications for intrusion to be tied to a suspect's actual conduct, which serves as a bulwark (at least in theory) against bias and caprice.[35]

---

30. For particularly incisive criticism along these lines, *see generally* Tracey L. Meares, *Programming Errors: Understanding the Constitutionality of Stop-and-Frisk as a Program, Not an Incident*, 82 U. CHI. L. REV. 159 (2015); *see also* Butler, *supra* note 28, at 69. Of course, the other main pushback—interwoven with the problem of normalization—is racial bias.

31. *See* Meares, *supra* note 30, at 159 ("Although the constitutional framework is based on a one-off investigative incident, many of those who are stopped—the majority of them young men of color—do not experience the stops as one-off incidents. They experience them as a program to police them as a group, which is, of course, the reality."); Utah v. Strieff, 136 S. Ct. 2056, 2068–69 (2016) (Sotomayor, J., dissenting) (characterizing the practice of performing illegal stops to run checks for outstanding warrants—and taking advantage of the resulting "attenuation" for suppression purposes—as a routine practice of intrusion that should be forbidden by the Fourth Amendment); Floyd v. City of New York, 959 F. Supp. 2d 540, 557 (2013) ("No one should live in fear of being stopped whenever he leaves his home to go about the activities of daily life. Those who are routinely subjected to stops are overwhelmingly people of color, and they are justifiably troubled to be singled out when many of them have done nothing to attract the unwanted attention. Some plaintiffs testified that stops make them feel unwelcome in some parts of the City, and distrustful of the police."); Charles M. Blow, *The Whole System Failed Trayvon Martin*, N.Y. TIMES (July 15, 2013), http://www.nytimes.com/2013/07/16/opinion/the-whole-system-failed.html ("The idea of universal suspicion without individual evidence is what Americans find abhorrent and what black men in America must constantly fight").

32. *See* Kiel Brennan-Marquez, *"Plausible Cause": Explanatory Standards in the Age of Powerful Machines*, 70 VAND. L. REV. 1249, 1249 (2017).

33. *See id.* at 1249–50. Indeed, some commentators have gone so far as to suggest that achieving a desirable precision rate (true-positive to false-positive ratio) for police intrusion is the central purpose of the Fourth Amendment. *See, e.g.*, Tracy Meares & Bernard Harcourt, *Randomization and the Fourth Amendment*, 78 U. CHI. L. REV. 809, 810–17 (2011); CHRIS SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 37–46 (2007).

34. *See* Brennan-Marquez, *supra* note 32, at 1295–97 (compiling argument—and supportive authority—to this effect).

35. Of course, this is deeply imperfect in practice, partly because of the Court's own doing in cases like *Whren v. United States*, 517 U.S. 806, 818–19 (1996) (probable cause suffices to justify a

As it relates specifically to data surveillance, however, the Fourth Amendment's most important goal—whether it flies under the Founding Era banner of "security,"[36] or under the post-*Katz* banner of "privacy"[37]—is to enable participation in democratic life. By limiting the state's surveillance capacity, the Fourth Amendment protects us from monitoring that "chill[s] the exercise of [] civil liberties,"[38] especially those related to expression and association.[39] The point is intuitive and familiar; it lies to the heart of modern political thought. When watched, people tend to avoid "experiment[ing] with new, controversial, or deviant ideas,"[40] and they tend to shy away from activities and associations that, if broadcast socially, could come back to haunt.[41] In short, surveillance stunts autonomy.[42]

---

stop even if the stop was pursued for reasons unrelated to the suspected crime) and *Devenpeck v. Alford*, 543 U.S. 146, 154–56 (2004) (probable cause to arrest for *any* crime suffices to justify an arrest, even if the crime reported by the arresting officer and the crime ultimately grounding probable cause are different). But the point is that constraining discretion remains an *aspiration* of the Fourth Amendment. *See, e.g.*, Tracey Maclin, *The Central Meaning of the Fourth Amendment*, 35 WM. & MARY L. REV. 197, 201 (1993) ("[T]he central meaning of the Fourth Amendment is distrust of police power and discretion.").

36. *See generally* DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE (2017); Rubenfeld, *supra* note 23.

37. *See* Katz v. United States, 389 U.S. 347, 361–62 (Harlan, J., concurring) (outlining the famous "reasonable expectations of privacy" test). For a discussion of the difference between the security- and the privacy-based views of the Fourth Amendment (and a defense of the latter), *see* Christopher Slobogin, *A Defense of Privacy as the Central Value Protected by the Fourth Amendment's Prohibition on Unreasonable Searches*, 48 TEX. TECH. L. REV. 143 (2015).

38. Neil M. Richards, *Privacy and Technology: The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013).

39. *See* Hassan v. City of New York, 804 F.3d 277, 293 (2015) (holding that allegations of religiously-targeted surveillance are sufficient to establish an injury-in-fact, due to the chilling effect on association that such surveillance can have); NAACP v. Alabama, 357 U.S. 449, 466–67 (1958) (barring Alabama from demanding access to NAACP membership rolls as a condition of continuing to operate in the state, insofar as the demand curtailed "the right of the [NAACP's] members to pursue their lawful private interests privately and to associate freely with others . . . .").

40. Richards, *supra* note 38, at 1935. *See also* Strandburg, *supra* note 26, at 626–34 (exploring the breakdown in social life that surveillance can occasion). For a classic account of this dynamic, *see* MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1977).

41. *See* United States v. U.S. Dist. Court for E. Dist. Mich., 407 U.S. 297, 327 (1972) (Douglass, J., concurring) (explaining that a "core" reason for the Fourth Amendment's prohibition on suspicionless surveillance is "the recurring desire of reigning officials to employ dragnet techniques to intimidate their critics"). *See also* Rubenfeld, *supra* note 23, at 127 (arguing that the "insecurity" against which the Fourth Amendment protects us "is the stifling apprehension and oppression that people would justifiably experience if forced to live their personal lives in fear of appearing 'suspicious' in the eyes of the state. . . . Freedom requires that people be able to live their personal lives without a pervasive, cringing fear . . . produced by the justified apprehension that their personal lives are subject at any moment to be violated and indeed taken from them if they become suspicious in the eyes of governmental authorities").

42. *See, e.g.*, JULIE COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICES 122–23 (2012) (arguing that privacy gives people space, insulated from the social world, in which to develop identities); LAWRENCE LESSIG, CODE AND OTHER LAWS OF

But it gets worse. For one thing, the chilling effects of surveillance are not evenly distributed. In practice, already-marginalized populations tend to bear a greater share of the burden.[43] As Christopher Slobogin once put it, although many of us, as we go about our everyday lives, likely feel "perfectly secure from [the] . . . pressure [caused by surveillance]," the important thing is to

> [I]magine you are a Mexican American in Southern California who is subjected to document checks on major highways far from the border, or . . . an inner-city resident subject to routine checkpoint stops as you walk around your own neighborhood, or an Arab American . . . subject to FBI interviews because a data-mining program indicates that you fit a terrorist profile.[44]

For someone in this kind of position, the experience that originally animated the Fourth Amendment's guarantee of security—that of living under a government "willing to treat [everyone] like wrongdoers even though most of them [are] not"[45]—is alive and well.[46]

CYBERSPACE, 152–53 (1999) (using the example of "a gay man in an intolerant small town" to argue that "[p]rivacy, or the ability to control data about yourself, supports [the] desire [for separate communities]. It enables these multiple communities and disables the power of one dominant community to norm others into oblivion"). Another harm associated with surveillance—which I leave largely to one side here—is "hassle," i.e., concrete interference with someone's life. *See generally* Jane Bambauer, *Hassle*, 113 MICH. L. REV. 461 (2014). In so doing, I do not mean to suggest that hassle is never part of private surveillance. For example, when ISPs screen email for contraband and find a suspected match, they often divert the email from the recipient's inbox and quarantine it—an obvious case of concrete interference in everyday life. For further background on this process, *see* United States v. DiTomasso, 56 F. Supp. 3d 584, 587 (S.D.N.Y. 2014) (addressing whether an individual had an expectation of privacy in his emails and online chats, which were examined by ISPs and subsequently law enforcement).

43. For recent examples, *see, e.g.*, Charlie Savage, *Justice Department Demands Data on Visitors to Anti-Trump Website, Sparking Fight*, N.Y. TIMES (Aug. 15, 2017), https://www.nytimes.com/2017/08/15/us/politics/justice-department-trump-dreamhost-protests.html?_r=0; *Hassan*, 804 F.3d at 285–88 (documenting allegations of targeting of Muslim-Americans by the NYPD after 9/11). And the historical examples, of course, are legion—and infamous. *See, e.g.*, Sinclair v. Kleindienst, 645 F.2d 1080, 1081–83 (1981) (discussing the FBI's surveillance of the Black Panther Party); Gibson v. Florida Legislative Investigation Comm., 372 U.S. 539, 540–43 (1963) (discussing the targeting of suspected communists during the McCarthy Era).

44. Slobogin, *supra* note 23, at 124–25.

45. *Id*. at 124. *See also* Utah v. Strieff, 136 S. Ct. 2056, 2070–71 (2016) (Sotomayor, J., dissenting) (arguing that the majority, by "legitimizing" the use of illegal stops to conduct fishing expeditions for outstanding warrants, "tells everyone, white and black, guilty and innocent, that an officer can verify your legal status at any time[,]" "that your body is subject to invasion while courts excuse the violation of your rights[,]" and "that you are not a citizen of a democracy but the subject of a carceral state, just waiting to be cataloged").

46. *See also* Maryland v. King 133 S. Ct. 1958, 1989 (2013) (Scalia, J., dissenting) (arguing that "[s]olving unsolved crimes is a noble objective, but it occupies a lower place in the American pantheon of noble objectives than the protection of our people from suspicionless law-enforcement searches").

Moreover, for the same reasons that surveillance diminishes *individual* autonomy, it also imperils *collective* autonomy—it hobbles democracy. As Julie Cohen has argued, "[a] society that permits the unchecked ascendancy of surveillance infrastructures cannot hope to remain a liberal democracy."[47] Rather, unconstrained surveillance causes liberal democracy to be "replaced, gradually but surely, by a different form of government that [we could] call modulated democracy," modulated, that is, "by powerful commercial and political interests" that will increasingly hamper our "ability to form and pursue meaningful agendas for human flourishing."[48] Once again, the idea here is intuitive and familiar. Stunted selves do not make for a healthy body politic. A social order in which individuals feel unable to express their views and experiment with different modes of life is hardly conducive to "the practice of informed and reflective citizenship."[49]

None of this, moreover, was lost on the Founders. The Fourth Amendment was ratified explicitly in response to the "Crown's practice of using general warrants and writs of assistance,"[50] legal instruments that equipped agents of the Crown with blanket license to search wherever, and *whomever*, they wanted, sometimes within specific geographical bounds (such as a township), and sometimes without limit.[51] What was so vexatious about general warrants and writs of assistance? It was not simply that they caused "intrusion per se."[52] Rather, the problem (in addition to their being a reminder of odious colonial rule) was that general warrants and writs of assistance allowed officials to engage, at will, in "a general, exploratory rummaging [of any] person's belongings," giving rise to a climate in which state officials might invade one's life at any time,

---

47. Julie Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1912 (2013). *See also* FRANK PASQUALE, THE BLACK BOX SOCIETY: TECHNOLOGIES OF REPUTATION, SEARCH, AND FINANCE 3–4 (2013).

48. *See* Cohen, *supra* note 47, at 1912.

49. *Id.* at 1905. For a slightly different—but conceptually similar—exploration of the relationship between surveillance constraints and democratic health, *see generally* Thomas P. Crocker, *The Political Fourth Amendment*, 88 WASH. U. L. REV. 303 (2010).

50. Messerschmidt v. Millender, 132 S. Ct. 1235, 1252 (2013) (Sotomayor, J., dissenting). *See also King*, 133 S. Ct. at 1980–82 (Scalia, J., dissenting) (documenting copious authority for the proposition that general warrants were the Fourth Amendment's specific target during the Founding Era); Sundby, *supra* note 23 at 509 (suggesting that the "concern over general warrants . . . suppl[ies] a theoretical and historical underpinning" for Fourth Amendment law); Ohm, *Massive Hard Drives*, *supra* note 23, at 10 n.37 (compiling sources to the same effect).

51. For excellent historical background, *see generally* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547 (1999).

52. Andresen v. Maryland, 427 U.S. 463, 480 (1976).

particularly when the state wishes to shut down "seditious"—or in today's parlance, democratic—activity.[53]

Against this backdrop, the question is whether the intermediation of private actors in the surveillance process—having private companies facilitate the collection of data by state officials—changes the normative calculus. A moment's reflection shows why the answer must be no. If the animating concern here is that when people are subject to "panvasive"[54] state surveillance, they modulate their behavior, decline to experiment with new ideas, and withdraw from democratic life, why should the *channel* through which the surveillance occurs make a difference? Chilling effects, after all, do not arise exclusively in response to the initial collection of sensitive information; they can also stem from anxiety about where sensitive information, once collected, might flow.[55] For example, suppose Lyra has reason to suspect that her employer monitors (or could start monitoring) her online activity at work; this would likely deter her from checking her personal Gmail at work.[56] Would the situation be different, in terms of chilling effects, if Lyra (1) knew that Google was monitoring her online activity, and (2) had reason to suspect that Google was (or might begin) sending reports of that activity to her employer? No. The only difference between these scenarios is the number of steps that must occur before Lyra's employer becomes aware of her online activity; the latter requires two steps (Google would have to share reports of Lyra's online activity, and her employer would have to review those reports), whereas the former requires only one. But the deterrent effect would be equivalent, because from Lyra's perspective—the perspective that matters for assessing chilling effects—the concern is that negative consequences that could follow if her employer realizes that she has been spending work-

---

53. *Id.* *See also* Maryland v. Garrison, 480 U.S. 79, 84 (1987) ("The [] purpose of [the Amendment's] particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit."); Crocker, *supra* note 49, at 308 ("Privacy is no doubt an important constitutional value . . . . But privacy exclusiveness ignores a 'more majestic conception' of the Fourth Amendment that protects a political 'right of the people' to organize community life free from pervasive government surveillance and interference.") (citing Herring v. United States, 555 U.S. 135, 151 (2009) (Ginsburg, J., dissenting)).

54. *See generally* Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Non-Delegation Doctrine*, 102 GEO. L. J. 1721 (2014) (arguing that "pervasive and invasive" mass surveillance technologies are "panvasive").

55. *See generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010) (developing a theory of privacy based on expected information flows in different contexts). *See also* Kiel Brennan-Marquez & Stephen Henderson, *Fourth Amendment Anxiety*, 55 AM. CRIM. L. REV. 1 (2018).

56. Of course, this could be a socially beneficial instance of chilling. But the point remains.

time on personal email. The important thing is not *how* that realization comes to pass, only that it does.

This is why "any solution [to government surveillance today] must grapple with the complex relationships between government and corporate watchers."[57] When the boundary between the two becomes porous, as it plainly does in the context of informal data-sharing, the concerns about chill that have traditionally animated scrutiny of direct state surveillance also apply to private surveillance efforts that seamlessly *underwrite* state surveillance. At some level, in fact, the point is even starker. Since (at least) Edward Snowden's revelations in 2013, it has become clear that the actors most likely to spearhead ongoing, indiscriminate data surveillance today are the very intermediaries—information companies—that facilitate communication, political participation, and other expression.[58] Accordingly, data-sharing between the private sector and law enforcement may even *more* prone, by comparison to traditional state surveillance, to encourage self-censorship and recession from democratic life. After all, private companies today enjoy direct access to information that state officials of past generations could only have dreamt of having: data, in ever-larger quantities, about exactly who our friends are, exactly how we spend our time, and exactly what we think about—well, everything.

None of this to say, of course, that all informal data-sharing between the private sector and law enforcement should be forbidden. Nor does it mean the Fourth Amendment should necessarily constrain informal data-sharing in the same way it constrains compulsory data seizures by the government. Our tools for regulating the latter—like warrants—may prove impracticable for regulating the former. The point is simply that at a *normative* level, informal data-sharing and compulsory data seizures are two sides of the same coin. Both raise the same core concern: that when a polity becomes accustomed to (1) constant surveillance of daily life, coupled with (2) knowledge that the government will ultimately have access to the fruits of that surveillance, democracy wilts. And the proper *doctrinal* question, accordingly, is whether the legal rules for extending Fourth Amendment protection to informal data-sharing are adequately attentive to this concern. Under current law, alas, the answer is no.

---

57. *See* Richards, *supra* note 38, at 1935.

58. *See* Packingham v. North Carolina, 137 S. Ct. 1730, 1735–36 (2017) (expounding the centrality of social media to modern political life). *See also generally* Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. (forthcoming 2018), https://ssrn.com/abstract=2937985.

III. EXISTING LAW, RECONSIDERED

Existing doctrine has not been blind to the problem of private surveillance becoming entwined with law enforcement. But its approach to the problem—asking whether private action was deputized by the state—cannot contend with the realities of private surveillance today. This Part explores why.

A. Description

The deputization framework has a long historical pedigree—reaching back to the Supreme Court's first private search case in 1921, *Burdeau v. McDowell*, which concerned the admissibility of evidence discovered by an ex-employer. McDowell's boss, having grown suspicious of McDowell's workplace conduct, searched McDowell's office, where he located documents (which he then relayed to the authorities) suggesting McDowell's involvement in a fraud.[59] Once charged, McDowell moved to suppress the documents on the grounds that his boss's entry into a private office constituted an illegal search (and the procurement of his private papers, an illegal seizure).[60] The Court rejected McDowell's theory.[61] Acknowledging that his boss had, indeed, violated the law—the boss had no right to enter McDowell's office,[62] and even if he could conceivably claim a possessory interest in work-related material, his seizure included some of McDowell's personal papers[63]—the Court concluded that this alone did not make out a constitutional violation. Put simply, the Fourth Amendment was "intended as a restraint upon the activities of sovereign authority," and "no [government] official . . . had anything to do with the wrongful seizure . . . ."[64]

It would take half a century for the Court to hear its next private search case, *Coolidge v. New Hampshire*.[65] In essence, *Coolidge* presented two questions. First, how does *McDowell* apply to homes rather than offices? Second, if police know about a private search at its outset, does the analysis change? Suspecting that Edward Coolidge had kidnapped and murdered a fourteen year-old girl, the police visited his residence and

---

59. Burdeau v. McDowell, 256 U.S. 465, 470–71 (1921).
60. *Id.*
61. *Id.* at 475–76.
62. *Id.* at 470–71.
63. *Id.* at 470.
64. *Id.* at 475.
65. Coolidge v. New Hampshire, 403 U.S. 443 (1971).

interviewed his wife. At the close of the interview, Mrs. Coolidge volunteered to furnish the police with numerous pieces of evidence—including multiple guns, as well the clothes that Mr. Coolidge had been wearing the day the girl disappeared—which ultimately ended up implicating him in the crime.[66]

There was no allegation that the police had directed, much less forced, Mrs. Coolidge to hand over the evidence. Nevertheless, her husband moved to suppress the items on the grounds that "when Mrs. Coolidge brought out the guns and clothing and then handed them over to the police, she was acting as an 'instrument' of the officials . . . ."[67] The Court disagreed; because the police had not "coerce[d] or dominate[d] [Mrs. Coolidge]," or even "direct[ed] her actions by the more subtle techniques of suggestion . . . available to officials in circumstances like these,"[68] the Court held that Mrs. Coolidge, when she furnished the evidence, was acting as a private person, not as an instrument of the state—so the Fourth Amendment protection did not apply. In the Court's words:

> [I]t is no part of the policy underlying the Fourth . . . Amendment[] to discourage citizens from aiding to the utmost of their ability in the apprehension of criminals. If, then, the exclusionary rule is properly applicable to the evidence taken from the Coolidge house . . . it must be upon the basis that some type of unconstitutional police conduct occurred.[69]

A decade later, the Court's next foray into private searching was *Walter v. United States*, a case that, by the majority's own estimation, involved "bizarre facts."[70] A package of video tapes was inadvertently delivered to the wrong recipient, a small company outside Atlanta.[71] After opening the package, the employees became suspicious (based on drawings and written descriptions on the outside of the VHS boxes) that the tapes contained illicit pornography. So, without watching the tapes,[72] the employees called the FBI, who took possession of the tapes and confirmed the employees' suspicions.[73] Eventually, the search was challenged,[74] and the Court, relying on *McDowell* and *Coolidge*, held that

66. *Id.* at 445–46.
67. *Id.* at 487.
68. *Id.* at 489–90.
69. *Id.* at 488.
70. Walter v. United States, 447 U.S. 649, 651 (1980).
71. *Id.*
72. *Id.* at 652.
73. *Id.*
74. In fact, *Walter* presented two distinct questions—but only one is relevant here. The

it has long "been settled . . . that a wrongful search or seizure conducted by a private party does not violate the Fourth Amendment and that such private wrongdoing does not deprive the government of the right to use evidence that it has acquired lawfully."[75] Thus, because "there was nothing wrongful about the [FBI's] acquisition of the package [of tapes]," the Fourth Amendment did not come into play.[76]

This brings us to what is probably the best-known of the Court's private search cases: *United States v. Jacobsen*.[77] Like *Walter*, *Jacobsen* concerned the private search of a package. Unlike *Walter*, however, the private actors conducting the search in *Jacobsen* were not the package's (inadvertent) recipients, but employees of Federal Express ("FedEx"). After a package broke in transit, its handlers dismantled it—per company policy, for insurance reasons—only to discover tubes of suspicious-

---

defendants in *Walter* challenged both (1) the initial transfer of the films to the FBI agents, and (2) their subsequent viewing. As to the first question, the Court held that *McDowell* and *Coolidge* were squarely on point, precluding any Fourth Amendment challenge. *See id.* at 656–57. As to the second question, however, the Court agreed with defendants: the FBI agents needed a warrant to watch the video tapes. *Id.* at 658–59. The reason for this holding, the Court explained, was that although the government is free, as a general matter, to capitalize on the fruits of private searches, it "may not exceed the *scope* of [those] search[es] unless it has the right to make an independent search." *Id*. at 656. In other words, if law enforcement officials wish to perform a search beyond the already-executed private search, it needs probable cause. *See id*. at 657 ("[Here], the private party had not actually viewed the films. Prior to the Government screening one could only draw inferences about what was on the films"). Of course, this analysis invites two conclusions that are not terribly easy to swallow. The first is that state officials may retrace any investigative ground already traversed by private actors. Invoking this principle, the *Walter* Court distinguished sharply between law enforcement taking possession of the illicit films—an act that clearly would have constituted a Fourth Amendment seizure, had it not been occasioned by interceding private action—and the actual viewing of the tapes. Later, the Court doubled down on this conceptual distinction, holding that, in cases that involve private searches and law enforcement searches, "invasions of [] privacy by the government agent must be tested by the degree to which they exceeded the scope of the [previous] private search." Jacobsen v. United States, 466 U.S. 109, 115 (1984). A moment's reflection, however, shows why this seemingly modest proposition is, in fact, astonishingly broad. On its face, this logic would reach, for example, private searches of homes—if a stranger (like a burglar) were to enter my home and perform a private search, law enforcement would have carte blanche, prospectively, to do the same. It is difficult to imagine anyone—even someone with solidly pro-police convictions in this area—embracing that result. Not surprisingly, lower courts tasked with applying *Walter* and *Jacobsen* to contexts other than in-transit packages have routinely declined to protract its logic that far. *See, e.g.*, U.S. v. Young, 573 F.3d 711, 720–21 (9th Cir. 2009) (holding that *Jacobsen's* "expanded search" rule does not apply to the private search of a guest's hotel room and effects); U.S. v. Allen, 106 F.3d 695, 698–700 (6th Cir.) (same), *cert. denied*, Allen v. U.S., 520 U.S. 1281 (1997). *Cf.* U.S. v. Paige, 136 F.3d 1012, 1024 (5th Cir.) (holding that a previous private search does not extinguish one's *possessory* interest—as opposed to privacy interest—in contraband), *reh'g denied*, 142 F.3d 1281 (5th Cir. 1998). For background, *see* Orin Kerr, *Searches and Seizures In a Digital World* 119 HARV. L. REV. 531, 554–56 (exploring the "expanded search" rule).

75. *Walter,* 447 U.S. at 656.

76. *Id.*

77. 466 U.S. 109 (1984).

looking white powder concealed within.[78] At that point, the FedEx employees "summoned a [DEA] agent, who removed a trace of the powder, subjected it to a chemical test and determined that it was cocaine."[79] When this drug evidence was introduced against him, Jacobsen moved to suppress.[80] Following its other precedents, the Court rejected his claim; it held that the FedEx employees' search of the package, regardless of whether it was "accidental or deliberate,"[81] was not subject to Fourth Amendment scrutiny. In the Court's words—echoing *Coolidge* and *McDowell*—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.'"[82]

B. Diagnosis

The deputization framework is not entirely void of appeal. It deals well with cases of overt influence by the state: when, for example, an informant, operating as an ongoing agent of law enforcement rifles

78. *Id.* at 111.

79. *Id.*

80. *Id.* at 112.

81. *Id.* at 115.

82. *Id.* at 113 (emphasis added). *Jacobsen* also has the distinct honor of proposing an entirely new—though, on scrutiny, wholly untenable—principle to govern private searches. Namely, as long as the fruits of private surveillance are in "plain view" when transmitted to law enforcement, no Fourth Amendment violation occurs. *See id.* at 116, 119; *see also id.* at 130 (White, J., concurring) ("Where a private party has revealed to the police information he has obtained during a private search or exposed the results of his search to plain view, no Fourth Amendment interest is implicated because the police have done no more than fail to avert their eyes"). The shortcoming of this logic is not hard to see. Suppose S is a suspect, G is a government official, and P is a third-party that procures incriminating evidence from S and transmits it to G. The "private search as plain view" logic would suggest that G should be free—categorically—to make use of evidence, as long as the transmission from P to G caused the evidence to be in plain view. The problem is that whether the information was in plain view from G's vantage point tells us nothing, one way or another, about the circumstances under which P initially procured the information. Suppose, for example, that T is an NYPD officer, and G is a DEA agent. Believing that S is manufacturing drugs, T enters S's apartment—without a warrant—where T finds and takes pictures of a drug lab. Then, instead of making use of them himself, T sends the pictures to G, with a note indicating the address where they were taken, and encouraging G to procure a warrant to search S's residence on the strength of the pictures. In this example, two things are clear. First, when T sends the pictures to G, they are certainly in "plain view" from G's perspective. Second, the method by which T acquired evidence from S's apartment was plainly a Fourth Amendment violation. More importantly, *nothing about the first observation changes the second*. T's actions do not become more legitimate because they result in G being able to "plainly view" the evidence. The fruit of the poisonous tree doctrine obviously applies (and the same would be true if T is a private party, not an NYPD officer, but T is operating at the behest of the NYPD). Put simply, whether or not evidence is furnished to law enforcement in plain view says nothing about the legality of its initial procurement. The two issues are orthogonal.

through customer property, looking for contraband;[83] or when state officials transform a corporate officer into the "eyes and ears" of law enforcement by alerting him to an open investigation at his firm, and instructing him to look for specific documents.[84] Furthermore, the framework also does a good job *excluding* certain types of "spontaneous" private searches—like those on display in *McDowell*, *Coolidge*, and *Jacobsen*—from Fourth Amendment protection.[85]

Where the deputization framework falters, however, is in its treatment of systematic but informal private surveillance: when private actors turn *themselves* into the "eyes and ears" of law enforcement. Faithful to the framework, the Seventh Circuit has held, for example, that a FedEx manager who repeatedly looked through packages and reported the results to law enforcement was not operating as an agent of the state—this, in spite of the fact that the employee had an undisputed "history of cooperation . . . [with] law enforcement authorities," and the fact that he penned a "memorandum [to] senior managers," extoling the "value of good relations with law enforcement agencies."[86] Similarly, the Fourth Circuit has held that a hacker who continually assisted the FBI by—illegally—accessing private computers to look for child pornography (and then transmitting the results to law enforcement) was not operating as an agent of the state; although the hacker's "motivation . . . stemmed solely from his interest in [helping] law enforcement," the government did no more than "passively [] acquiesce" to the assistance (over and over again), so, the court reasoned, no Fourth Amendment scrutiny was warranted.[87]

The deputization framework also has difficulty with data surveillance by private companies. Many ISPs, for example, have started "hashing" the email that flows through their servers, a process that uses unique alphanumeric identifiers (known as hash values) to identify files and,

---

83. *See, e.g.*, United States v. Walther, 652 F.2d 788, 793 (9th Cir. 1981) (holding that an airline employee, who had been an official informant in the past and had received payments for his aid on several occasions, performed a luggage search, he was operating as an agent of the government).

84. *See, e.g.*, United States v. King, 212 F. Supp. 3d 1113, 1129 (W.D. Okla. 2015) (holding that a law enforcement search occurred when state officials directed a company's CFO to surreptitiously search for, and transmit copies of, documents relevant to an ongoing investigation).

85. *See* Coolidge v. New Hampshire, 403 U.S. 443, 490 (1971). For other examples of spontaneous private searches that seem not to extend law infrastructure—and therefore come out correctly (albeit it for the wrong reasons)—under the encouragement framework, *see, e.g.*, United States v. Bowers, 594 F.3d 522, 526–27 (6th Cir. 2010) (finding no Fourth Amendment search when a tenant found contraband on her roommate's dresser); United States v. Runyan, 275 F.3d 449, 458 (5th Cir. 2001) (finding no Fourth Amendment search when ex-spouse entered the other ex-spouse's property without permission to locate evidence of contraband).

86. United States v. Koenig, 856 F.2d 843, 848–50 (7th Cir. 1988).

87. United States v. Jarrett, 338 F.3d 339, 345–46 (4th Cir. 2003), *cert. denied*, 540 U.S. 1185 (2004).

where applicable, match them to databases of known child pornography.[88] When ISPs locate an offending file, they are required to notify the National Center for Missing and Exploited Children (NCMEC),[89] a hybrid entity that operates privately but with an explicit statutory blessing, who then reviews the file and sends a report to the FBI.[90]

When defendants have challenged hashing on constitutional grounds—arguing that ISPs are, in effect, operating as an arm of law enforcement when they screen email—courts have uniformly concluded that the Fourth Amendment does not reach the ISPs' conduct.[91] Why? Because the hashing is entirely voluntary; there is no formal agency relationship between the ISPs and law enforcement, and beyond that, government officials have done nothing to direct, or even to *encourage*, hashing—much as they obviously benefit from the practice. Indeed, this result is effectively required by the logic of the deputization framework.

To be clear, the problem with eliminating all constitutional protection for informal data-sharing between state officials and private actors—whether those actors are powerful companies or flesh-and-blood individuals—is *not* that all such surveillance should be forbidden. The problem is that it should be subject to reasonableness review, the Fourth Amendment's veritable "touchstone."[92] In fact, one can imagine all sorts of justifications for practices like indiscriminate email hashing by ISPs and programmatic monitoring by FedEx employees. But those justifications

---

88. For greater detail on the technical mechanisms of hashing, *see* Robyn Burrows, Comment, *Judicial Confusion and the Digital Drug Dog Sniff: Pragmatic Solutions Permitting Warrantless Hashing of Known Illegal Files*, 19 GEO. MASON L. REV. 255, 261 (2011); Salgado, *supra* note 7, at 39. For a judicial discussion of the process, *see, e.g.,* United States v. DiTomasso, 56 F. Supp. 3d 584, 587 (S.D.N.Y. 2014). At present, hashing is largely confined to child pornography. But other applications of the technique are certainly possible: for instance, hashing could, in principle, be used to identify pirated software, or copyright-infringing media files. *See, e.g.*, In re Cunnius, 770 F. Supp. 2d 1138, 1152 (W.D. Wash. 2011).

89. *See* 18 U.S.C. § 2258A (2012). From there, once NCMEC verifies the contents of the file, it is obligated to forward a report to the appropriate federal law enforcement agency (and it is permitted to forward a report to state law enforcement agencies at its discretion). *See id.* § 2258A(c).

90. Although NCMEC is a private, nonprofit 501(c)(3) organization, it works in "partnership" with the United States Department of Justice pursuant to Congressional authorization under 34 U.S.C. § 11293 (2012). *See also* 18 U.S.C. § 2258C(a)(2) (permitting the NCMEC to provide "hash values or other unique identifiers associated with a specific image" to ISPs to prevent the transmission of child pornography). The Center receives an annual grant from the Office of Juvenile Justice and Delinquency Prevention, an agency housed within the DOJ. *See* 34 U.S.C. § 11293(b).

91. *See, e.g.*, United States v. Stevenson, 727 F.3d 826, 830 (8th Cir. 2013); United States v. Cameron, 699 F.3d 621, 637–38 (1st Cir. 2012), *cert. denied*, 569 U.S. 939 (2013); United States v. Richardson, 607 F.3d 357, 365 (4th Cir.), *cert. denied*, 562 U.S. 982 (2010). *But see* United States v. Ackerman, 831 F.3d 1292, 1295 (10th Cir. 2016) (reserving the question of whether a private ISP—here, AOL—was operating as a state actor when it hashed user email).

92. *See* Riley v. California, 134 S. Ct. 2473, 2482 (2014) ("As the text makes clear, 'the ultimate touchstone of the Fourth Amendment is 'reasonableness.'"").

would stem from the *nature* of the relevant surveillance: its purpose, its scope, its duration, its level of intrusiveness, and so forth.[93] In other words, the surveillance would be justified because it strikes a reasonable balance between privacy interests, on one hand, and law enforcement need, on the other—not because it happens to be spearheaded by a private actor.

As the law currently stands, it would make no difference if, for example, ISPs began performing comprehensive data analysis on the content of user email, and passing the results on to law enforcement.[94] The activity would be no less private, and no less voluntary, than the (far more limited) practice of hashing; and under the deputization framework, it would be similarly immune from Fourth Amendment scrutiny. Likewise, it would make no difference if FedEx put in place a "crime prevention" wing tasked with performing X-Ray review of all packages and shuttling anything suspicious to law enforcement. Again, the doctrine would have nothing to say—by design—about the program's reasonableness.

IV. FROM "DEPUTIZATION" TO "EXTENDED INFRASTRUCTURE"

It may be tempting to recast the examples just imagined as poor *applications* of the deputization framework; after all, one can imagine a court stretching the notion of "agency," or finessing the idea of "government participation," to reach informal private surveillance. Indeed, that is exactly what some lower courts—no doubt intuiting the need for reform—have done.[95] But these contortions would ultimately be just that. When all is said and done, the deputization framework is incapable, because of its conceptual structure, of adequately limiting the state's capitalization on private surveillance it had no hand in instigating. For that, a new starting point—a functional test, focused on law enforcement infrastructure—is needed.

Fortunately, the new starting point need not eschew the virtues of the deputization framework. In fact, every single case the deputization framework gets right would be equally well captured by an "extended infrastructure" test. Ultimately, deputization is one *means* by which law enforcement infrastructure can be extended. The point is that it is not the only one. Informal private surveillance, too, can extend infrastructure—

93. For an argument to this effect, with regard to ISP hashing in particular, *see* Salgado, *supra* note 7, at 38–39.

94. *See supra* notes 3–4, and accompanying text.

95. *See, e.g.*, United States v. Spicer, 432 F. App'x 522, 523–24 (6th Cir. 2011) (holding that the deputization rule 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) (holding the Fourth Amendment was violated when security personnel at a hotel—private employees—engaged in a non-deputized search of defendant's hotel room, opened suitcases to locate contraband, and gave the contraband to the police).

when it is repeated, systematic, and transformative of the law enforcement process.

A. Light Through the Cracks: Skinner v. Railway Labor Executives' Association

In some sense, the "extended infrastructure" framework is already on display—in refracted form—in the single private search case excluded from last Part's genealogy: *Skinner v. Railway Labor Executives' Association*, which involved a challenge to various regulations promulgated by the Federal Railroad Administration ("FRA").[96] One set of regulations ("Subpart C") required private railroad companies to perform "blood and urine tests of employees who [were] involved in certain train accidents," while another regulation ("Subpart D") permitted companies "to administer breath and urine tests to employees who violate[d] certain safety rules."[97] Plaintiffs disputed the constitutional reasonableness of both Subparts. With respect to each, the threshold question was the same: given the formally private nature of the testing, does the Fourth Amendment apply in the first instance?

The Court answered in the affirmative, holding the Fourth Amendment applicable to both Subparts. With respect to Subpart C, this conclusion was unremarkable.[98] As the Court put it, "[a] railroad that complies with the provisions of Subpart C of the regulations does so by compulsion of sovereign authority, and the lawfulness of its acts is controlled by the Fourth Amendment," which clearly turned the private companies into "instrument[s] or agent[s] of the Government."[99] More remarkable was the Court's conclusion with respect to Subpart D. As the government pointed out, "nothing in Subpart D compel[led] any testing by private railroads."[100] Rather, the Subpart merely *facilitated* blood and urine testing, in case private railway companies decided, of their own volition, to perform such testing. Accordingly—the government argued—Subpart D should not come under Fourth Amendment scrutiny.

The Court made short work of this logic. Noting, up front, that "[t]he fact that the Government has not compelled a private party to perform a search does not, by itself, establish that the search is a private one," the Court identified three features of Subpart D that aroused constitutional

96. Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602 (1989).
97. *Id.* at 606.
98. *See* Brennan-Marquez, *supra* note 15, at 803.
99. *Skinner*, 489 U.S. at 614.
100. *Id.*

concern: first, Subpart D had a preemptory effect on state laws prohibiting urine and blood testing by private railway companies;[101] second, Subpart D "mandated that the railroads not bargain away the authority to perform tests," as conferred by the regulations;[102] and third, the FRA had "made plain not only its strong preference for testing, but also its desire to share [in] the fruits" of testing.[103] The Court regarded these features of Subpart D, in tandem, as "clear indices of the Government's encouragement" of voluntary urine testing—encouragement that "suffice[d] to implicate the Fourth Amendment."[104]

I take no issue with *Skinner*'s holding regarding the Fourth Amendment's reach. In fact, the holding verges on self-evident, and it echoes the conclusion reached by every Court of Appeals to pronounce on the matter before the Court stepped in.[105] Nevertheless, *Skinner* represents a stark departure from the deputization principle traced above. Although the case is styled as a garden-variety application of precedent—the proper "inquir[y]," the Court wrote, was whether the railway companies were "act[ing] as [] instrument[s] or agent[s] of the government"—in fact *Skinner* is far more radical, and far better attuned to the salience of infrastructure, than any of the Court's other private search cases.[106]

Agency law is mobilized around two core principles. The first is that agency relationships form by "mutual assent."[107] If there is no meeting of minds—no agreement on the part of both the principal and the agent—there can be no agency relationship.[108] The second principle is that for a

---

101. *Id.* at 615.

102. *Id.*

103. *Id.*

104. *Id*. at 615–16.

105. *See* Ry. Labor Execs.' Ass'n v. Burnley, 839 F.2d 575, 589–90 (9th Cir. 1988) (compiling cases), *rev'd*, *Skinner*, 489 U.S. 602 (1989).

106. I will be assuming for the sake of analysis here—as numerous circuits have held, and as plain language suggests—that when the Court invokes "agency" in the private search context, it has in mind the common law of agency. *See, e.g*., United States v. Ackerman, 831 F.3d 1292, 1300–02 (10th Cir. 2016) (offering an elaborate discussion of the agency law principles underpinning the private search doctrine); United States v. Ellyson, 326 F.3d 522, 527 (4th Cir. 2003) (explaining that the "agent or instrument" test stems from "common law agency principles"). This is hardly a foregone conclusion, but it seems like a natural assumption for analytic purposes. *See, e.g*., United States v. Koenig, 856 F.2d 843, 847 n.1 (7th Cir. 1988) (looking to the "common law of agency" for clues in determining whether a private actor was operating as a state agent, but also noting that "the constitutional issue [is not] necessarily [] governed by the common law definition of agency").

107. RESTATEMENT (THIRD) OF AGENCY § 1.01 (AM. LAW INST. 2005) ("Agency is the fiduciary relationship that arises when one person (a 'principal') manifests assent to another person (an 'agent') that the agent shall act on the principal's behalf and subject to the principal's control, and the agent manifests assent or otherwise consents so to act"). *See also* 19 WILLISTON ON CONTRACTS § 54:14 (4th ed. 2015) ("The relationship of principal and agent . . . requires mutual consent").

108. In practice, this requirement can lead to thorny factual questions. Agency law is

relationship to be genuinely one of *agency*, as opposed to an informal relationship in which one party simply does something to aid another, the principal must exercise "control" over the agent's actions. As the Supreme Court (in another context) has explained, "[a]gency requires more than mere authorization to assert a particular interest [insofar as] '[a]n essential element of agency is the principal's right to control the agent's actions.'"[109]

In *Skinner*, neither of these conditions was satisfied.[110] The closest thing to a bona fide agency relationship was the fact that the FRA, in promulgating Subpart D, had cleared away preexisting obstacles to private surveillance. By creating a framework for data-sharing, and by immunizing railway companies from state-level liability, Subpart D certainly made it easier for railway companies to assist in the law enforcement.[111] Typically, however, that A enables B to perform an action

---

commendably pragmatic, rather than formalistic, in the tools it uses to determine when "mutual assent" exists. A principal's "manifestation of assent" need not be explicit, much less codified in a formal instrument like a contract. *See* RESTATEMENT (THIRD) OF AGENCY § 1.01 cmt. d. Rather, the principal's "manifestation [of assent] may be made directly [] to the agent or may reach the agent through a more circuitous route." *Id.* § 3.01 cmt. b. For example, industry customs and prior dealings between the parties can, depending on the circumstances, imply the existence of mutual consent. *See id*. § 1.03 cmt. e ("A manifestation [of assent] does not occur in a vacuum, and the meaning that may be reasonably inferred from it will reflect the context in which [it] was made.").

109. Hollingsworth v. Perry, 133 S. Ct. 2652, 2666 (2013) (citing RESTATEMENT (THIRD) OF AGENCY § 1.01 cmt. f). Control, too, can raise complicated issues of fact. For example, if a principal "request[s] another to act on the principal's behalf," and the "putative agent"—the counterparty to the request—"does the requested act, it is appropriate [under most circumstances] to infer that the action was taken as agent for the person who requested the action . . . ." RESTATEMENT (THIRD) OF AGENCY § 1.01 cmt. c. In other words, "control" does not necessarily mean "coercive authority." The question is whether, at a functional level, the principal was responsible for dictating the agent's conduct—through formal channels (e.g., an employer-employee relationship) or otherwise—such that the principal may be legitimately held accountable for that conduct.

110. No evidence suggested that the arrangement created by Subpart D resulted from mutual consent. Regardless of how "strong" the government's "preference" for drug testing may have been (*see* Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 615 (1989)), the railway companies in question had not assented to the agent role (at least, there was nothing in the Court's analysis, or that of the opinion below, to suggest such assent). Nor, furthermore, was there any evidence of control on the government's part. In fact, Subpart D explicitly left private railway companies free to implement drug testing procedures or not. So, while the *Skinner* Court is correct, of course, that Subpart D circumscribed the autonomy of private railway companies in some respects—for example, by limiting their room to maneuver in collective bargaining—the important question is whether the government, as would-be principal, was able to dictate the specific conduct (i.e., drug testing) subject to the challenge. On that score, the answer is plainly no. Subpart D operated to ensure that railway companies *could* perform drug testing. From this, however, it does not follow that railway companies *had* to perform drug testing, or that the companies would see any downside, even of a minor sort, for declining to perform such testing. At day's end, nothing in Subpart D—including the restraint on collective bargaining—made drug testing less-than-voluntary on the part of railway companies.

111. In this vein, the *Skinner* Court's logic bears a fleeting resemblance to the "ratification" principle in agency law—the notion that a would-be principal's ex post assent to a would-be agent's action can create an agency relationship *nunc pro tunc*. The difficulty in applying the ratification logic

does not render B an agent of A.[112] In the landlord-tenant context, for example, courts have been quite clear that when landlords give tenants permission to make changes to property (e.g., performing repairs), the tenant is not thereby converted into the landlord's agent.[113]

In short, if *Skinner*'s holding regarding Subpart D was justified—as I think it was—the justification must come from elsewhere than agency principles. Here, the Court's emphasis on "encouragement, endorsement, and participation" is telling. Subpart D relied, in effect, on private companies to perform the first-line of surveillance in a government program designed to eliminate drug use by railway employees. The Court was troubled, for good reason, at the idea that such reliance, because it involved no conscription, would elude Fourth Amendment scrutiny. So

---

to *Skinner* is two-fold. First, ratification only applies to a principal who manifests assent to "a *prior act* done by another." RESTATEMENT (THIRD) OF AGENCY § 4.01(1) (emphasis added). *See also* Estate of Stephens, 49 P.3d 1093, 1097 (Cal. 2002) ("Ratification is the *voluntary election* by a person to adopt in some manner as his own an act which was purportedly done on his behalf by another person, the effect of which, as to some or all persons, is to treat the act as if originally authorized by him.") (citations omitted) (emphasis added); Il Giardino, LLC v. Belle Haven Land Co., 757 A.2d 1103, 1120 (Conn. 2000) ("As a general rule, [r]atification is defined as the affirmance by a person of a *prior act* which did not bind him but which was done or professedly done on his account." (citations and quotation marks omitted) (emphasis added)). In *Skinner*, the relevant conduct of government's—promulgating Subpart D—occurred *before* the private searches. Second, ratification is not effective unless the principal has full knowledge of all of the material facts and circumstances surrounding the unauthorized transaction. *See* RESTATEMENT (THIRD) OF AGENCY § 4.06 ("A person is not bound by a ratification made without knowledge of material facts involved in the original act when the person was unaware of such lack of knowledge."); Dillon v. S. Mgmt. Corp. Ret. Tr., 326 P.3d 656, 665 (Utah 2014) ("[A]n essential fact that is implicit to a finding of ratification is the principal's knowledge that an individual has acted purportedly on behalf of the principal or as the principal's agent."). For ratification to have occurred in *Skinner*, therefore, the government would have needed to be aware of the circumstances surrounding all private drug testing—a factual predicate that, even if satisfied, played no role in the Court's analysis.

112. An exception occurs when the would-be agent (here, B) "actually [] belie[ves]" that the would-be principal seeks a particular outcome, and the would-be agent takes steps, in light of that belief, to secure the outcome. *See* RESTATEMENT (THIRD) OF AGENCY § 2.02 cmt. e. This, however, necessarily gives rise to a "subjective" question about the basis of the would-be agent's decision—a question the *Skinner* Court never broached, much less answered. To remain faithful to the "agency" formulation, *Skinner* would have needed to examine the motivations of the specific railway companies that implemented drug testing protocols pursuant to Subpart D. That it performed no such examination—indeed, that it failed to express any interest in such an examination—is strong evidence that something besides traditional agency principles are at play.

113. *See, e.g.*, Redco Constr. v. Profile Props., 271 P.3d 408, 410 (Wyo. 2012). There, a contractor entered into an agreement with a tenant to perform repairs; when the tenant defaulted on his obligations, the contractor attempted to recover against a landlord, on the theory that the tenant had been acting as the landlord's agent when he contracted—with the landlord's permission—to obtain repairs. The Wyoming Supreme Court rejected this argument, holding that the landlord's permission did not convert the tenant into an agent, because the landlord "did not *require* [the tenant] to make any improvements, and [the landlord] retained no control over the scope or details of the improvements [the tenant] chose to make." *Id*. at 421. And this was so, the court held, despite the fact that the repairs were clearly desired by the landlord and ultimately operated to the landlord's benefit.

the Court devised a new test: when the state "encourages" private surveillance, it should be subject to constitutional review, even if the surveillance does not involve deputization per se.[114]

Yet the "encouragement" framework, too, seems like a misfire. After all, the *Skinner* Court surely did not mean that *any* government encouragement transforms private conduct into state action. If it did, the framework would sweep in many routine (and innocuous) forms of police work. Imagine, for example, that officers decide to go on patrol after a spate of crime, disseminating information and encouraging civilians to "keep an eye out" for potential evidence. If, in response, Lyra—an especially zealous member of the local neighborhood watch—decides to rummage through a suspicious neighbor's basement, and to relay whatever she finds there to law enforcement, would her conduct qualify as state action? Surely not. There may be other problems with Lyra's conduct; perhaps it would constitute a civil infraction. (Indeed, it almost certainly would.) But the fact that Lyra was responding to a prompt from state officials hardly suffices to turn her into an extension of law enforcement. Moreover, the "encouragement" framework runs headlong into the Court's *other* private search cases. In *Coolidge*, for instance, government encouragement was plainly a but-for cause of the wife's conduct, yet her search nevertheless had the flavor of "spontaneous" conduct.[115] Perhaps more importantly, it would be odd—even perverse—if the Fourth Amendment precluded private individuals, especially those with a stake in the outcome of investigation, from assisting law enforcement on a one-off basis.[116]

Ultimately, *Skinner* is best conceptualized as an infrastructure case. What seemed to truly bother the Court, beyond deputization—which was clearly not present—and even beyond encouragement, was the notion that an entire domain of law enforcement could systematically capitalize on private surveillance, but because of the sheer *informality* of the arrangement, the Fourth Amendment would have nothing to say. No, the government was not directing private action; and yes, the companies were free, at any point, to walk away. But that did not change the reality on the

---

114. *Skinner*, 489 U.S. at 615–16.

115. Coolidge v. New Hampshire, 403 U.S. 443, 489–90 (1971).

116. One setting where this principle has surfaced in the case law is co-tenancy. The Court has been quite clear that any co-tenant's consent is sufficient to authorize police entry—even if other co-tenants, given the opportunity, would have objected to the entry. *See* United States v. Matlock, 415 U.S. 164, 170–72 (1974) (first articulation of the rule). *Compare* Georgia v. Randolph, 547 U.S. 103, 122–23 (2006) (holding that if both co-tenants 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 consent of co-tenant sufficed to justify search after (1) the other tenant invoked his Randolph rights but (2) had been removed from the premises).

ground: by capitalizing on the activity of private companies, law enforcement had, in effect, expanded its infrastructural capability.

B. State Action Analogies

Skinner is not alone. Although the case may be unique within the Fourth Amendment canon, bedfellow precedents emerge elsewhere in the Court's state action jurisprudence. In fact, there are two other settings in which the Court has recognized that private activity can effectively extend the reach of public infrastructure—in a manner that requires a concomitant extension of the Constitution. The first setting is elections; the second is property attachments in advance of repossession or bankruptcy.

1. Elections

In the early 1950's, black voters in Jim Crow Texas brought an equal protection suit against the Jaybird Democratic Association, a private political organization that exerted considerable influence over local politics—essentially, by dictating the result of Democratic primaries through informal balloting—and whose membership was restricted to whites.[117] The threshold question in *Terry* was whether the Jaybird Association, in spite of its private character, was bound by the Fourteenth and Fifteenth Amendments, given its intimate connection to the official electoral system.

The Court said yes, though without consensus as to the rationale. Justice Clark, writing for a four-Justice plurality, argued that decisions by the Jaybirds operated, in practice, as a kind of shadow-primary. "Over the years," Justice Clark wrote, the Jaybirds' balloting "ha[d] emerged as the locus of effective political choice."[118] Because this conferred the Jaybirds "decisive power in the county's recognized electoral process," and thus "[struck] to the core of the electoral process in Fort Bend County," it rendered the organization a state actor for constitutional purposes.[119] Justice Black, meanwhile, wrote for three other Justices, concurring in the judgment on slightly different grounds.[120] In Justice Black's view, the "decisive power" of the Jaybirds was not enough, by itself, to render the association a state actor; rather, what "deprived [] petitioners of their right to vote on account of their race and color" was the "combined Jaybird-

117. Terry v. Adams, 345 U.S. 461, 462–66 (1953) (opinion of Black, J.).
118. *Id*. at 484 (Clark, J., concurring).
119. *Id*.
120. *Id.* at 462 (opinion of Black, J.).

Democratic-general election machinery."[121] In other words, the constitutional violation stemmed from "[t]he effect of the whole procedure, Jaybird primary plus Democratic primary plus general election . . . ."[122]

For our purposes, the daylight between Justice Clark's position and Justice Black's position, assuming any exists,[123] can be comfortably bracketed. The upshot of both positions is that private conduct—here, the Jaybird primary—can qualify as state action, not because of the "participation or acquiescence" of the state,[124] or (as the *Skinner* Court might have put it) the "encouragement" of the state, but because of what role the private organization played in the electoral infrastructure of Texas. In *Terry*, in other words, the orienting question was not "Who?" but "What?" The issue was not that the Jaybirds' actions were attributable to, much less spearheaded by, the state. The problem was that the Jaybird Association had become, in effect, an *extension* of the state, playing gatekeeper to a public process of great constitutional import and sensitivity: voting.[125]

2. Property Attachments

A second setting where the Court has adopted an "extended infrastructure" approach to state action is the state-facilitated attachment of property. Take *Lugar v. Edmonson Oil Co.*, which involved a Section 1983 suit—naming a private company as defendant—challenging the constitutionality of state procedures for attaching debtor property in

---

121. *Id*. at 470.

122. *Id*. at 469–70.

123. Although the two positions are very close (what "decisive power" often *means* is power over the "machinery" of local politics), one can imagine cases in which the two diverge. Imagine, for example, a private organization whose goal is to foment voter participation by leafleting and knock-and-talks. Imagine, furthermore, that the organization's explicit aim is to increase the white vote—and only the white vote. It is conceivable that such an organization could "decisive power" over a local election, but without any control over the "election machinery."

124. *See Terry*, 345 U.S. at 477 (opinion of Frankfurter, J.). Justice Frankfurter was the only Justice to agree with the result in *Terry* but also to depart from the public function logic (in favor of a "state participation" principle).

125. Implicit in *Terry*—and explicated in subsequent case law—is another feature of the public function test that makes it particularly useful for analyzing outsourced law enforcement: because the test focuses on specific conduct, not on the (formal or functional) status of the private actor, it can distinguish between an actor's activities. As the Second Circuit has explained, "[t]he extent of state action [under the public function test] correlates directly with the performance of the public function, which [] is limited to . . . those areas of [the private actor's] facility where the public function takes place . . . ." Cooper v. USPS, 577 F.3d 479, 493 (2d Cir. 2009). It is possible, in other words, for private actors to perform public functions in certain capacities but not others—as would be true of many of the private actors I have in mind here (e.g., ISPs performing email surveillance).

advance of repossession.[126] Allowing the Section 1983 suit to proceed against the private company, the *Lugar* Court explained that "we have consistently held that a private party's joint participation with state officials in the seizure of disputed property is sufficient to characterize [the private party] as a 'state actor' for purposes of the Fourteenth Amendment."[127] In other words, when someone has been dispossessed of her property via formal attachment proceedings, she may challenge the constitutionality of those proceedings by bringing a suit not only against the state actors who issued the writ of attachment, but also against the private counter-party that *requested* the writ of attachment.[128]

The reason for this rule, the *Lugar* Court explained, is that private creditors, in seeking the attachment of property, effectively operate as an extension of the state. A creditor who requests the writ of attachment and an "officer[] of the state" who supplies the writ "act jointly,"[129] often by way of "*ex parte* applications" that are especially susceptible to abuse,[130] in the process of stripping another party of property rights. Of course, the two parties' *roles* in the process are quite different; the creditor's role is to put the process in motion by applying for a writ, while the officer's role is to bestow legal force to the process. But when it comes to assessing the rights of the party whose property has been attached, the important thing, as the *Lugar* Court recognized, is the process as a whole. And when private parties have the capacity, given their social role, to extend the reach of state infrastructure—here, infrastructure related to the forcible reconfiguration of property rights—the Constitution cannot be blind to private conduct.

In other words, although the public aspect of attachment and repossession is what ultimately gives rise to the constitutional problem, it would be insufficient to hold state officials exclusively accountable for the procedural deprivation—just as it would have been insufficient, in *Terry*, to hold traditional political parties exclusively accountable for racial exclusion in the electoral process, and it would be insufficient, in the law enforcement setting, to require only state officials to abide by the strictures of reasonableness when performing surveillance. In all three settings, the

126. Lugar v. Edmonson Oil Co., 457 U.S. 922, 922 (1982).

127. *Id.* at 941.

128. For earlier applications of this principle, *see* N. Ga. Finishing, Inc. v. Di-Chem, Inc., 419 U.S. 601, 608 (1975) (extending liability to private creditors that make use of US state-created garnishment procedures); Sniadach v. Family Fin. Corp., 395 U.S. 337, 341–42 (1969) (same); *see also* Mitchell v. W. T. Grant Co., 416 U.S. 600, 618–20 (1974) (effecting the same extension with regard to lien procedures).

129. *Lugar*, 457 U.S. at 932–33.

130. *Id*. at 942.

same core issue arises: the actions of Private Actor A have the capacity to extend—and transform—a public process in a way that implicates the rights of (typically less powerful) Private Actor B. And when that happens, constitutional rules should follow suit.

To be sure, I am not trying to suggest that all state action jurisprudence tracks the *Skinner* Court's concern about infrastructural extension.[131] Indeed, a full theory of how the reasoning on display in *Skinner*, *Adams*, and *Lugar* meshes with the rest of the Court's state action canon—replete as it is with seemingly contradictory holdings,[132] warring legal tests,[133] and tangled vines of doctrine—must wait for another day. For present purposes, the point is that *Skinner* is not alone in recognizing that private conduct can extend and reshape the exercise of state power even if it does precisely *substitute for* such power.[134] In other words, sometimes it

131. At some level, this should not be surprising, since state action is an area of infamous confusion. *See* Sklansky, *supra* note 15, at 1233 ("[S]tate action doctrine has never received high marks for clarity."); *id*. at 1246 n.451 (compiling sources to that effect). Charles Black famously referred to state action as a "conceptual disaster area." Charles L. Black, Jr., *The Supreme Court, 1966 Term—Foreword: "State Action," Equal Protection, and California's Proposition 14*, 81 HARV. L. REV. 69, 95 (1967).

132. To take but one example, *compare* Rendell-Baker v. Kohn, 457 U.S. 830, 843 (1982) (holding that a private school established to serve particular student populations was not a state actor, in spite of its connection to the public school system), *with* Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass'n, 531 U.S. 288, 305 (2001) (holding that an intercollegiate athletic association was a state actor, because of its connection to the public school system).

133. *Compare* Blum v. Yaretsky, 457 U.S. 991, 1004 (1982) (holding that the state action inquiry centers on whether private conduct can be "attributed" to the state) *with* Evans v. Newton, 382 U.S. 296, 299 (1966) (holding that state action depends on whether private conduct is sufficiently "entwined" with governmental policies), Edmonson v. Leesville Concrete Co., Inc., 500 U.S. 614, 640 (1991) (O'Connor, J., dissenting) (explaining that state action depends on whether a private actor "exercises a power traditionally exclusively reserved to the [government]") (internal citations omitted), and Moose Lodge No. 107 v. Irvis, 407 U.S. 163, 173 (1972) (holding that where "the impetus for [constitutionally-contestable conduct] is private," the question is whether "the state . . . significantly involved itself" with the conduct). Sometimes, moreover, the Court simply dispenses with analytic benchmarks, opting instead for a "fact-bound" analysis of all relevant circumstances—whatever exactly that means. *See, e.g.*, *Brentwood Acad.*, 531 U.S. at 298. Or it opens the inquiry up to situations in which there is no state action whatsoever—save for the state's role in enforcing private agreements, which would, of course, subsume the entirety the state action requirement. *See* Shelley v. Kraemer, 334 U.S. 1, 22–23 (1948) (holding it unconstitutional for state courts to enforce "racial covenants" on the disposition of private property). *See also* Erwin Chemerinsky, *Rethinking State Action*, 80 NW. U. L. REV. 503, 526–27 (1985) (discussing the radicalism of *Shelley*); G. Sidney Buchanan, *Challenging State Acts of Authorization Under the Fourteenth Amendment: Suggested Answers to an Uncertain Quest*, 57 WASH. L. REV. 245, 259 (1982).

134. Indeed, this dichotomy—private conduct that *substitutes for* the exercise of state power v. private conduct that extends or reshapes the exercise of state power—could be one way of bringing greater analytic clarity to the Court's otherwise-chaotic state action jurisprudence. The "public function" cases and the "attribution" cases would tend to fall into the former category, while the "entwinement" cases, along with the infrastructure-focused cases that I discuss here, would tend to fall into the latter category. Another line of doctrine that would fall into the latter category is the Court's "authorization" case law, which deals with situations in which state regulation "authorizes,"

qualifies as conduct worthy of constitutional scrutiny—and corresponding protection—when Private Actor A interacts with the governance system in a way that impinges on the rights of Private Actor B. The facilitation of primary elections and the attachment of property are two examples in existing law. We ought to recognize law enforcement as a third.

C. The "Extended Infrastructure" Framework in Practice

Armed with these analogies, and the example of *Skinner* itself, we now turn to the nuts and bolts: what should courts look to when asking if law enforcement infrastructure has been extended through private surveillance activity?

Here, lower court jurisprudence contains two useful clues. The first is focusing on whether a private actor's interaction with state officials is repeated and ongoing or, instead, spontaneous.[135] Typically—and reasonably, given the Supreme Court's directive—repeated interaction has been conceptualized as evidence of an agency relationship.[136] But it also bears (albeit for different reasons) on the question of whether private surveillance has effectively extended law enforcement infrastructure. Indeed, while repeated interaction with the police is not strictly *necessary* under the infrastructural view, it promises to be true of many cases; when

---

but does not compel, constitutionally-problematic private conduct. *See, e.g.*, Reitman v. Mulkey, 387 U.S. 369, 380–81 (1967) (holding that a California referendum repealing a previously-enacted anti-discrimination ordinance effectively "authorized" private discrimination, running afoul of the Equal Protection Clause).

135. *See, e.g.*, Pleasant v. Lovell, 876 F.2d 787, 798 (10th Cir. 1989) (holding that "[t]he variety of the information obtained on [a] fishing expedition [by informant], the degree of supervision [over the informant] by [officers], and the sheer number of contacts between [the informant] and [officers] belie the notion that [the informant] merely was acting as a responsible citizen and merely delivering [evidence] to government agents."); United States v. Walther, 652 F.2d 788, 793 (9th Cir. 1981) (holding that an airline employee, who had been an official informant in the past and had received payments for his aid on several occasions, performed a luggage search, he was operating as an agent of the government). *See also* United States v. King, 212 F. Supp. 3d 1113, 1123–24 (W.D. Okla. 2015) (holding that a law enforcement search occurred when state officials directed a company's CFO to surreptitiously search for, and transmit copies of, documents relevant to an ongoing investigation). To be sure, some lower courts have also *failed* to note the importance of repeated interaction—a failure that might be attributable to the "deputization" way of thinking. *See, e.g.*, United States v. Koenig, 856 F.2d 843, 848 (7th Cir. 1988) (holding, per *Jacobsen*, that the private search rule applies to the activity of a FedEx employee who exhibited particular enthusiasm for law enforcement, having "contact[ed] the DEA at least eight times" over the course of his employment—a holding that, depending on other background facts, may well have changed under the infrastructural approach). *See also* United States v. Ramsey, 81 Fed. App'x 547, 549–50 (6th Cir. 2003) (holding that an airline employee was not operating as an instrument of the state when she opened a passenger's luggage, despite the fact that she had routinely assisted the DEA, and the DEA had approached her about formalizing an informant relationship a few days prior to the search in question).

136. *See supra* notes 108–114 and accompanying text.

private surveillance serves as the "first of line of offense" for law enforcement,[137] interactions tend to become, if not routine, certainly more than spontaneous.[138]

The second clue is lower courts' focus on the motivation behind private surveillance. Some courts have cast "law enforcement motives" as sufficient to transform otherwise-private searches into state action,[139] while others have described such motives as one ingredient in the analysis.[140] Either way, the upshot is the same: if private surveillance is guided by a desire to assist law enforcement, that should be germane to the Fourth Amendment analysis. Here, I agree with the spirit, but the specifics need clarifying. Lower courts—again understandably, given the agency frame of reference[141]—have focused on whether *collection* of data is geared toward law enforcement ends. From an infrastructural vantage point, however, the important moment is not data collection; it is the

137. *See* Brennan-Marquez, *supra* note 15, at 780.

138. *See* Coolidge v. New Hampshire, 403 U.S. 443, 490 (1971).

139. 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" (emphasis omitted) (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).

140. *See, e.g.*, United States v D'Andrea, 648 F.3d 1, 10 (1st Cir. 2011) (holding that state instrumentality test depends on a mélange of "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"); 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"). *See also* 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 (citations omitted)); United States v. Smythe, 84 F.3d 1240, 1243 (10th Cir. 1996) (for a private search to constitute state action, the government "the 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) (citations omitted)).

141. *See supra* note 106 (exploring the sense in which a would-be agent's motives could be probative—though not necessarily dispositive—of *ex post* ratification by the principal, which is understood to create a *nunc pro tunc* agency relationship, even if none existed at the moment of the disputed action).

transfer of data to law enforcement.[142] If a private actor discovers or intercepts about another private actor, and then decides to relay that information to the state *for the explicit purpose of assisting police*, that should be a tick in column of state action.[143]

So much for the lower court jurisprudence. What else, beyond (1) repeated interaction between state officials and the relevant private actor, and (2) law enforcement motivation at the time of transfer, should contribute to the infrastructural analysis? With the caveat that, as always, the answer might change as underlying practices change, I propose—with an eye to *Skinner*—two other criteria for the "extended infrastructure" test. First, at a practical level, what kind of surveillance capacity does the private actor actually possess? This question has both technological and sociological components; it depends, in other words, both on (1) how much surveillance the private actor is technically capable of performing and (2) whether the private actor wields power—relative to a surveilled party—sufficient to enable surveillance in practice. (Needless to say, in the case of a company like Google, the answers here are "a lot" and "yes.") The second criterion, which is related to—but also distinct from—the "repeated interaction" criterion, is whether law enforcement practices have changed, even just subtly or incrementally, in response to private surveillance. Has the law enforcement system evolved to accommodate private surveillance practices? If so, this is clearly probative of infrastructural change; indeed, it may be the strongest evidence of all.

To summarize, then—the question of whether law enforcement infrastructure has been extended involves (at least) four elements: first, whether data-sharing is repeated or, instead, spontaneous; second, whether the data-transfer was aimed to assist law enforcement; third, how powerfully-equipped the private actor is to perform data surveillance; and fourth, whether law enforcement practice has evolved to reflect the availability of privately-collected data. By flagging these elements, I do not mean to imply that any particular combination of them should be

142. The problem with focusing on collection is that much data is collected for non-law enforcement purposes (or for a variety of different purposes) that then ends up making its way into the state's hands. So, it would be a woefully under-inclusive test that asked only after the collection of data, given how much data might be—and in practice is—*repurposed* for law enforcement ends. Of course, this isn't to say that motivation at the collection stage is entirely de-linked from the dynamics in which this Article is interested. The problem has to do with correlation versus causation. To be sure, law enforcement motivation at the time of collection to be correlated to the extension of infrastructure. But the link is contingent, not necessary; nothing about the fact that collection is *not* motivated by a law enforcement purpose makes the collection unproblematic from a Fourth Amendment, and likewise, nothing about the fact that collection *is* motivated by a law enforcement purpose explains, in a manner independent of focusing on transfer, why the Fourth Amendment should come into play.

143. My thanks to Bethany Berger for helping me see this point.

necessary (or even sufficient) to find an extension of law enforcement infrastructure. Rather, the elements are simply meant to focus the inquiry, which, at day's end, is an overtly functional one. What does law enforcement actually look like on the ground? Are state officials capitalizing on private surveillance infrastructure in ways that raise alarm, in a manner equivalent to direct state surveillance, for expressive autonomy and democratic health?

An easy case, on this metric, would be the indiscriminate monitoring of sensitive user data by powerful information companies that routinely turn information over to law enforcement—for example, email-hashing by ISPs, which easily satisfies all four elements described above. And an easy case on the other side would be, for example, Roommate A stumbling upon contraband in Roommate B's bedroom, and opting to notify the authorities.[144] As imagined, this scenario would satisfy only one of the elements—law enforcement purpose in transferring the information—though the case could be different, of course, if Roommate A were making use of special surveillance technology (which would go to the private actor's surveillance capacity), or if, in the relevant jurisdiction, roommate-surveillance had become a routine practice and local police had set up a recurring "chain of custody" workshop to train concerned citizens about how best to handle evidence recovered in private residences.[145]

In 2012, Paul Ohm argued—presciently—that we are headed for a future in which "the police [will] shift from . . . producer to consumer of surveillance data,"[146] and the constitutional dynamics of policing will change accordingly; the question will be less one of probable cause and warrants, and more one of the scope, scale, and duration limits that

144. *See Bowers*, 594 F.3d at 525–27 (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).

145. I am not saying these changes would necessarily tip the scales toward a finding of extended law enforcement infrastructure—only that they would make the case closer. That said, one can certainly *imagine* cases along these lines, where the practices of a private individual (as opposed to an information company) would seem to affect an extension of infrastructure. For example, suppose Betty, a self-styled vigilante, uses a fleet of drones to monitor certain neighbors' activities throughout all hours of the day, reporting any suspicious activity to the police, who—having grown reliant on Betty's zealous surveillance practices—have stopped sending as many patrol units to the immediate vicinity. There is an open question, of course, as to whether Betty's use of drones constitutes a search—under California v. Ciraolo, 476 U.S. 207, 214–15 (1986) (no search when police performed aerial surveillance of defendant's backyard)—but this certainly feels like an extension of infrastructure; in other words, this conduct might escape Fourth Amendment scrutiny because it amounts to an observation in public (and would therefore fall outside the "search" category even if carried out by law enforcement). But it should not escape Fourth Amendment scrutiny simply because Betty is a private citizen.

146. Ohm, *The Fourth Amendment*, *supra* note 18, at 1348.

emanate from the "requirement of 'reasonableness'" itself.[147] Ohm even marshaled statistics to his cause: from 2000-2011 (when his article was published), the number of wiretap warrants diminished considerably,[148] even as overall data collection ballooned—suggesting, albeit circumstantially, that the amount of informal cooperation between law enforcement and the private sector has multiplied exponentially. In some sense, the future, as Ohm envisioned it, is now—making doctrinal reform all the more urgent. Before courts can flesh out what the "reasonableness" requirement demands, they must have the opportunity. And for that to happen, the Fourth Amendment's zone of coverage must expand.

Of course, the foregoing analysis—counseling Fourth Amendment limits on informal data-sharing between law enforcement and information companies *at all*—says us nothing about *which* limits to impose. Suppose I am right; when extensions of law enforcement infrastructure occur, the Constitution should pay attention. From that observation, what follows? How should courts assess the "reasonableness" of data-sharing practices that begin in the private sphere?

A full answer lies beyond the scope of this article. The question is a vast one, and the under-protectiveness of the "deputization" test—the fact that, to date, most challenges to private surveillance activity have been dismissed on threshold grounds—means that scant doctrine exists. Indeed, that is part of what makes reform so pressing. Instead of trying to fashion standards from whole cloth, I want to close by suggesting that constraints on private surveillance should take their conceptual cues from the constraints that Fourth Amendment law has traditionally placed on state surveillance. On that front, the key principle, in keeping with the concerns about individual autonomy and democratic participation discussed in Part I, is that surveillance should track wrongdoing, lest it come to resemble the general warrants and writs of assistance that motivated the Amendment's initial ratification.[149] From this principle,

147. *Id*.

148. *Id*. at 1323.

149. *See supra* note 21. *See also* United States v. Knotts, 460 U.S. 276, 284 (1983) (implying that "dragnet type law enforcement practices" are particularly suspect under the Fourth Amendment); Berger v. New York, 388 U.S. 41, 65 (1967) (Douglas, J., concurring) (explicating the prohibition against general warrants as a concern about "dragnet," "sweeping" intrusions upon "those not even suspected of crime"). The Fourth Amendment's aversion to dragnet surveillance is a prominent theme among scholars. *See, e.g.*, Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254, 279–86 (2011) (explaining that dragnet surveillance has been permitted by the Court only as a species of "administrative search"); Strandburg, *supra* note 26, at 667 ("Supreme Court opinions have repeatedly recognized the danger that technological advances might turn plain view observation into constitutionally troubling dragnet searches."). *Cf*. Miriam Baer, *Secrecy, Intimacy, and Workable Rules*: *Justice Sotomayor Stakes Out the Middle Ground in* United States v. Jones, 123 YALE L.J. F.

numerous practical criteria follow. For one thing, how precisely does a given surveillance practice target wrongdoing, as opposed as to sweeping in innocent conduct? There is clearly a distinction between, say, email hashing that exclusively targets known contraband and data analyses that draw inferences from the contents of communication, the latter of which plainly infringes on expressive activity.[150] For another thing, how frequent is the surveillance? There is likewise a clear distinction between constant, indiscriminate monitoring—of *all* users, at *all* times—and more targeted monitoring, such as surveillance that ramps up in the event of suspected fraud.[151]

These two examples are meant to be illustrative, not exhaustive. Ultimately, the point is that reasonableness analysis should proceed with a careful eye toward the danger we have been trying, these many generations, to avoid: a social order in which everyone—no matter their identity, their background, or their conduct—is made to feel like a criminal, subject to the watchful gaze of the state.[152] When that happens, whether by direct state surveillance or through partnerships between state officials and the private sector, democracy withers. Which means, as elsewhere in Fourth Amendment law, that a balance must be struck.

393, 394, 407 (2014) (suggesting that the Alito and Sotomayor concurrences in *United States v. Jones* stem from anti-dragnet principles).

150. *See* United States v. Place, 462 U.S. 696, 707 (1983) (explaining that dog sniffs are not "searches" at all, because they only target contraband—and implying, as a general matter, that surveillance practices become more reasonable the more narrowly they target contraband without spilling over into innocent activity); Salgado, *supra* note 7, at 44–46 (extending the logic of *Place* to digital contexts). *See also* Kyllo v. United States, 533 U.S. 27, 38–39 (2001) (suggesting that a technology that effectively filter out all "intimate details" from collected data might not constitute a search at all).

151. For recitations of a similar principle in the case law, see, for example, Maryland v. Garrison, 480 U.S. 79, 84 (1987) ("The [] purpose of [the Fourth Amendment's] particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the [f]ramers intended to prohibit."). From there, things get complicated, because the *level* of suspicion required to justify a given search or seizure varies with context. Some categories of "administrative search," for example, require only the availability of "pre-compliance review." *See, e.g.*, City of Los Angeles v. Patel, 135 S. Ct. 2443, 2453 (2015) (striking down a statute requiring hotel managers to turn over guest lists to law enforcement, with no opportunity for administrative review). Furthermore, some non-administrative—i.e., law enforcement—searches and seizures require only "reasonable suspicion," which no one precisely knows how to define, but everyone agrees is lower than probable cause.

152. *See* Slobogin, *supra* note 23, at 124–26 (elaborating the point and compiling sources in support).

V. CONCLUSION

If the government wishes to capitalize on the surveillance infrastructure built and maintained by private companies, it has two options. The first is to compel companies to turn over data; the second is to coax them into turning it over voluntarily. *Carpenter* is poised to limit in the first dynamic, but—due to contingent features of Fourth Amendment doctrine—it will likely have nothing to say about the second.

That should give us pause. When officials draw on private surveillance technology to amass data whose collection, if pursued by the government directly, would be subject to Fourth Amendment limits, should it matter exactly *how* the officials do so? No, I have argued—the question should be posed in functional terms, with an eye toward the mechanics of data collection and data-sharing on the ground. Just as the third-party doctrine exempts wide swaths of data surveillance from scrutiny by allowing the state to extract information from companies, the "deputization" framework exempts wide swaths of data surveillance from scrutiny by permitting companies to funnel information to the government. Six of one; half a dozen of the other. Reform is long overdue, as Fourth Amendment doctrine races to keep up with information technology. The hope motivating this article is that reform will be holistic, not partial; lasting, not illusory.