California Law Review

VOL. 102 OCTOBER 2014 NO. 5

Too Much Information: How Not to Think About Privacy and the Fourth Amendment

David Alan Sklansky*

Fourth Amendment law today is overloaded with information: not just in the sense that the explosive growth of digitized information requires rethinking traditional rules of search and seizure, but also and more importantly in the sense that a preoccupation with data flows has led to the neglect of important dimensions of privacy. There is no doubt that the control of personal information is an important value and one uniquely threatened by the rise of social media, the proliferation of technological surveillance, and the arrival of Big Data. But the reduction of privacy to control over information has made it more difficult to think sensibly about the distinctive threats raised by government searches, and it is partly to blame for the growing and unwarranted sense that the Fourth Amendment should be decoupled from privacy—because the concept of privacy is meaningless, because privacy is dead or dying, or because the main threats to privacy are largely orthogonal to the chief dangers posed

* Professor of Law, Stanford Law School. For guidance and criticism, I thank Mitch Berman, James Forman Jr., Mary Anne Franks, Alon Harel, Chris Hoofnagle, Sarah Igo, Chris Kutz, Tracey Meares, Martha Minow, Melissa Murray, Michael Musheno, Robert Post, Pamela Samuelson, Jonathan Simon, Jennifer Urban, Shane Witnov, workshop participants at UC Berkeley School of Law, Loyola Law School, Los Angeles, and University of Texas School of Law, and participants in the 2014 Criminal Justice Roundtable at Harvard. Tatiana August-Schmidt, Hamilton Jordan Jr., Tanay Kothari, Corey Laplante, Erica Posey, and Leah Romm provided excellent research assistance.

by law enforcement. Search-and-seizure law would be better served by an understanding of privacy rooted in respect for a zone of refuge and informed by privacy's longstanding associations with enclothement, retreat, and personal sovereignty. This alternative conception of privacy—privacy as refuge—should also be attentive to the relational nature of privacy, the connection between privacy and civility, and the effects of privacy violations on the perpetrators as well as the victims.

INTRODUCTION

Privacy has long been thought the core concern of the Fourth Amendment, and there is more talk about privacy today than ever before. Nonetheless, the connection between privacy and constitutional restrictions on law enforcement has rarely been less clear.

For roughly the last quarter of the twentieth century, there was a consensus among judges and legal scholars about the relationship between privacy and the Fourth Amendment right "against unreasonable searches and seizures." The consensus was that privacy was what the Fourth Amendment chiefly protected, and that this was as it should be, because respect for privacy by government agents, especially law enforcement agents, was what prevented a democracy from sliding into totalitarianism. Accordingly, the test for whether a particular government action fell within the category of "searches and seizures" regulated by the Fourth Amendment was, first and foremost, whether

it infringed on "reasonable expectations of privacy."[1] If it did, the action was unconstitutional unless it was itself "reasonable," which generally meant that absent a judicially defined exception it had to be based on probable cause and carried out pursuant to a warrant.

That consensus has unraveled. The problem is not simply doctrinal disarray, although there is plenty of that—more, probably, than at any time since the 1960s. The problem extends to the underlying philosophy of search-and-seizure law, and in particular to the idea that the Fourth Amendment's job is to protect privacy. That idea, in turn, has been put into doubt by uncertainty about how privacy can best be defined, and whether it can be defined at all.

The sources of doctrinal disarray are twofold. First, exceptions to the warrant and probable cause requirements have proliferated and in some cases grown so open-ended that the Supreme Court now treats those requirements as special applications of the constitutional requirement of "reasonableness," relevant only in narrow circumstances. One of the former "exceptions" to the warrant and probable cause requirements, the "special needs" doctrine, has been particularly important in this transformation. The original idea was that searches based on some "special need," beyond the "normal" imperatives of law enforcement—needs like safety and discipline in public schools—might best be regulated through tailor-made substitutes for the warrant and probable cause requirements.[2] Over time, though, the doctrine has morphed into a rationale for upholding virtually any search not conducted by police officers in a run-of-the-mill criminal investigation, as long as it is carried out under procedures that strike the Supreme Court as "reasonable." And this has led to predictable questions about why the government should face more obstacles in searching for evidence of, say, murder or sexual assault, than in checking for drunk or unlicensed drivers.

The second major source of disarray in current Fourth Amendment law is persistent and growing confusion about the meaning and continuing validity of the "reasonable expectations of privacy" test. Nothing illustrates the extent of the confusion better than the manner in which the Supreme Court decided *United States v. Jones*, the recent, high-profile case involving satellite tracking of a drug suspect's car on public highways.[3] Three decades earlier, the Court had ruled that a "person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another,"[4] but all nine Justices agreed that the monitoring in *Jones* was a "search" under the Fourth Amendment. They did so for different reasons. Justice Scalia, writing for a five-member majority, focused on the physical trespass involved when government agents attached a transmitter to the

1. Katz v. United States, 389 U.S. 347, 362 (1967) (Harlan, J., concurring).
2. *E.g.*, New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring).
3. 132 S. Ct. 945 (2012).
4. United States v. Knotts, 460 U.S. 276, 281 (1983).

defendant's car; Justice Scalia reasoned that the "reasonable expectations of privacy" test supplemented, but did not replace, an older, trespass-based test for what the Fourth Amendment covered.[5] Justice Alito, writing for a four-Justice minority, adhered to the longstanding, consensus view that the Court had done away with the trespass test in *Katz v. United States*[6] in favor of the "reasonable expectations of privacy" approach.[7] But Justice Alito criticized the circularity and subjectivity of the *Katz* test (echoing complaints long voiced by scholars and by other members of the Court[8]), and he departed from conventional understandings of *Katz* in reasoning that satellite monitoring of vehicles' movements on public highways *can* infringe "reasonable expectations of privacy," depending on how long it continues. Justice Scalia, in turn, criticized the concurrence for introducing "novelt[ies]" and "thorny problems" of line-drawing into Fourth Amendment jurisprudence, but even he conceded that the Court would need to face those problems if it confronted a satellite monitoring case that did not involve a physically installed transmitter.[9] To further complicate matters, Justice Sotomayor, who provided the fifth vote for Justice Scalia's opinion in *Jones*, also wrote a separate, concurring opinion agreeing with Justice Alito that there would have been a Fourth Amendment "search" even without the physical trespass,[10] and calling for reconsideration of the longstanding, repeatedly reaffirmed—and heavily criticized—doctrine that "an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[11]

The upshot of *Jones* is that "reasonable expectations of privacy" are no longer the exclusive test for a "search" under the Fourth Amendment; that the heavily reviled trespass test, long assumed dead, is very much alive; that

5. United States v. Jones, 132 S. Ct. 945, 950–53 (2012).

6. 389 U.S. 347 (1967). The following Term, Justice Scalia again declared for a five-Justice majority that *Katz* simply "add[ed] to the baseline" provided by the old, trespass-based view of the Fourth Amendment. Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013).

7. *Jones*, 132 S. Ct. at 959–60 (Alito, J., concurring).

8. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001) (Scalia, J.); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 106–07 & n.23 (2008). The Court nicely illustrated the potential of the *Katz* test for circularity the following term when it upheld the routine collection of DNA samples from felony arrestees, reasoning in part that arrestees have reduced "expectations of privacy"—and citing for that proposition earlier decisions by the Court authorizing searches incident to arrest. *See* Maryland v. King, 133 S. Ct. 1958, 1969–70 (2013). "Reasonable expectations of privacy" can be defined by social norms rather than legal rules, see, for example, Rubenfeld, *supra* , at 107, but the *Katz* test runs into a different kind of circularity: the tendency over time for people to become accustomed to governmental violations of privacy. *See* Frederick Schauer, *Internet Privacy and the Public-Private Distinction*, 38 JURIMETRICS J. 555, 560–64 (1998); *infra* notes 91–99 and accompanying text.

9. *Jones*, 132 S. Ct. at 953–54. For a longer discussion of the difficulties introduced by Justice Alito's approach, see Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).

10. *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) (citing Smith v. Maryland, 442 U.S. 735, 742 (1971) and United States v. Miller, 425 U.S. 435, 443 (1976)).

11. *Id.* at 957.

"reasonable expectations of privacy" may or may not depend, in unexplained ways, on how long surveillance is conducted and on what kind of crime is being investigated; and that at least one Justice wants to reconsider the well-entrenched but highly unpopular assumption that information voluntarily shared with third parties loses any Fourth Amendment protection. *Jones* thus gives new urgency to the complaints law professors have been making for decades about the confusion and disarray of search-and-seizure law.

But the doctrinal disarray is only the tip of the iceberg. Lurking below are more fundamental uncertainties about the mission of the Fourth Amendment and the nature of privacy—uncertainties that reflect a larger unraveling of the late twentieth-century consensus about the constitutional regulation of searches and seizures. That consensus rested in part on assumptions that seemed so obvious and so basic they often went unarticulated: that there was such a thing as privacy, that it was important for democracy, that it was threatened in particularly important ways by widespread strategies of law enforcement, that the dangers those tactics posed to privacy were among their greatest costs, and that courts and the law were critical tools in containing those dangers. None of these assumptions seems obvious today, in part because decades of scholarship have thrown each into doubt. Academics, along with popular writers, have questioned whether there is any real content to the concept of privacy, whether there is any hope of preserving privacy in the modern world, and whether the loss of privacy is truly worth mourning. To the extent that privacy exists, is important, and is threatened, the threats today seem to come more from the private sector—from Internet search engines, social networking sites, credit reporting agencies, and private surveillance systems—than from government investigators. Recent revelations about government monitoring of electronic communications have drawn some of the attention of privacy scholars and privacy activists back to the government. But the concerns have centered on intelligence gathering by national security officials working in cooperation with telecommunication companies, not on the day-to-day operations of the criminal justice system. The threats that law enforcement poses to privacy seem dwarfed not just by commercial threats to privacy but also by other threats posed by law enforcement: racial profiling, police violence, and mass incarceration. As a result, privacy scholars by and large remain less interested in the police than in Google, Facebook, and Equifax, and criminal justice scholars are less interested in privacy than in fairness, proportionality, and legitimacy.

This article is about the relationship between privacy and constitutional restrictions on law enforcement in the information age. My approach will be largely cautionary and contrarian. I will challenge two ideas about privacy and the Fourth Amendment that have emerged over the past few decades. Each of these ideas is a reaction and a useful corrective to aspects of the consensus understanding of privacy and the Fourth Amendment that held sway twenty-five years ago, but each can be—and has been—carried too far.

The first idea I want to challenge is that we should forget about privacy. There are three versions of this idea. One is conceptual, one is empirical, and one is specific to criminal justice. The conceptual reason for giving up on privacy is that the term is so vague as to be empty: it simply means too many different things. We would do better to replace any invocations of privacy with invocations of whatever underlying value the term is standing in for: bodily autonomy, or control over information about oneself, or whatever. In contrast, the empirical reason to forget about privacy—to "get over it," in the often-quoted words of one computer industry executive[12]—is that technological and social developments have made or soon will make privacy impossible, whether we like it or not.[13] The criminal-justice-specific reason for giving up on privacy is that the main threats to privacy no longer come from law enforcement, and that the main threats that law enforcement poses today have to do with things other than privacy.

As I will explain, one reason to resist the latter two arguments against worrying about privacy is that each draws in part on a particular idea about what privacy means. Each equates privacy, more or less, with what used to be called "informational privacy": the ability to control the dissemination and use of information about oneself. There is no doubt this is an important interest and one that is uniquely threatened by the advent of social media, the proliferation of technological surveillance, and the rise of Big Data. But the reduction of privacy to control over information is the second of the two main ideas I want to challenge here. Fourth Amendment law is overloaded with information: not just in the sense that the explosive growth of digitized information requires rethinking traditional rules of search and seizure, but also in the sense—and this is what I want to stress—that a preoccupation with data flows has led to the neglect of some important dimensions of privacy.

Part I of this Article will discuss the arguments for decoupling search-and-seizure law from privacy, and the reasons those arguments are ultimately unpersuasive. Part II will challenge the reduction of privacy to informational privacy. Parts III and IV will sketch a different understanding of privacy, rooted in respect for a zone of personal refuge, and will explore the implications of this view for Fourth Amendment law.

I want to be clear at the outset about certain claims I am not making. I am not asserting that what is sometimes called "informational privacy" is

12. *See* Polly Sprenger, *Sun on Privacy: 'Get Over It'*, WIRED, (Jan. 26, 1999), http://archive.wired.com/politics/law/news/1999/01/17538 (quoting Scott McNealy).

13. *See, e.g.*, Thomas L. Friedman, *Four Words Going Bye-Bye*, N.Y. TIMES, May 21, 2014, at A23 (arguing that "privacy is over," because "[i]t is now so easy for anyone to record, film, or photograph anyone else anywhere and share it with the world . . . that we are all now on Candid Camera"); Michael Arrington, *OK You Luddites, Time to Chill Out on Facebook Over Privacy*, TECHCRUNCH (Jan. 12, 2010), http://techcrunch.com/2010/01/12/ok-you-luddites-time-to-chill-on-facebook-over-privacy/ (arguing that "privacy is already really, really dead," because "[e]verything we do, everything we buy, everywhere we go is tracked and sitting in a database somewhere").

unimportant, or that it is not really a form of privacy, or that it is tangential to the mission of the Fourth Amendment. We live in the information age, and no area of law—certainly not search-and-seizure law—can safely ignore the way that digitized data flows are transforming our lives. But information is not everything.

I.
DOES PRIVACY MATTER?

The Constitution does not mention privacy, and it is not obvious that the "unreasonable searches and seizures" banned by the Fourth Amendment should be defined by reference to privacy. Until the 1960s, in fact, the constitutional law of searches and seizures paid more attention to property and trespass than to privacy. Justice Brandeis famously argued in *Olmstead v. United States*[14] that the Fourth Amendment protected against any "unjustifiable intrusion by the government upon the privacy of the individual," but he wrote in dissent.[15] Even the majority opinion in *Katz v. United States*[16]—the decision generally thought to have vindicated Justice Brandeis's position in *Olmstead*[17]—went out of its way to declare that "the Fourth Amendment cannot be translated into a general constitutional 'right to privacy,'" and that the rights provided by that provision "often have nothing to do with privacy at all."[18] But a concurring opinion in *Katz* explicitly tied Fourth Amendment protections to "reasonable expectations of privacy"[19]—to those "actual" expectations of privacy "that society is prepared to recognize as reasonable"[20]—and the Court soon embraced that formulation and made it the centerpiece of its search and seizure jurisprudence.[21] By the end of the 1960s, it was conventional wisdom that the Fourth Amendment was concerned, first and foremost, with privacy. Even today, that proposition is often treated as close to self-evident.[22]

A growing number of scholars, though, want to sever the link between privacy and the Fourth Amendment. They are motivated in part by a sense that privacy is dead or dying: that if the Fourth Amendment protects only privacy,

14. 277 U.S. 438 (1928).

15. *Id.* at 478 (Brandeis, J., dissenting).

16. 389 U.S. 347 (1967).

17. For the conventional understanding of *Katz*, see David A. Sklansky, *Katz v. United States: The Limits of Aphorism*, *in* CRIMINAL PROCEDURE STORIES 223, 223 (Carol S. Steiker ed., 2006).

18. 389 U.S. at 350. Justice Stewart, the author of the majority opinion in *Katz*, edited his law clerk's draft to remove two passages suggesting that the Fourth Amendment "protects . . . privacy" or "secures personal privacy." *See* David Alan Sklansky, *A Postscript on* Katz *and Stonewall: Evidence from Justice Stewart's First Draft*, 45 U.C. DAVIS L. REV. 1487, 1491–92 (2012).

19. 389 U.S. at 362 (Harlan, J., concurring).

20. *Id.* at 361.

21. *See* Terry v. Ohio, 392 U.S. 1, 9 (1968); Sklansky, *supra* note 17, at 254.

22. *See, e.g.*, JEANNIE SUK, AT HOME IN THE LAW: HOW THE DOMESTIC VIOLENCE REVOLUTION IS TRANSFORMING PRIVACY 124 (2009) (calling privacy "the concept at the core of the Fourth Amendment").

there soon will be little left for it to protect.[23] But most of them also think there are and always have been more important values at stake when assessing government searches and seizures.[24] As a group, these writers therefore raise two objections to the traditional idea that the Fourth Amendment has a close connection with privacy. First, they suggest that we would do well to forget about privacy because it has vanished or is rapidly disappearing. This is a version of "get over it." Second, regardless whether privacy still exists and is worth protecting, they argue that it is tangential to the main issues raised by government searches and seizures.

I will engage each of these arguments below. First, though, I want to address a more basic question: Is the concept of privacy too vague or multifaceted to be helpful? A respectable body of scholarship says that it is. So before asking whether privacy is dead or irrelevant, it makes sense to ask whether the concept has any real content.

A. Is Privacy Meaningless?

The re-anchoring of search-and-seizure law in privacy at the end of the 1960s was part of a broad intellectual trend. Concerns about privacy ballooned in the 1960s. Best-selling books warned that privacy was under attack and that if privacy disappeared, freedom and democracy would disappear along with it.[25] Scholarly attention to privacy also increased dramatically, and the academic writing, while less alarmist than the popular literature, tended to agree that privacy was under attack and that the attack endangered liberty and self-government.[26] Scholars and popular writers alike linked totalitarianism with an absence of privacy; it became common, even ubiquitous, to cite George Orwell's *Nineteen Eighty-Four* for what life would look like if attacks on privacy were not resisted.[27] The 1960s were also, of course, when the Supreme

23. *See, e.g.*, Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309 (2012); Rubenfeld, *supra* note 8, at 118; Scott E. Sundby, *"Everyman" 's Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1758–59, 1775 (1994).

24. *See, e.g.*, Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307 (1998); Thomas P. Crocker, *From Privacy to Liberty: The Fourth Amendment After* Lawrence, 57 UCLA L. REV. 1 (2009); Rubenfeld, *supra* note 8, at 103–04, 108; Sundby, *supra* note 23, at 1777–83.

25. *See* MYRON BRENTON, THE PRIVACY INVADERS (1964); VANCE PACKARD, THE NAKED SOCIETY (1964).

26. *See, e.g.*, ARTHUR RAPHAEL MILLER, THE ASSAULT ON PRIVACY (1971); Charles Fried, *Privacy*, 77 YALE L.J. 475 (1968).

27. *See, e.g.*, PACKARD, *supra* note 25, at 11, 25; *see also* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRATION OF SOCIAL LIFE 93 (2010). There is a book to be written about the role of *Nineteen Eighty-Four* in discussions of privacy. It is remarkable how persistently the novel is put forward, even today, not just as an illustration of what can happen when privacy disappears, but as *the* definitive statement of how a world without privacy would look. By now there is a long tradition of complaining wearily about invocations of Orwell in privacy debates, but even the writers making those complaints often find it difficult to resist the book's rhetorical pull. *See,*

Court began to protect intimate autonomy under the rubric of a penumbral right to privacy.[28]

Americans saw assaults on privacy in many places in the 1960s: not just in government surveillance and in regulations of intimate association, but in employment screening, both public and private; in workplace monitoring; in loyalty oaths and polygraphs; in personality testing of schoolchildren; in investigations by insurance companies and credit bureaus; in the encroaching noise and commotion of urban life; and even in the introduction of additives to foods and drinking water.[29] The wide diversity of concerns grouped together as threats to privacy led to debates among scholars about how best to define the concept. Those debates took on new urgency when the Supreme Court ruled in 1973 that broad bans on abortion, like overly intrusive bans on contraceptive sales, violated the constitutional right to privacy.[30]

Notwithstanding the escalating uncertainty about what privacy meant, there was broad, if usually unstated, agreement that it meant *something*, and something important. Judges as well as scholars assumed that there was such a thing as privacy and that it mattered; the legal debate was simply about how much and what kind of protection privacy received. Some members of the Supreme Court—including Justice Stewart, who wrote the majority opinion in *Katz*—denied there was a constitutional right of privacy, but their point was jurisprudential, not philosophical. Much the same could be said of Dean William Prosser, who argued influentially in 1960 that tort cases purporting to vindicate privacy in fact recognized "four distinct and only loosely related torts."[31] Prosser disputed the existence of a comprehensive "right of privacy" in tort law,[32] much as Justice Stewart later claimed there was no broad "right to privacy" in constitutional law. But neither challenged the usefulness of the underlying idea of privacy, except insofar as it was thought to be protected by an all-inclusive, legally enforceable right.

---

e.g., ALAN F. WESTIN, PRIVACY AND FREEDOM 4, 210 (1967); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1945, 1948 (2013). Over time, though, the taken-for-granted meaning of *Nineteen Eighty-Four* in privacy discussions has shifted: in keeping with the reduction of privacy to informational privacy, today the book is generally seen as a warning not so much about privacy in general as about surveillance. *See, e.g.*, Richards, *supra*, at 1948; Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1651–53 (1999). That seems reductive, but then it is awkward to describe some of what is most chilling in *Nineteen Eighty-Four*—the evisceration of the past, the cultivation of hate, the enfeeblement of language, not to mention the imprisonment and torture—as invasions of "privacy" in any conventional sense.

28. *See* Griswold v. Connecticut, 381 U.S. 479, 484–86 (1965) (holding that laws that criminalized the use of contraceptives were unconstitutional violations of the unenumerated right to marital privacy).

29. *See, e.g.*, BRENTON, *supra* note 25; PACKARD, *supra* note 25.

30. *See* Roe v. Wade, 410 U.S. 113 (1973).

31. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 422 (1960).

32. This aspect of Prosser's argument was not entirely novel. *See, e.g.*, Frederick Davis, *What Do We Mean by "Right to Privacy"?*, 4 S.D. L. REV. 1 (1959).

A broader challenge arose in the 1970s. The philosopher Judith Jarvis Thompson argued in a particularly influential essay that the whole idea of a moral right to privacy was invariably "derivative" of other, more basic claims, and that dropping the rhetoric of privacy altogether would advance clear thinking.[33] By the 1980s, this kind of skepticism or "reductionism" was common in scholarly treatments of privacy.[34] And today it has become something of a truism in privacy scholarship that it is "misleading and confining even to try to provide a general definition of privacy."[35] The comparative legal scholar James Whitman, for example, argues that privacy in the United States basically means "freedom from intrusions by the state, especially in one's home," whereas in Europe privacy means the right to control one's public image.[36] "There is no such thing," he says, "as privacy *as such*. The battle, if it is to be fought, will have to be fought over more fundamental values than that."[37]

Probably the most familiar version of this argument comes from the privacy law scholar Daniel Solove, who explains that privacy is "a plurality of different things,"[38] lacking any "'essential' or 'core' characteristics."[39] Solove identifies sixteen kinds of privacy infringements, ranging from surveillance to "decisional interference," and he groups them into four clusters: "information collection," "information processing," "information dissemination," and a catchall category of "invasion."[40] In defense of his approach, Solove enlists Ludwig Wittgenstein, who Solove takes to have argued that "certain concepts might not have a single common characteristic; rather, they draw from a common pool of similar elements."[41] Privacy, Solove suggests, is one of those

33. Judith Jarvis Thompson, *The Right to Privacy*, 4 PHIL. & PUB. AFF. 295, 313 (1975).

34. Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 422 (1980); *see also* JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 21, 39 n.1 (1996).

35. Colin J. Bennett & Rebecca Grant, *Introduction*, *in* VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE 3, 5 (Colin Bennett & Rebecca Grant eds., 1999); *see also* Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1339 (1992); Peter Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 951, 975 (2006); Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 299 (1983).

36. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1161 (2004).

37. *Id.* at 1221.

38. DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 24 (2011).

39. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 8 (2008). For examples of Solove's influence, see Crocker, *supra* note 24, at 9; Peter Galison & Martha Minow, *Our Privacy, Ourselves in the Age of Technological Intrusions*, *in* HUMAN RIGHTS IN THE 'WAR ON TERROR' 258, 269 (Richard Ashby Wilson ed., 2005); *see also* Leslie Meltzer Henry, *The Jurisprudence of Dignity*, 160 U. PA. L. REV. 169, 188–89 (2011). *See generally* Richard B. Bruyer, *Privacy: A Review and Critique of the Literature*, 43 ALBERTA. L. REV. 553 (2006).

40. SOLOVE, *supra* note 39, at 10–11.

41. SOLOVE, *supra* note 39, at 9 (citing LUDWIG WITTGENSTEIN, PHILOSOPHICAL INVESTIGATIONS (G. E. M. Anscombe trans., 3d ed. 1958)).

concepts, consisting of "many different yet related things"[42]—things that share, in Wittgenstein's terminology, a "family resemblance."[43]

Wittgenstein was more radical than Solove makes him out to be,[44] but put that aside for the moment. We do not need Wittgenstein to tell us that some words have multiple meanings, nor do we need a dictionary to recognize that "privacy" is one of those words. Privacy can mean not being asked questions: "I'll respect your privacy by not inquiring." Privacy can mean solitude and freedom from observation: "Can we get some privacy in here?" Privacy can mean restraint in using or disseminating personal information: "Facebook needs a better privacy policy." And privacy can mean freedom from interference: "Bans on abortion violate a woman's right to privacy."

It is far from obvious, though, that this diversity of meanings makes it fruitless to try to formulate a unitary definition of privacy. It simply means that any such definition must differ in part from the way the term is used in everyday conversation and in legal doctrine. As Solove himself acknowledges, "[a] conception of privacy is different from the usage of the word 'privacy.'"[45] The conception can vary from the usage. The word "science" gets employed in some odd ways—calling boxing, for example, "the sweet science"—but science can be defined more narrowly and precisely. Part of the point of a definition, after all, "is to make our referential language more exact."[46] Any persuasive definition of science, or of privacy, will need to overlap to some extent with the way the term under consideration is typically used, but it might depart from common usage in some ways, too. It is not a telling objection to a conception of "science" that it excludes boxing.

Some people, of course, *do* find that a telling objection; they say it is senseless to define any term in a way that diverges from its actual usage. This appears to have been Wittgenstein's position. Wittgenstein did not suggest simply that "certain concepts" resist simple definition because they have a "series of meanings."[47] He was advancing an anti-essentialist theory of language: words generally could be understood, he suggested, only by looking at how they were used.[48] The meaning of the word "game," for example,

---

42. *Id.*

43. LUDWIG WITTGENSTEIN, PHILOSOPHICAL INVESTIGATIONS, at ¶ 67 (G. E. M. Anscombe trans., 3d ed. 2001).

44. *Cf.* Paul M. Schwartz & Karl-Nikolaus Peifer, *Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better Than One Unitary Concept?*, 98 CALIF. L. REV. 1925, 1940 (2010) (noting that although Solove "explicitly references Ludwig Wittgenstein's concept of a 'family resemblance' as his chief paradigm, his basic methodology is shared by Prosser").

45. SOLOVE, *supra* note 39, at 13.

46. BERNARD SUITS, THE GRASSHOPPER: GAMES, LIFE AND UTOPIA 166 (Broadview Press ed. 2005).

47. Henry, *supra* note 39, at 188.

48. *See* WITTGENSTEIN, *supra* note 43, at ¶¶ 65–70, 75. To be consistent, Wittgenstein took this approach even with the meaning of "meaning": "For a *large* class of cases—*though not for all*—in

consisted for Wittgenstein in the ways in which people employed that term.[49] And there were no characteristics shared by all of the things people called "games," only "a complicated network of similarities overlapping and criss-crossing," like "the various resemblances between members of a family."[50] Games had no essential features, no core identity. Nor did they fall into a series of well-defined subcategories. They simply were all the things called "games."

Wittgenstein's ideas about language have long been popular with legal scholars.[51] It is instructive, though, that scholars who study games as games, not just as an illustration of how language works, almost invariably do exactly what Wittgenstein suggested was futile: they try to identify the core, unifying characteristics of games. They do so despite recognizing that any formal definition of "game" will differ from the everyday uses of the term. Their purpose in trying to *define* games is to help them *understand* games: to help them recognize what is valuable about games and what is necessary for games to work.[52]

Scholars arguing about the meaning of privacy have been similarly motivated. They have not been interested simply in a positive, lexicographical account. Theories of privacy are invariably normative as well as descriptive, employing some version of reflective equilibrium.[53] The point of talking about privacy is to help to identify what is valuable about it and how it is fostered or endangered. The problem with dropping the language of privacy, or treating it

---

which we employ the word 'meaning' it can be defined thus: the meaning of a word is its use in the language." *Id.* at ¶ 43 (second emphasis added).

49. *See id.* at ¶ 69.

50. *Id.* at ¶¶ 66–67.

51. *See, e.g.*, P.S. ATIYAH, ESSAYS ON CONTRACT 5 (1986); H.L.A. HART, THE CONCEPT OF LAW 234 (1961); JEREMY WALDRON, THE RIGHT TO PRIVATE PROPERTY 49–50 (1988); Stuart P. Green, *The Concept of White Collar Crime in Law and Legal Theory*, 8 BUFF. CRIM. L. REV. 1, 29 (2004); Kent Greenawalt, *Religion as a Concept in Constitutional Law*, 72 CALIF. L. REV. 753, 763–64 (1984); Andrew Koppelman, *The Troublesome Religious Roots of Religious Neutrality*, 84 NOTRE DAME L. REV. 865, 880–81 (2009); Frederick Schauer, *The Best Laid Plans*, 120 YALE L.J. 586, 617 (2010).

52. *See, e.g.*, JANE MCGONIGAL, REALITY IS BROKEN: WHY GAMES MAKE US BETTER AND HOW THEY CAN CHANGE THE WORLD 20–22 (2011); KATIE SALEN & ERIC ZIMMERMAN, RULES OF PLAY: GAME DESIGN FUNDAMENTALS 72, 82 (2004); SUITS, *supra* note 46. Bernard Suits, who proposed a particularly influential definition of games, argued plausibly that Wittgenstein had failed to follow his own advice to "*look and see* whether there is anything common" to games: "He looked, to be sure, but because he had decided beforehand that games are indefinable, his look was fleeting, and he saw very little." SUITS, *supra* note 46, at 21 (quoting WITTGENSTEIN, *supra* note 43, at ¶ 66). For criticism of Suits's account, see, for example, Mitchell N. Berman, *Sprints, Sports, and Suits*, 40 J. PHIL. SPORT 163 (2013).

53. On reflective equilibrium, see JOHN RAWLS, A THEORY OF JUSTICE 48–51 (1971); John Mikhail, *Rawls' Concept of Reflective Equilibrium and its Original Function*, *in* A Theory of Justice, 3 WASH. U. JUR. REV. 1 (2011).

simply as a label applied to other, more basic interests, is that we can lose sight of what is genuinely distinctive and important about privacy.[54]

This assumes, of course, that there *is* something distinctive and important about privacy. Even if Wittgenstein was wrong about games, it does not follow that a concept lies behind every abstract noun: the fact that some concepts are definable does not mean that every concept is definable.[55] Some words really may be so vague that they impede careful thinking. Some people think, for example, that "democracy" has lost whatever meaning it once had and has become little more than a kind of verbal clapping of approval.[56] Others have a similar view of "equality" as a legal or political ideal.[57] I think they are wrong about those concepts,[58] but like most people I have my own candidates for concepts so empty or ambiguous we might do better to discard them. How can we tell if privacy belongs in that category? Ultimately the test is whether we can find or devise an account of privacy that seems plausible and helpful, or if we find reasons to think that the search for such an account is valuable even if the objective remains elusive. The main lesson for now is not to reject these possibilities at the outset.

Three other points are also worth noting. First, the language used in discussions of privacy, particularly in the 1960s and 1970s, provides suggestive evidence there is in fact a distinctive and important concept lying behind the term. Two features of that language are striking: the repeated reference to a "realm," "sphere," or "domain" of privacy, and the use—prevalent until quite recently—of the metaphor of stripping naked when describing invasions of privacy. Both go back well over a century. James Fitzjames Stephen, for example, wrote of the "sphere" and "province" of privacy, and he took, as the paradigmatic invasion of that sphere, the practice of religious confession in which a person was asked to "strip his soul stark naked for the inspection of another."[59] References to the realm or sphere or domain of privacy, with their

54. In this regard see Ruth Gavison's helpful discussion of privacy "reductionism" in Gavison, *supra* note 34, at 460–67.

55. Even Bernard Suits, a particularly forceful critic of Wittgenstein's anti-essentialism, suggested one should "begin with the hypothesis that some things are definable and some are not, and that the only way to find out which are which is to follow Wittgenstein's excellent advice and *look and see*." SUITS, *supra* note 46, at 22. Brian Leiter makes a similar point in connection with the concept of religion in constitutional law: "[T]oo many scholars have . . . fallen back on the Wittgensteinian habit of not even attempting an analysis of religion on the grounds that it is a family resemblance concept. Perhaps that will prove the best that we can do, but we should at least first try to do better before giving up." Brian Leiter, *Foundations of Religious Liberty: Toleration or Respect?*, 47 SAN DIEGO L. REV. 935, 937 (2010).

56. *See, e.g.*, Edward L. Rubin, *Getting Past Democracy*, 149 U. PA. L. REV. 711 (2001).

57. *See, e.g.*, Peter Westen, *The Empty Idea of Equality*, 95 HARV. L. REV. 537 (1982).

58. *See* DAVID ALAN SKLANSKY, DEMOCRACY AND THE POLICE 10, 102–04 (2008).

59. JAMES FITZJAMES STEPHEN, LIBERTY, EQUALITY, FRATERNITY 107 (Stuart D. Warner ed., Liberty Fund 1993) (1873).

connotations both of sovereignty and physical space,[60] were ubiquitous in legal, popular, and philosophical discussions of privacy in the 1960s and 1970s; they are still common, although less so, today.[61] There has been a more dramatic move away from the metaphor of stripping naked, which was a fixture of privacy discussions in the 1960s and 1970s—the era in which concerns about privacy and the notion of a comprehensive right to privacy rose rapidly to prominence. Vance Packard called his best-selling exposé of threats to privacy *The Naked Society*, and it was common to describe privacy violations as leaving the victim "naked before the world."[62]

The conjunction of these two connotations—*sovereign space* and *enclothement*—suggests that privacy, at least as it was invoked in the late twentieth century, is indeed a distinctive concept. No other concept has quite that set of connotations: not secrecy, not autonomy, not dignity. (Dignity probably comes closest; I will return to the connections between privacy and dignity later in this article.) It is a different question, of course, whether a precise definition can be formulated to capture these connotations. And it is still another question whether a definition of that kind would have any purchase today, when both of the distinctive connotations that privacy had in the 1960s and 1970s seem to have faded.

Those connotations have faded as discussions of privacy have become, for the most part, discussions of informational privacy—a set of concerns not well captured by metaphors of sovereign space or enclothement. This is the second of the three closing points I will make about whether the concept of privacy has any content. Despite the popularity of Solove's suggestion that privacy is a diversity of things without any common essence, most discussions of privacy today—certainly most discussions by people who think of themselves as "privacy scholars"—*do* treat privacy as having a core meaning. The core meaning of "privacy" for these scholars is control over the use and dissemination of personal information. Solove himself purports to reject "control-over-information conceptions" of privacy as in various ways "too vague," "too broad," and "too narrow,"[63] but the taxonomy of privacy that he

60. *See, e.g.*, INNESS, *supra* note 34, at 64, 112 (describing the "realm of privacy" as a "sphere" over which an individual "has evident moral rulership, a rulership that deserves the respect and protection of society").

61. *E.g.*, Jones v. United States, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring) (referring to the "sphere of privacy" protected by the Fourth Amendment).

62. Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 1006 (1964); *cf., e.g.*, BRENTON, *supra* note 25, at 11 (warning that every decrease in privacy "denudes us further still"); WESTIN, *supra* note 27, at 33 (suggesting that penetrating an individual's "inner zone" of privacy "would leave him naked to ridicule and shame and would put him under the control of those who knew his secrets"). So common was this rhetoric that it seemed natural to William Styron in *Sophie's Choice* to describe Sophie as having been metaphorically "stripped bare" by a sexual assault. WILLIAM STYRON, SOPHIE'S CHOICE 100 (First Vintage Int'l ed. 1992) (1979).

63. SOLOVE, *supra* note 39, at 24–29.

proposes is, he says, "arranged . . . around a model that begins with the data subject,"[64] and fourteen of the sixteen topics in his taxonomy pertain, by his own analysis, to "information collection," "information processing," or "information dissemination."[65] For the most part, Solove's account of privacy is an account of informational privacy, and in this respect he is fully in keeping with privacy scholarship more broadly.

At the close of the twentieth century, a conception of privacy centered so strongly around regulating the collection, processing, and dissemination of information could still be described as novel,[66] but today it has taken over. Control over data flows has become "the cornerstone of our modern right to privacy."[67] This conception of privacy is sometimes traced back to Alan Westin's 1967 book, *Privacy and Freedom*. Westin's ideas about privacy were complex. Much of his book treated privacy as a kind of withdrawal or isolation from society.[68] For example, he described privacy as having "four basic states"—"solitude, intimacy, anonymity, and reserve"[69]—and he suggested that "[e]ither too much or too little privacy can create imbalances which seriously jeopardize the individual's well-being."[70] Elsewhere, though, he defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[71] Within a decade, this became perhaps the most widely cited definition of privacy among scholars,[72] on its way toward becoming "a dogma of contemporary jurisprudence."[73] When Westin died in

64. *Id.* at 103.

65. *Id.* at 10–11. Solove calls the two other topics in his taxonomy "intrusion" and "decisional interference," and he groups them together in a category called "invasion." *Id*. at 11. These are plainly catchall topics in a catchall category; they are places to put the odds and ends that do not fit in the main parts of his taxonomy.

66. *See* Pamela Samuelson, *A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy*, 87 CALIF. L. REV. 751 (1999).

67. Margalit Fox, *Alan F. Westin, Who Transformed Privacy Debate Before the Web Era, Dies at 83*, N.Y. TIMES, Feb. 22, 2013, http://www.nytimes.com/2013/02/23/us/alan-f-westin-scholar-who-defined-right-to-privacy-dies-at-83.html (quoting Marc Rotenberg, Executive Director of the Electronic Privacy Information Center); *see also* Schwartz, *supra* note 27, at 1659 (noting that "academics and the law have gravitated towards the idea of privacy as a personal right to control the use of one's data").

68. That, too, is a common way to think about privacy, or at least it was at the time. *See, e.g.*, A. H. MASLOW, MOTIVATION AND PERSONALITY 212 (1954); Sam Keen & John Raser, *An Interview with Herbert Marcuse*, PSYCHOL. TODAY, Feb. 1971, at 35, 37–38.

69. WESTIN, *supra* note 27, at 31.

70. *Id.* at 40.

71. *Id.* at 7. For an earlier version of this idea, see Fried, *supra* note 26, at 486 (defining privacy as "control over information about oneself").

72. *See* Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 262 (1977).

73. W. A. Parent, *Recent Work on the Concept of Privacy*, 20 AM. PHIL. Q. 341, 343 (1983). Parent exaggerated a bit in suggesting that Westin's information-based definition of privacy had already achieved the status of dogma in 1983; outside of academia the idea that privacy was principally a matter of controlling data flows was still a little exotic. Sixteen years later Pamela Samuelson noted that "[t]he idea of legal protection for personal data resonates so little with the

2013, he was chiefly remembered for this definition of privacy. As one scholar explained, Westin "transformed the privacy debate by defining privacy as the ability to control how much about ourselves we reveal to others."[74]

Despite the nods toward anti-essentialism in much modern scholarship about privacy, a unified conception of privacy underlies and shapes that scholarship, as well as more and more discussions outside of academia. It is the conception of privacy as control over personal information.[75] The frequent suggestion that privacy cannot be defined has obscured the fact that a particular definition has become dominant. And whatever else can be said about that definition, it does not make the concept of privacy empty or redundant. Control over the collection, processing, and dissemination of personal information matters, and it matters more and more as the technologies of data collection, data processing, and data sharing gain power exponentially and penetrate ever deeper into daily life. The question is not whether it is helpful to have a way of talking about the individual's interest in his use as a "data subject"; the question is whether the concept of privacy, in particular, has other work to do.

My third and last point about the meaningfulness of privacy is this: it may be helpful and important to try to define privacy even if the definition proves to be compound or elusive. There may be more than one kind of privacy, or privacy may be something like what the philosopher W. B. Gallie called an "essentially contested concept." Gallie had in mind concepts that are both descriptive and evaluative, that are "internally complex" (in the sense that they are multifaceted and cannot be applied without making judgments about the relative importance of their various characteristics), and for which disputes about definition serve as a way of debating normative questions—often framed as the best way of being faithful to or understanding the merit of some generally agreed upon exemplars or paradigmatic cases.[76] Gallie's principal examples were "work of art," "democracy," and "a Christian life." I will suggest later in this article that privacy may in fact be an "essentially contested concept" in Gallie's sense. Even if it is not, though, we should remain open to the possibility that, for reasons related to but not identical to the ones Gallie

---

average American lawyer that it is surely not easy to decide what title to give a U.S.-published book on the subject, let alone how to market the book." Samuelson, *supra* note 66, at 752–53. There would be no such difficulties today.

74. Fox, *supra* note 67 (quoting Professor Jeffrey Rosen).

75. *See, e.g.*, Somini Sengupta, *Web Privacy Becomes a Business Imperative*, N.Y. TIMES, Mar. 4, 2013, at B1 (quoting Facebook privacy officer Erin Egan's definition of privacy as "understanding what happens to your data and having the ability to control it"); Natasha Singer, *An American Quilt of Privacy Laws, Incomplete*, N.Y. TIMES, Mar. 31, 2013, at BU1 (using the term "privacy laws" to refer to laws regarding control over information); *cf.* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 68–71 (2013) (arguing that Fourth Amendment law should take guidance from scholarship on "information privacy law").

76. W.B. Gallie, *Essentially Contested Concepts*, 56 PROC. ARISTOTELIAN SOC'Y 167 (1956), *reprinted in* THE IMPORTANCE OF LANGUAGE 121, 135 (Max Black ed., 1962).

discussed, debates over the definition of privacy may be intractable but nonetheless useful and important.

B. Is Privacy Dead?

For the growing number of scholars seeking to sever the link between privacy and the Fourth Amendment, the problem is not that privacy is meaningless. Most of them take for granted that the concept of privacy has content. Their concerns are different: first, that privacy is dead, or at least breathing its last; and second, that there are other, more important interests threatened by government searches and seizures, even if there is still some privacy worth protecting.

Is there still privacy worth protecting? Many people—not just Fourth Amendment scholars—say there is not, and they point to evidence all around us. First, technologies of surveillance grow cheaper, more various, and more ubiquitous by the day.[77] Cameras mounted in public and semi-public places—what used to be called, quaintly, "closed-circuit television cameras"—are increasingly unremarkable, their presence taken for granted.[78] They are joined by a growing number of audio sensors[79] and, of course, by the explosion of cameras on mobile telephones and now on eyeglass frames.[80] Police departments are making increasing use of cameras mounted on aerial drones; in the near future, that technology will almost certainly be used much more widely, and not just by the police.[81] Meanwhile mobile telephones track their users' locations even when their cameras and microphones are turned off.[82]

Second, more and more of our lives are carried out online: in email and other forms of digital communication; in reading, viewing, requesting, and commenting on material over the Internet; in business and commercial transactions conducted by computer or smart phone; and in the burgeoning world of social media. No sensors are required to spy on this conduct: by its very nature, it leaves a digital record, typically one with multiple copies scattered across a series of computer servers.

Third, technologies for sharing, aggregating, and analyzing digital records—what is sometimes called "Big Data"—are growing exponentially

77. *See, e.g.*, JAMES B. RULE, PRIVACY IN PERIL (2007).

78. *See, e.g.*, SIMON CHESTERMAN, ONE NATION UNDER SURVEILLANCE: A NEW SOCIAL CONTRACT TO DEFEND FREEDOM WITHOUT SACRIFICING LIBERTY 145–54 (2011).

79. *See, e.g.*, Candy Thomson, *MTA Recording Bus Conversations to Eavesdrop on Trouble*, BALTIMORE SUN, Oct. 17, 2012, http://articles.baltimoresun.com/2012-10-17/news/bs-md-mta-bus-safety-20121016_1_mta-bus-audio-recordings-mta-police.

80. *See, e.g.*, Charles Arthur, *Google Glass: Is it a Threat to Our Privacy?*, THE GUARDIAN, Mar. 6, 2013, http://www.theguardian.com/technology/2013/mar/06/google-glass-threat-to-our-privacy.

81. *See, e.g.*, Nick Paumgarten, *Here's Looking at You*, NEW YORKER, May 14, 2012, at 46.

82. *See, e.g.*, Eric Lichtblau, *More Demands on Cell Carriers in Surveillance*, N.Y. TIMES, July 9, 2012, at A1; Eric Lichtblau, *Police Are Using Phone Tracking as a Routine Tool*, N.Y. TIMES, Apr. 1, 2012, at A1.

more powerful.[83] Video images from far-flung camera systems are stitched together;[84] license plates photographed by surveillance cameras are automatically read, identified, and tracked;[85] automated facial recognition is crude but getting steadily more accurate.[86] Store purchases—and, increasingly, other behaviors while shopping—are tracked and cross-referenced.[87] Online clicks are compiled and analyzed. Medical records, school transcripts, and credit reports are increasingly accessible.[88] Merging separate databases makes it difficult if not impossible to maintain the anonymity of any records.[89] The federal government is said to be constructing a vast data facility "to store all of the trillions of words and thoughts and whispers captured in its electronic net."[90]

Fourth, in response to these technological developments and amplifying their effects, social behaviors are changing. People expect less privacy and do less to preserve it. We carry smart phones that track our locations; we let retailers track our purchases; we broadcast our movements and activities on social media; we communicate with technologies that never forget what we have said.[91] Moreover, surveillance practices that once set off alarms about privacy—for example, video cameras mounted in public places—now are either ignored or welcomed. In 1998, when police installed two video cameras in Washington Square Park, the press described this as "a crime-fighting experiment that civil libertarians call Orwellian."[92] Fifteen years later, when the newspaper editorialized in favor of more cameras on city streets—noting that "only 150" of the city's intersections currently had cameras—it did not mention

83. *See, e.g.*, Steve Lohr, *The Age of Big Data*, N.Y. TIMES, Feb. 12, 2012, at SR1.

84. This is why the term "closed-circuit" is "[a]lready … misleading." CHESTERMAN, *supra* note 78, at 147.

85. *See, e.g.*, *id.* at 147; Julia Angwin & Jennifer Valentino-Devries, *New Tracking Frontier: Your License Plates*, WALL ST. J., Sept. 29, 2012, http://online.wsj.com/news/articles/SB10000872396390443995604578004723603576296; Ali Winston, *Police Tracking of Cars on Rise*, S.F. CHRON., June 26, 2013, at A1.

86. *See* Charlie Savage, *Facial Scanning is Making Gains in Surveillance*, N.Y. TIMES, Aug. 21, 2013, at A1.

87. *See* Stephanie Clifford & Quentin Hardy, *Attention Shopper: Stores Are Tracking Your Cell*, N.Y. TIMES, July 15, 2013, at A1; Charles Duhigg, *Psst, You in Aisle 5*, N.Y. TIMES MAG., Feb. 19, 2012, at MM30.

88. CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 10 (2007).

89. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

90. James Bamford, *The NSA is Building the Country's Biggest Spy Center (Watch What You Say)*, WIRED (Mar. 15, 2012, 7:24 PM), http://www.wired.com/2012/03/ff_nsadatacenter/.

91. *See, e.g.*, LORI ANDREWS, I KNOW WHO YOU ARE AND I SAW WHAT YOU DID: SOCIAL NETWORKS AND THE DEATH OF PRIVACY 17–18 (2011); JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 107 (2012).

92. Nick Ravo, *Police Install Cameras in Washington Sq. Park*, N.Y. TIMES, Jan. 2, 1998, at B2; *cf., e.g.*, Andrea Estes, *Smile! You're on "Traffic Camera"*, BOSTON HERALD, Dec. 15, 1994 (reporting that a proposal to install traffic light cameras in Boston was criticized by a member of the city council as "rais[ing] the spectre of *1984*").

privacy concerns.[93] So taken-for-granted are the benefits and acceptability of public video monitoring that the New York City Police Commissioner argued against a measure to deter racial profiling by warning that it might require the removal of surveillance cameras.[94] In October 2001, Jeffrey Rosen thought it an open question whether the United States would "resist the pressure to follow the British example and wire itself up with surveillance cameras"; before the terrorist attacks of September 11, 2001, he noted, "the idea that Americans would voluntarily agree to live their lives under the gaze of a network of biometric surveillance cameras, peering at them in government buildings, shopping malls, subways and stadiums, would have seemed unthinkable."[95] Today public surveillance cameras in the United States are commonplace, just as in Britain.[96] In the wake of the 2013 Boston Marathon bombings, no one thought it remarkable, let alone troubling, that law enforcement officials could quickly find video records of the suspects walking along the sidewalk.[97] Nor are shrinking expectations of privacy limited to conduct carried out in public. In June 2013, when a former government contractor disclosed that the National Security Agency was collecting and storing massive amounts of data about telephone calls between United States citizens and Internet communications by foreign targets, the immediate response in many quarters was "something of a collective national shrug."[98] There is a downward creep in what strikes us as creepy.[99]

Collectively, these four trends—the proliferation of surveillance devices, the growth in online activity, the advent of Big Data, and the related transformations of behavior and expectations—have led some observers, and not just business executives with skin in the game,[100] to write off privacy as a lost cause. Privacy's disappearance is sometimes celebrated and sometimes mourned. Either way, it has in turn led some thoughtful scholars to suggest that protections against search and seizure need a new foundation. "So long as

93. *See* Editorial, *More Cameras for New York City Streets*, N.Y. TIMES, Mar. 2, 2013, at A18.

94. *See* J. David Goodman, *City Council Votes to Increase Oversight of New York Police*, N.Y. TIMES, June 28, 2013, at A1.

95. Jeffrey Rosen, *A Watchful State*, N.Y. TIMES MAG., Oct. 7, 2001, at 38, 40.

96. *See, e.g.*, SLOBOGIN, *supra* note 88, at 88 (noting that the question is no longer "whether such systems will be installed or maintained, but whether and how their use will be regulated").

97. *See* Katharine Q. Seelye, Michael Cooper & Michael S. Schmidt, *F.B.I. Posts Images of Pair Suspected in Boston Attack*, N.Y. TIMES, Apr. 18, 2013, at A1.

98. Adam Nagourney, *In U.S., News of Surveillance Effort is Met With Some Concern but Little Surprise*, N.Y. Times, June 8, 2013, at A12; *see also* James B. Rule, *The Price of the Panopticon*, N.Y. TIMES, June 12, 2013, at A27 (noting with dismay that "[t]he revelation that the federal government has been secretly gathering records on the phone calls and online activities of millions of Americans and foreigners seems not to have alarmed most Americans").

99. For an earlier example, *see* BRENDAN I. KOERNER, THE SKIES BELONG TO US: LOVE AND TERROR IN THE GOLDEN AGE OF HIJACKING 41–42, 46–47 (2013) (describing belief by airlines and regulators in the 1960s that travelers would not tolerate the "invasion of privacy" if x-ray machines and metal detectors were installed in airports).

100. *See supra* notes 12 & 13.

Fourth Amendment privacy is parasitical on private-sphere privacy," Jed Rubenfeld warns, "the former must die as its host dies, and this host is undoubtedly faltering today in the networked, monitored and digitized world we are learning to call our own."[101] Bennett Capers concludes: "Quite simply, we have become a surveillance state."[102] What we need, Paul Ohm explains, is a Fourth Amendment for "a world without privacy."[103]

The most important fact to note about this line of thinking—both the announcements that privacy is sinking and the calls to abandon ship—is that it focuses on a particular conception of privacy: the conception of privacy as control over the dissemination and use of personal information. *That* is what is threatened by our "networked, monitored and digitized world." *That* is the loss we are asked to "get over." Not even David Brin—whose insightful book, *The Transparent Society*,[104] has become something of a touchstone for death-of-privacy enthusiasts[105]—foresees or would welcome a world without *any* kind of privacy. "It is already far too late," Brin argues, "to prevent the invasion of cameras and databases"; the question is how to live in a "transparent society," not whether we want one.[106] Still, he insists that ways can and must be found to protect what he calls "bedroom privacy":[107]

> [T]here is a realm that each of us calls deeply personal, wherein we seek either solitude or intimacy. A place to hold things we want kept private . . . . In the coming era, when camera-bearing robots may swarm the skies, we will all need . . . some zone of sanctuary where we can feel unobserved. Some corner where our hearts can remain forever just our own.[108]

Brin explicitly links this kind of privacy with traditional protections of the home and the venerable legal concept of "curtilage."[109] I will have more to say about that linkage later.[110] What matters for now is that even the most widely cited prophet of the end of privacy makes clear that what is ending is a particular *kind* of privacy—informational privacy. That point tends to get lost because of the assumption, unstated but ever more prevalent, that privacy *is* informational privacy.

---

101. Rubenfeld, *supra* note 8, at 118.

102. I. Bennett Capers, *Crime, Surveillance, and Communities*, 40 FORDHAM URB. L.J. 959, 960 (2013).

103. Ohm, *supra* note 23, at 1310; *cf.* Sundby, *supra* note 23, at 1758 (suggesting the need to adapt the Fourth Amendment to "a [n]on-[p]rivate [w]orld").

104. DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (1998).

105. *See, e.g.*, A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1501, 1538–39 (2000); Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 510 n.33 (1999); Ohm, *supra* note 23, at 1313.

106. BRIN, *supra* note 104, at 8–9.

107. *Id.* at 269.

108. *Id.* at 269–70.

109. *See id.* at 270.

110. *See infra* notes 228–45 and accompanying text.

Actually, the privacy widely thought to be dead or dying is an even more specific variety of informational privacy, what might be called absolute informational privacy: the ability to prevent any unauthorized dissemination or use of personal information. *That* is what now seems impossible. We no longer expect control over information about ourselves "in any *complete* sense."[111] But of course we never did.[112] What has happened is that our degree of control over some kinds of information about ourselves has dramatically diminished, and the uses to which that information is put have dramatically increased. What is now called "privacy law" is precisely a set of rules for the exploding commerce in personal information. Some people, Brin presumably included, think the whole field of privacy law quixotic, but most knowledgeable observers—including many of Brin's admirers—do not. An all-or-nothing approach to privacy—denying that people have any interest in controlling the use or dissemination of information that is less than fully confidential—has long been, with justification, one of the most heavily criticized aspects of the Supreme Court's Fourth Amendment jurisprudence.[113] It is bad enough for the Supreme Court to talk that way; we should avoid making it part of our own thinking about privacy.

C. Is Privacy Irrelevant?

Privacy means something: at least, there are no good reasons to conclude at the outset that the concept is meaningless, and there are strong indications to the contrary. And privacy is not dead: the obituaries are for *informational* privacy, and they are premature. But there is a third argument for severing the Fourth Amendment from privacy. Even if privacy has content, and even if there is still privacy worth worrying about, a growing number of scholars think that concerns about privacy are simply tangential to the concerns raised by government searches and seizures.

That assessment is widely shared both among criminal procedure scholars and among scholars of "privacy law." Privacy law scholars give relatively little attention to government searches and seizures because the privacy they are concerned about is control over personal information, and these days the most dramatic infringements of that control come not from the government but from private entities. Police departments matter less than retailers, credit bureaus, and Internet service providers.[114] Even law enforcement officials increasingly

111. Sundby, *supra* note 23, at 1759 (emphasis added).

112. *See* Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2090–91 (2001).

113. *See, e.g.*, Rubenfeld, *supra* note 8, at 110–15; *cf. supra* note 11 and accompanying text (discussing Justice Sotomayor's suggestion that the third-party doctrine in Fourth Amendment jurisprudence should be reconsidered).

114. *See, e.g.*, COHEN, *supra* note 91, at 107; AMITAI ETZIONI, THE LIMITS OF PRIVACY 10–11 (1999); Daniel Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 MINN. L. REV. 1137, 1139–40 (2002).

rely on information collected and collated by private companies.[115] Criminal procedure scholars recognize all this, and some of them also note that, even if we are especially concerned about the *government's* collection and use of personal information, the kinds of investigation regulated by the Fourth Amendment is still just the tail: the dog is the vast array of mandatory reporting requirements imposed by agencies ranging from the Internal Revenue Service to the Occupational Safety and Health Administration.[116] Given these other, much larger threats to data privacy, constitutional restrictions on the collection of information in the course of criminal investigations seem increasingly odd and increasingly pointless.

They also seem disconnected from the "distinctive threats" posed by law enforcement.[117] For most scholars of criminal procedure, the foremost challenges posed by contemporary policing pertain, first, to the way in which policing feeds and maintains America's swollen and overly harsh system of carceral punishment; and, second, to the violence, racial bias, and alienating incivility of personal encounters between law enforcement agents and suspects. Neither of those sets of concerns relate directly to control over personal information.[118]

Not only that, but the threats that police investigations do pose to informational privacy—say, the compelled disclosures inherent in the search of a home or a computer—are threats that matter most to people with the resources to live in spacious homes and to own and use computers. These may be the people who need the fewest legal protections against the police: they can protect themselves through the normal channels of politics. By protecting "the wrong interest," search-and-seizure law may therefore have wound up protecting "the wrong people."[119] That was a plausible argument even before the digital age, because people with large and comfortable residences lived more of their lives at home and therefore benefited more from Fourth Amendment protections centered around the home.[120] Today, the wealthy not only have bigger homes than the poor; they also tend to be more networked: they have more digital devices, and they are more technologically savvy. That makes them easier to monitor online, and it makes informational privacy even more of a rich person's concern.

For all of these reasons, protecting privacy seems like something of a diversion to many scholars of criminal procedure. The police are an

115. *See, e.g.*, Angwin & Valentino-Devries, *supra* note 85; Galison & Minow, *supra* note 39, at 265; Ohm, *supra* note 23, at 1311, 1321; Winston, *supra* note 85, at A8.

116. *See* William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016 (1995).

117. Rubenfeld, *supra* note 8, at 118.

118. *See* Stuntz, *supra* note 116, at 1021–22.

119. William J. Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 GEO. WASH. L. REV. 1265, 1289 (1999).

120. *See id.*

increasingly marginal part of the overall threat to privacy, and privacy is tangential to the most important threats posed by the police. Again, though, what we are talking about here is "*informational* privacy," what William Stuntz—a particularly insightful critic of the privacy focus of Fourth Amendment law—called "privacy-as-secrecy."[121] Stuntz was careful to point out that criminal procedure law also protects a "second kind" of privacy, focused on "preventing invasions of dignitary interests, as when a police officer publicly accosts someone and treats him as a suspect."[122] He explained that "[a]rrests or street stops infringe privacy in this sense because they stigmatize the individual, single him out, and deprive him of his freedom."[123] But "[t]his second kind of privacy" was "much harder to get one's hands on"; the privacy that was "preeminent" in criminal procedure law was "about protecting secrets and information."[124] And it was that kind of privacy—informational privacy—that seemed tangential to the largest threats raised by police searches and seizures.

Even if those searches are a second-order threat to informational privacy, and even if informational privacy is a second-order concern in regulating police conduct, we still may want informational privacy to matter under the Fourth Amendment. The command of the Fourth Amendment is famously broad: searches and seizures are prohibited if they are "unreasonable," and any number of factors might affect whether a search or seizure is reasonable.[125] At least at first blush, there is a good deal less reason to expect a unitary theory of reasonableness than a unitary theory of privacy. Whether something is "reasonable" seems naturally to call for an open-ended assessment; the same cannot be said for whether something should count as "private." Informational privacy might matter—almost certainly should matter—under the Fourth Amendment even if it is not the only thing that matters, or even the most important thing.

Nevertheless, if privacy means informational privacy there is good reason to believe it should play a much smaller role in Fourth Amendment law than it has long been thought to play. If privacy means informational privacy, then the late twentieth-century consensus about the Fourth Amendment—that privacy was and deserved to be the core concern of search-and-seizure law—is

121. Stuntz, *supra* note 116, at 1021–22.

122. *Id.* at 1021.

123. *Id.*

124. *Id.* at 1021–22.

125. *See, e.g.*, AKHIL REED AMAR, THE CONSTITUTION AND CRIMINAL PROCEDURE: FIRST PRINCIPLES 35–40 (1998). The phrase "unreasonable searches and seizures" in the Fourth Amendment has sometimes been read by the Supreme Court and by scholars as a term of art—code for "searches and seizures barred by eighteenth-century common law" or "searches and seizures and seizures pursuant to general warrants." But there is little reason to read the constitutional language that way, even for an originalist. "Reasonable" meant in the late eighteenth century roughly what it means today. *See* David A. Sklansky, *The Fourth Amendment and Common Law*, 100 COLUM. L. REV. 1739 (2000).

increasingly difficult to defend. All of which raises the question whether privacy *should* mean informational privacy, and if not what it should mean instead.

II.
PRIVACY AND INFORMATION

A. How Privacy Became Informational Privacy

Privacy did not always mean control over information, but that is how the concept is generally understood today, notwithstanding the lip service given to the notion that privacy is no one thing. Reducing privacy to informational privacy makes it difficult to understand certain intuitions that were once widespread: that violating privacy is akin to stripping someone bare, and that it is useful to think in terms of a "realm" of privacy. As we have seen, equating privacy with informational privacy also makes possible the claim that privacy is dead or dying, and it helps to explain the widespread sense, among privacy scholars as well as criminal procedure scholars, that the privacy threats raised by law enforcement activity are matters of only secondary importance. There are other reasons, too, to resist equating privacy with informational privacy, and I will discuss some of them below. At the outset, though, it will help to understand why this particular conception of privacy, "privacy-as-secrecy," has become so dominant. There are at least four reasons.

First, by the 1970s, the concept of privacy began to appear overextended to many judges and scholars, and not just to those who found the entire concept derivative and unhelpful.[126] Much of the unease pertained to the Supreme Court's use of the term "privacy" to describe a constitutionally protected interest in intimate autonomy, an interest the Court invoked when striking down bans on the sales of contraceptives and, later and more controversially, bans on abortion.[127] For critics of these decisions, including some members of the Court, and even for some supporters of the decisions, it made no sense to describe intimate autonomy as "privacy": what was at stake was a certain kind of *liberty*, a right to engage in certain conduct.[128] Many judges and scholars thought it close to self-evident that the usage of "privacy" in cases like *Griswold v. Connecticut*, *Eisenstadt v. Baird*, and *Roe v. Wade* was disconnected from any traditional meaning of the term.[129]

126. *See supra* notes 33–34 and accompanying text.

127. *See* Roe v. Wade, 410 U.S. 113 (1973); Eisenstadt v. Baird, 405 U.S. 438 (1972); Griswold v. Connecticut, 381 U.S. 479 (1965).

128. *See, e.g.*, Louis Henkin, *Privacy and Autonomy*, 74 COLUM. L. REV. 1410 (1974); W. A. Parent, *Recent Work on the Concept of Privacy*, 20 AM. PHIL. Q. 341, 343 (1983).

129. *See, e.g.*, Henkin, *supra* note 128, at 1410–11; William H. Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement? Or: Privacy, You've Come a Long Way, Baby*, 23 U. KAN. L. REV. 1, 5 (1975); Geoffrey R. Stone, *The Scope of the Fourth*

They were wrong about that: there was nothing novel about "characterizing intimate decisions as 'private' or 'personal'—unfit subjects for the state's regulatory power."[130] The "sphere" of privacy described by James Fitzjames Stephen, for example, was the sphere "within which law and public opinion are intruders likely to do more harm than good," a sphere that included "the internal affairs of a family" and "the relations of love or friendship."[131] Nevertheless, there was a sense by the mid-1970s—especially, but not only, among scholars and judges opposed to the rulings in *Griswold*, *Eisenstadt*, and *Roe*—that the concept of privacy had been stretched too far in those cases. There was a corresponding desire for a narrower definition of privacy, one that would exclude interests in intimate autonomy.[132] Alan Westin's suggestion, that privacy had to do with controlling the circulation of personal information, fit the bill.[133] And one measure of the wide acceptance of Westin's definition is the shrinking role that privacy has come to play in efforts to protect intimate autonomy. Same-sex marriage—the defining issue of intimate autonomy of the past decade—is hard to describe as a matter of privacy; the question is which partnerships the state should officially recognize. Debates over same-sex marriage have largely been debates about equality, not privacy.[134]

Second, for many on the left, privacy—particularly the idea of a "sphere" or "realm" or "zone" of privacy—lost much of its appeal in the 1970s and 1980s; this was why even scholars who supported the ruling in *Roe* tended to criticize the role that privacy played in the Court's opinion. At the center of the zone of privacy were the family and the home, and feminists came to see the privacy of the family and the home as a shield for oppression and violence.[135] Then, too, renewed interest in classic ideals of civic virtue left many scholars uncomfortable with the valorization of the private, at least as it had traditionally been understood.[136] And many scholars grew suspicious of the entire distinction between "public" and "private": it seemed part and parcel of the kind of binary formalism, the taming of social experience through false

Amendment: Privacy and the Police Use of Spies, Secret Agents, and Informers, 1976 AM. BAR FOUND. RES. J. 1193, 1206.

130. INNESS, *supra* note 34, at 64.

131. STEPHEN, *supra* note 59, at 107–08.

132. *See, e.g.*, Sundby, *supra* note 23, at 1763–64. Privacy so defined might *foster* autonomy, but the idea was it should not *consist in* or *require* autonomy. On the distinction between the value of privacy and the components of privacy, see, e.g., INNESS, *supra* note 34, at 23, 56–73.

133. *See, e.g.*, Stone, *supra* note 129, at 1207 n.49.

134. *See, e.g.*, United States v. Windsor, No. 12-307 (U.S. June 26, 2013); *but cf.* Melissa Murray, *Marriage as Punishment*, 112 COLUM. L. REV. 1 (2012) (arguing for broadening debates about marriage equality to include reconsideration of the relationship between marriage and intimate privacy).

135. *See*, *e.g.*, DEBORAH COHEN, FAMILY SECRETS: SHAME AND PRIVACY IN MODERN BRITAIN 244–46 (2013); SUK, *supra* note 22, at 4–8, 125–27; Suzanne A. Kim, *Reconstructing Family Privacy*, 57 HASTINGS L.J. 557, 567–77 (2006).

136. *See, e.g.*, Frank Michaelman, *Law's Republic*, 97 YALE L.J. 1493, 1533–36 (1988).

polarizations, that Critical Legal Studies often took as its primary target.[137] Redefining privacy as control over information blunted these attacks by reducing privacy from a fundamental value to something more mundane: an interest that society could choose to recognize and to defend to whatever extent it deemed proper.

Third, an information-centered view of privacy grew more attractive as data flows became increasingly central to our lives, both as a lens through which to understand the world and as a locus of economic activity. Information theory, a branch of applied mathematics focused on the quantification of order, was developed in the mid-twentieth century to address problems in electrical engineering and signal processing, but it proved so productive in those fields that it was soon adopted in a range of other technical and scientific disciplines. Then it became a kind of conceptual touchstone for academics of all stripes, much as Newtonian physics and Darwinian evolution had done earlier.[138] This was not just an intellectual fad: part of the reason it has become so common to see the world in terms of data flows is that data flows are a bigger part of the world.[139] The amount of information collected, processed, and disseminated has grown exponentially—and with it has grown an entire sector of the economy. Increasingly, how data is shared, aggregated, and used determines not just who gets targeted by advertisements but who gets hired and promoted, who can borrow money and on what terms, who is insured and at what cost, and who is detained, arrested, or deported. Rules for the collection and dissemination of information matter more and more, whatever name is given to what those rules protect. Calling it "privacy" connects that concept to a problem of undeniable importance—even if it also divorces the concept from other concerns it has traditionally embraced.

Fourth and finally, defining privacy as control over information was particularly attractive within the context of search-and-seizure law, because it focused attention on a threat widely understood to be particularly pressing. The threat was that the mere collection of information, however that information wound up being used, would chill independent thought, robust debate, personal growth, and intimate friendship. Call this the stultification thesis: the belief that

137. *See, e.g.*, Duncan Kennedy, *The Structure of Blackstone's Commentaries*, 28 BUFF. L. REV. 209 (1979); Joan Williams, *The Development of the Public/Private Distinction in American Law*, 64 TEX. L. REV. 225 (1985); *cf.* Louis Michael Seidman, *The Problems with Privacy's Problem*, 93 MICH. L. REV. 1079, 1101 (1995) (arguing that "privacy's problem is the central problem for modern constitutional law" and "is about nothing less than hanging onto a conception of ourselves as autonomous individuals living private lives in a post-*Lochner* intellectual environment").

138. *See, e.g.*, RAY FISHMAN & TIM SULLIVAN, THE ORG: THE UNDERLYING LOGIC OF THE OFFICE 145 (2013) (explaining that in a large organization, "[t]he fundamental role of managers . . . is in large part the gathering and processing of information"); JAMES GLEICK, THE INFORMATION: A THEORY, A HISTORY, A FLOOD (2011).

139. *See* GLEICK, *supra* note 138.

surveillance deters the kinds of activities and communications necessary for people to lead full lives as individuals and democratic citizens.

It is difficult to overstate the role that the stultification thesis has played in discussions of government searches, in debates about informational privacy, and in the newly established field of "surveillance studies."[140] All these discourses take as axiomatic that people under surveillance become more guarded about what they say and do, less trustful and playful, more fearful and conformist.[141]

Vance Packard warned in 1964 that surveillance "breeds not only sameness but a watchfulness completely untypical of the exuberant, free-wheeling American so commonly accepted as typical of this land in earlier decades."[142] That may not yet have been conventional wisdom: a student editor of the *Harvard Law Review* suggested two years later that although the electronic tracking devices then under development might "upset some wearers" and "restrain free association and movement to some extent," many people might "come to regard wearing a tracking transmitter as no more offensive than wearing a watch."[143] By 1971, though, Justice Harlan thought "[a]uthority [was] hardly required to support the proposition that words would be measured a good deal more carefully and communication inhibited if one suspected his conversations were being transmitted and transcribed."[144] He warned that informants carrying hidden microphones could "smother that spontaneity—reflected in frivolous, impetuous, sacrilegious, and defiant discourse—that liberates daily life."[145] Justice Harlan's opinion was widely quoted, invariably with approval,[146] and his concerns, generalized and amplified, soon became a fixture of academic discussions of surveillance, rarely if ever questioned.

Thus, for example, Spiros Simitis, a leading European scholar of privacy law, warns that "[i]nhibition . . . tends to be the rule once automated processing

---

140. On surveillance studies, see, for example, DAVID LYON, SURVEILLANCE STUDIES: AN OVERVIEW (2007); THE SURVEILLANCE STUDIES READER (Sean P. Hier & Josh Greenberg eds., 2007).

141. *See, e.g.*, ANDREWS, *supra* note 91, at 55–57; Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1102–04 (2002).

142. PACKARD, *supra* note 25, at 9–10.

143. Note, *Anthropotelemetry: Dr. Schwitgebel's Machine*, 80 HARV. L. REV. 403, 408–09 (1966).

144. United States v. White, 401 U.S. 745, 787 (1971) (Harlan, J., dissenting).

145. *Id.*

146. *See, e.g.*, Arthur H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1256 n.125 (1983); Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 243 n.135 (2002); Lloyd L. Weinreb, *Generalities of the Fourth Amendment*, 42 U. CHI. L. REV. 47, 68 (1974); *cf.* Rubenfeld, *supra* note 8, at 134 (agreeing with Justice Harlan that *White* was wrongly decided because "state action that causes personal life to be lived under a cloud of fear—fear that the state is omnipresent, fear of retaliation for saying or doing the wrong things—violates the security the Fourth Amendment centrally protects").

of personal data becomes a normal tool of both government and private enterprises," with the result that "both the chance for personal assessment of the political and societal process and the opportunity to develop and maintain a particular style of life fade."[147] On this side of the Atlantic, Daniel Solove notes that surveillance "can lead to self-censorship"[148] and "can inhibit such lawful activities as free speech, free association, and other First Amendment rights essential for a democracy."[149] Charles Fried worried as early as 1968 that monitoring makes intimacy impossible and "undermines the subject's capacity to enter into relations of trust,"[150] and Peter Galison and Martha Minow explained more recently that "[j]eopardy to privacy is jeopardy to the space for individual self-invention that our society celebrates . . . the space people need to deliberate, to try out new ways of acting or different ways of speaking."[151] Privacy scholar Julie Cohen suggests that "[a] society that wishes to remain democratic, vibrant, and innovative cannot hope to do so based solely on practices and architectures directed toward transparency and exposure,"[152] because without informational privacy "we all may be more cautious"; monitoring pushes people's choices toward "the bland and the mainstream"[153] and "chills experimentation with the unorthodox, the unpopular, and the merely unfinished."[154] Paul Schwartz argues along similar lines that without "strong rules for information privacy," the Internet will not be used in the ways "most likely to promote democratic self-rule" and "each person's capacity for self-governance," because "who will speak or listen when this behavior leaves finely-grained data trails in a fashion that is difficult to understand or anticipate?"[155] Schwartz warns that "as habit becomes instinct and people . . . gain a sense that their every mouse click and key stroke might be observed, the necessary insulation for individual self-determination will vanish."[156] Likewise, the Fourth Amendment scholar Christopher Slobogin takes it as obvious that "[a]nonymity in public promotes freedom of action and an open society," and that "[l]ack of public anonymity promotes conformity and an oppressive society."[157] He explains that "[p]eople who know they are under government

147. Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 734 (1987).

148. SOLOVE, *supra* note 39, at 108; *see also id.* at 112 (describing the "chilling effects" of surveillance).

149. DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 27 (2011); *see also* Solove, *supra* note 141, at 1102 (noting that surveillance can "severely constrain democracy and individual self-determination").

150. Fried, *supra* note 26, at 490.

151. Galison & Minow, *supra* note 39, at 268, 286.

152. COHEN, *supra* note 91, at 140, 143, 149.

153. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000).

154. *Id.*

155. Schwartz, *supra* note 27, at 1651–53.

156. *Id.* at 1656–57.

157. SLOBOGIN, *supra* note 88, at 92.

surveillance will act less spontaneously, more deliberately, less individualistically, and more conventionally."[158] David Gray and Danielle Citron similarly note that monitoring nudges people "toward the benign and mainstream."[159] Neil Richards says that "when we are watched while engaging in intellectual activities, broadly defined—thinking, reading, web-surfing, or private communication—we are deterred from engaging in thoughts or deeds that others might find deviant." For that reason, he argues, "[s]urveillance . . . menaces our society's foundational commitments to intellectual diversity and eccentric individuality."[160]

The widespread acceptance of the stultification thesis owes something, at least among academics, to its resonance with Michel Foucault's hugely influential argument that power is exercised in modern societies through "disciplinary" processes modeled consciously or unconsciously on Jeremy Bentham's Panopticon.[161] Nonetheless, as Neil Richards notes, claims about the chilling effects of surveillance ultimately are "empirical."[162] And it is striking how little empirical support has been marshaled for the stultification thesis. It amounts to an article of faith. Almost always, claims that surveillance stifles nonconformity and personal growth are either taken as self-evident or are supported with citations to other scholars who make the same claims, either without support or with citations to still more scholars saying the same thing. It is turtles all the way down.

Richards, to his credit, tries to catalog the evidence for the stultification thesis, but the support he finds is remarkably thin. He says that the thesis is buttressed by "three different kinds of arguments."[163] Two of these—"cultural and literary works" like *Nineteen Eighty-Four* and assertions made by the Supreme Court in First Amendment decisions—pretty plainly amount to different species of turtle.[164] Richards also claims, though, that the stultification thesis is supported by a third set of arguments, "com[ing] from the empirical work of scholars in the interdisciplinary field of surveillance studies."[165] Alas,

158. *Id.* at 97–98.

159. Gray & Citron, *supra* note 75, at 76.

160. Richards, *supra* note 27, at 1948.

161. *See* MICHEL FOUCAULT, SURVEILLER ET PUNIR: NAISSANCE DE LA PRISON (1975). Foucault's influence is particularly strong in the relatively new field of surveillance studies. *See, e.g.*, COHEN, *supra* note 91, at 136 (noting that "[m]uch work in surveillance studies builds upon Foucault's landmark study of the prison and its role in the emergence of modern techniques of social discipline"); JOHN GILLIOM, OVERSEERS OF THE POOR: SURVEILLANCE, RESISTANCE, AND THE LIMITS OF PRIVACY 130–33 (2001); Maria Los, *The Technologies of Total Domination*, 2 SURVEILLANCE & SOC'Y 15, 15–18 (2004); *but cf.* JOHN GILLIOM & TORIN MONAHAN, SUPERVISION: AN INTRODUCTION TO THE SURVEILLANCE SOCIETY 21–22 (2013) (distinguishing modern surveillance from the Panopticon). For Foucault's influence on legal scholars studying surveillance, see, for example, SOLOVE, *supra* note 39, at 109; Capers, *supra* note 102, at 964.

162. Richards, *supra* note 27, at 1948.

163. *Id.*

164. *Id.*

165. *Id*.

these too turn out to be mostly turtles. Richards suggests, for example, that "studies of modern forms of surveillance in democratic societies" support "cultural intuitions about the self-censoring effects of surveillance," and he cites for this proposition Lilian Mitrou's study of the European regulation of data storage, which warns that "[u]nder pervasive surveillance, individuals are inclined to make choices that conform to mainstream expectations."[166] But Mitrou does not provide evidence for this claim; she simply cites to similar warnings by Spiros Simitis and Daniel Solove.[167]

The only actual empirical evidence Richards identifies for the stultification thesis—and among the only empirical evidence for that thesis identified anywhere[168]—is experience in communist states during the Cold War.[169] We have vivid accounts of the way that fear of the state suffused daily life in the Soviet Bloc, and many of these accounts suggest that the "assumption of being under surveillance . . . kept people on their guard," fostering a kind of "self-policing."[170] It is difficult in retrospect, though, to determine how much of the blame for this should be placed on surveillance practices, because the communist states of Eastern Europe, like their fictional counterparts in *Nineteen Eighty-Four*, did far more to inspire fear than simply watch their subjects. Some dissenters lost their jobs; some were exiled; many were given sham trials and then imprisoned, tortured, or executed. All of this,

166. *Id.* at 1949 (quoting Lilian Mitrou, *The Impact of Communications Data Retention on Fundamental Rights and Democracy—The Case of the EU Data Retention Directive*, *in* SURVEILLANCE AND DEMOCRACY 127, 138 (Kevin D. Haggerty & Minas Simatas eds., 2010)).

167. *See* Lilian Mitrou, *The Impact of Communications Data Retention on Fundamental Rights and Democracy—The Case of the EU Data Retention Directive*, *in* SURVEILLANCE AND DEMOCRACY 127, 138 (Kevin D. Haggerty & Minas Simatas eds., 2010).

168. Some additional support for the thesis is provided by a recent survey the PEN American Center conducted of its members. Sixteen of the 528 writers who responded to the online survey indicated they had avoided writing or speaking about a particular topic because of fear of government monitoring. PEN AMERICAN CENTER, CHILLING EFFECTS: NSA SURVEILLANCE DRIVES U.S. WRITERS TO SELF-CENSOR 6 (2013). It is a little hard to know what to make of the PEN survey, in part because it was conducted in the wake of disclosures of widespread NSA surveillance, and the questions about chilling effect came after a series of questions about the respondents' views on government monitoring. The writers who responded—less than 10 percent of the PEN members to whom the survey had been sent—expressed strong concerns about surveillance. *Id.* at 13. Those concerns may have been triggered in part by the writers' own experiences of self-censorship, but it is also possible—given the "widely shared assumption that the explosive growth and proliferating uses of surveillance technology must be harmful . . . to intellectual freedom, to creativity, and to social discourse," *id.* at 3—that concerns about surveillance primed the respondents to believe they had censored themselves.

169. Sometimes the reference is broadened to include Nazi Germany. *See, e.g.*, DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 306, 373–74 (1989); Stone, *supra* note 129, at 1195 n.3, 133 n.142.

170. Maria Los, *Post-Communist Fear of Crime and the Commercialization of Security*, 6 THEORETICAL CRIMINOLOGY 165, 169 (2002); *see also, e.g.*, PAUL KECSKEMETI, THE UNEXPECTED REVOLUTION: SOCIAL FORCES IN THE HUNGARIAN UPRISING 95 (1961); STELIAN TĂNASE, AT HOME THERE'S ONLY SPEAKING IN A WHISPER: FILE AND DIARY RECORDING THE LATE YEARS OF THE ROMANIAN DICTATORSHIP (2007).

of course, was *made possible* by surveillance, and so it offers reasons to worry about surveillance, but it provides only ambiguous evidence that surveillance by itself enforces conformity and stunts personal growth.

It is worth noting, too, that the most extensive and disruptive mechanisms of surveillance in the Eastern Bloc involved secret agents and informants, not electronic eavesdropping, mail monitoring, or other passive forms of data collection.[171] Secret agents and informants do not just collect information; they do so in a way that dramatically breaches trust and intrudes into intimate confidences.[172] So whatever part of the deadening fear of the state in the Soviet Bloc can be blamed on surveillance must be blamed on a particular kind of surveillance, one that threatens more than informational privacy.

Not only is empirical support for the stultification thesis limited, there is some suggestive evidence against it. That evidence begins with a phenomenon that is all around us: the sharing of personal information on the Internet, especially through social media, and especially by the young.[173] "Our growing collective compulsion to document our lives and share them online"[174] strikes many people (particularly if they grew up without the Internet) as both reckless and solipsistic.[175] Moreover, there are frequent suggestions that young people do not understand and appreciate the risks they run by posting material about themselves online.[176] That is doubtless true: they are young. Nevertheless, the porous nature of social media and the susceptibility of Internet communications to uninvited monitoring are not exactly secrets, even among adolescents: they "aren't oblivious to the fact that their digital dossiers are growing as they lead their lives mediated by digital technologies."[177] That is part of why the revelations in 2013 of extensive NSA snooping generated a "collective national shrug."[178] And there are precious few signs that lack of confidentiality has

171. *See, e.g.*, PAUL BETTS, WITHIN WALLS: PRIVATE LIFE IN THE GERMAN DEMOCRATIC REPUBLIC 24–35, 42–50 (2012); TĂNASE, *supra* note 170; Amir Weiner & Aigi Rahi-Tamm, *Getting to Know You: The Soviet Surveillance System, 1939–57*, 13 KRITIKA 5, 15, 26–28 (2012). Similarly, the few anecdotes one can find of surveillance discouraging open discussion in the United States involve secret agents and informants, not passive monitoring. Debates among student protest leaders in the 1960s, for example, were at times impaired by the distrust sowed by undercover officers and police provocateurs. *See, e.g.*, JAMES MILLER, DEMOCRACY IS IN THE STREETS: FROM PORT HURON TO THE SIEGE OF CHICAGO 297 (1987). More recently police informants may have inhibited open discussion among some participants in the anti-globalization movement. *See* LUIS A. FERNANDEZ, POLICING DISSENT: SOCIAL CONTROL AND THE ANTI-GLOBALIZATION MOVEMENT 112–16 (2009).

172. *See, e.g.*, ALEXANDRA NATAPOFF, SNITCHING: CRIMINAL INFORMANTS AND THE EROSION OF AMERICAN JUSTICE 116–18 (2009); Weiner & Rahi-Tamm, *supra* note 171, at 28.

173. *See, e.g.*, CHESTERMAN, *supra* note 78, at 9, 246; JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES (2008).

174. Jenna Wortham, Editorial, *Facebook Made Me Do It*, N.Y. TIMES, June 15, 2013, at SR5.

175. *See, e.g.*, Stephen March, *Is Facebook Making Us Lonely?*, THE ATLANTIC, May 2012, at 60, 69 (lamenting that "[c]urating the exhibition of the self has become a 24/7 obsession").

176. *See, e.g.*, ANDREWS, *supra* note 91, at 21; PALFREY & GASSER, *supra* note 173, at 24, 54, 75.

177. PALFREY & GASSER, *supra* note 173, at 51.

178. Nagourney, *supra* note 98, at A12.

made online communications more guarded or the lives of "digital natives"[179] less adventurous or experimental; the indications are rather strongly to the contrary.[180]

Digital natives may think differently about privacy than their elders.[181] (For one thing, they are likely to worry more about monitoring by their parents than by the government or by corporations.)[182] Reasons to doubt the stultification thesis are not limited to the young, though. For example, a study of government employees in Canada suggested that freedom of information laws—contrary to fears—do not affect the quantity or the quality of record-keeping or intra-governmental communication.[183] That will come as little surprise to anyone who uses email on a workplace network subject to employer monitoring: evidence of self-censorship on such networks is difficult to find.[184] People quickly become accustomed to monitoring and then ignore it. Something similar happens when criminal suspects are recorded when talking to the police. Law enforcement officials often oppose the recording of interrogations, because they fear that it will deter candor. In practice, though, it has virtually no effect: minutes after the recording device is turned on, the suspect forgets about it.[185] And despite Justice Harlan's warning that warrantless, surreptitious recording of conversations by confidential informants "might well smother [the] spontaneity . . . that liberates daily life,"[186] we have now lived with that practice for four decades, and it has had no observable impact on the vigor of national discourse.

None of this is to say that surveillance is harmless. Information is power: the more the government knows about people, the more it can do to them. Any society that hopes to remain democratic should worry about the government accumulating too much power and scrutinize how the government uses the powers it is allowed to amass.[187] Furthermore some techniques of surveillance—in particular, the widespread use of secret agents and undercover

179. PALFREY & GASSER, *supra* note 173; *but cf.* DANAH BOYD, IT'S COMPLICATED: THE SOCIAL LIVES OF NETWORKED TEENS 176–98 (2014) (warning against the assumption that young people, simply by virtue of their youth, are more sophisticated about digital technology).

180. *See, e.g.*, PALFREY & GASSER, *supra* note 173, at 21 (noting that "identity formation among Digital Natives is different from identity formation among predigital generations in the sense that there is more experimentation and reinvention of identities").

181. *See, e.g.*, *id.* at 51.

182. *See* BOYD, *supra* note 179, at 56.

183. *See* NATIONAL ARCHIVES OF CANADA, THE *ACCESS TO INFORMATION ACT* AND RECORD-KEEPING IN THE FEDERAL GOVERNMENT (2001).

184. *See* ALASDAIR ROBERTS, BLACKED OUT: GOVERNMENT SECRECY IN THE INFORMATION AGE 215–16 (2006).

185. *See, e.g.*, David A. Sklansky, *Quasi-Affirmative Rights in Constitutional Criminal Procedure*, 88 VA. L. REV. 1229, 1263–64 & nn.110–11 (2002).

186. United States v. White, 401 U.S. 745, 787 (1971) (Harlan, J., dissenting).

187. Points that Neil Richards, among others, has usefully elaborated. Richards, *supra* note 27, at 1952–58; *see also, e.g.*, GILLIOM, *supra* note 161, at 8, 119–28; James B. Rule, *The Whole World Is Watching*, DEMOCRACY, no. 22, Fall 2011, at 58.

informants—can generate paralyzing fear and distrust, if not in isolation then at least when combined with the kinds of authoritarian practices that surveillance makes possible. What deserves questioning, though, is the common suggestion that surveillance alone, simply collecting or threatening to collect information about people, is likely to stunt personal growth and the kind of full, vibrant discussions on which a healthy democracy depends. This suggestion—what I have been calling the stultification thesis—deserves questioning not, chiefly, because it is likely to have led us to be overly worried about surveillance, but rather because it has helped to reinforce the idea that the only privacy worth protecting is all about the control of information. It may have led us, as well, to worry about surveillance in the wrong ways: to focus too narrowly on the risk that being monitored will make people less candid and adventurous, and to pay too little attention to the harms that arise from failing to respect an individual's zone of personal refuge, whatever the effects on the subject's behavior.

A final caveat: it would be a mistake to reject the stultification thesis outright simply because there is so little evidence for it and some suggestive evidence to rebut it. First, there is *some* evidence supporting the thesis.[188] Second, the future may be different than the past. People may have learned to ignore the possibility that they are being monitored because, as a practical matter, the government cannot scrutinize all the information it collects. Even if cameras capture my every movement on public streets and sidewalks, and even if every message and search request I send over the Internet is recorded and archived, the enormous amount of similar data accumulated on everyone else has provided me with a degree of obscurity. I can hide in plain sight. That may change, though, as computers get better at searching images and text, drawing connections, and identifying interesting or suspicious occurrences.[189] When watching and not just recording and archiving can be automated, the chilling effects of surveillance may become more salient, and the stultification thesis may turn out to be true. That is speculation, though. Currently, the evidence for the stultification thesis is weak, and certainly insufficient to justify the assumption that the chilling effects of surveillance are what mainly makes it worth worrying about. Surveillance is troubling in part because of the power relationships it creates, and in part perhaps because of the ways in which certain forms of surveillance can threaten dimensions of privacy that have to do with things other than data.

188. *See supra* note 167.

189. *See, e.g.*, Tal Zarsky, *Mine Your Own Business!: Making the Case for the Implications of Data Mining of Personal Information in the Forum of Public* Opinion, 5 YALE J.L. & TECH. 4 (2006); Deven R. Desai, Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding (Feb. 27, 2014) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2404782.

B. What Informational Privacy Misses

An information-based conception of privacy has genuine attractions. It connects the concept of privacy to the dramatic and far-reaching changes that have occurred in daily life over the past several decades, and it gets privacy out of a line of work that was always controversial: constructing constitutional protections for bodily autonomy and freedoms of intimate association. Nevertheless there are strong reasons to think that privacy is about more than information. As we have seen, those reasons include the intuitions, at one point widespread, linking privacy to enclothement and to a zone of personal sovereignty; the extraordinarily thin support for the stultification thesis; and—not least—the ways in which a focus on information makes it increasingly difficult to understand the relationship between privacy and the reasonableness of government searches and seizures.

There also are more basic problems with defining privacy as control over information, problems so obvious they help to explain why even scholars like Solove, who think about privacy largely in terms of data flows, are careful to avoid claiming that that privacy can be reduced to informational privacy.[190] There is no way we could ever exercise anything close to complete control over the dissemination and use of information about ourselves, and neither would anyone want to live in a society where that was possible.[191] So any information-based theory of privacy has to focus on "private" or "personal" information, which means it must rely on some independent notion of what is "private" or "personal." Even then, it is hard to defend the idea that we could or would want to give people anything close to an absolute right to control this special subset of information about themselves.[192] Moreover, if certain information is private or personal, it is presumably because it relates to certain actions, places, or relationships that are themselves private or personal, and it is hard to see why, if those things deserve protection, they deserve protection only against the unwanted spread or use of information about them.[193] All of which is to say that even if privacy can be violated by using or disseminating certain kinds of information about people against their wishes—which it plainly can be—privacy itself consists in something other than control over information, something at once more basic and potentially more expansive.

---

190. *See, e.g.*, SOLOVE, *supra* note 39, at 21–29.

191. *See* Robert C. Post, *Three Conceptions of Privacy*, 89 GEO. L.J. 2087, 2088–90 (2001). "To interrupt the flow of information," Post points out, "is to short-circuit the formation of knowledge. . . . Most persons desire to define themselves and to have others accept their self-definition. But this desire is incompatible with the ways in which public discussion necessarily appropriates the authority and the power to define persons that are the subject of public consideration." *Id.*

192. *See id.* at 2090–91; *cf., e.g.*, SOLOVE, *supra* note 39, at 28 (arguing that "[e]ven if the conception [of privacy] is narrowed to include only intimate information, it is still too broad").

193. *See* INNESS, *supra* note 34, at 56–69; *cf., e.g.*, SOLOVE, *supra* note 39, at 29 (concluding that "conceptions of [privacy as information control] are too narrow," in part "because they reduce privacy to informational concerns").

The limitations inherent in an information-based approach to privacy—the approach that now dominates the way most judges and scholars think about the Fourth Amendment—can be seen most vividly, perhaps, in cases involving strip searches. Strip searches are paradigmatic violations of privacy, or at least they were, when intrusions into privacy were regularly analogized to forced disrobements.[194] Not surprisingly then, there has long been a sense that strip searches are particularly invasive and require particularly strong justification.[195] That sense lingers today, but the focus on informational privacy has made it increasingly difficult to discern what is exceptional or extreme about strip searches—aside, perhaps, from the amount of distress they cause.

Two recent cases illustrate the problem. In 2009 the Supreme Court ruled that middle-school officials violated the Fourth Amendment when they strip-searched a thirteen-year-old girl named Savana Redding to see if she was hiding prescription-strength ibuprofen.[196] Six federal judges concluded otherwise,[197] however, and the Court itself thought that the ultimate result was sufficiently unpredictable that school officials should be immune from liability.[198] Justice Thomas, along with three judges of the Ninth Circuit, did not believe that the search—which involved having Redding undress down to her bra and underpants, pull her bra away from her body to expose her breasts, and then pull her underpants away from her crotch[199]—should even be described as a "strip search"; they would have reserved that term for a search involving "full" disrobing.[200]

Three years after deciding *Redding*, the Court took up the case of an African-American man named Albert Florence, who had been strip-searched, twice, when he was jailed following his arrest on an obsolete bench warrant; he alleged that on both occasions he was forced to lift his genitals for visual inspection, and then made to "turn around, and cough in a squatting position."[201] Florence argued the searches were unconstitutional because he had been arrested for a minor offense and there were no grounds to suspect that he was concealing contraband.[202] Florence lost: the Supreme Court ruled that the

194. *See supra* notes 59–62 and accompanying text.

195. *See, e.g.*, New Jersey v. T.L.O., 469 U.S. 325, 382 (1985) (Stevens, J., concurring in part and dissenting in part) (suggesting that it was "clear under any standard" that "the shocking strip searches that are described in some cases have no place in the schoolhouse," and that outside prisons and jails, such "deeply intrusive searches" could be justified, if at all, "only to prevent imminent, and serious harm").

196. Safford Unified School Dist. No. 1 v. Redding, 557 U.S. 364 (2009) [*Redding III*].

197. *See* Redding v. Safford Unified Sch. Distr. No. 1, 504 F.3d 828 (9th Cir. 2007) [*Redding I*], *rev'd*, 531 F.3d 1071 (9th Cir. 2008) (en banc) [*Redding II*], *aff'd in part and rev'd in part*, 557 U.S. 364 (2009) [*Redding III*]; *Redding II*, 531 F.3d at 1091 (Hawkins, J., dissenting); *Redding III*, 557 U.S. at 382 (Thomas, J., dissenting).

198. *See Redding III*, 557 U.S. at 377–79.

199. *See id.* at 369, 374.

200. *Id.* at 388 n.2 (Thomas, J., dissenting).

201. Florence v. Bd. of Chosen Freeholders, 132 S. Ct. 1510, 1514 (2012).

202. *Id.* at 1514–15.

jail could strip-search all new prisoners because that policy "struck a reasonable balance between inmate privacy and the needs of the institution,"[203] at least with respect to prisoners admitted to the general jail population.[204] Again, there was uncertainty even about whether to call what had happened a "strip search." Justice Kennedy's majority opinion said that term was "imprecise" and noted that searches in this case were not alleged to have involved "any touching of unclothed areas by the inspecting officer."[205] The Court split 5–4, and there was a sharp dissent,[206] but the most instructive aspect of the decision is how little attention it received. *Jones v. United States*—the satellite tracking case decided the same term—drew an avalanche of commentary,[207] but Florence's case was largely ignored, both by scholars and by the press.[208]

Some of that neglect may be explained by the fact that Florence was searched when he was jailed. There are special rules for jails and prisons,[209] and judges, scholars, and members of the public generally do not think those rules might wind up applied to *them*. But there are special rules for criminal suspects, too, and in truth most scholars, like most judges and most members of the general public, are at least as likely to be arrested and jailed for a minor offense (like Florence) as they are to be targeted in a narcotics investigation (like Jones). *Jones* received vastly more attention than *Florence* in part because the intrusion in *Jones*—tracking with a GPS device by law enforcement—lies close to the heart of the practices that are understood as the main threat to privacy today, the aggregation and analysis of data about people's lives. *Jones* is a paradigmatic case of an intrusion into informational privacy. *Florence* involved a paradigmatic violation of a different kind of privacy, one that has come to be seen as increasingly peripheral. The strip search in *Florence*, like the one in *Redding*, was seen as raising concerns largely having to do with the

203. *Id.* at 1523.

204. Four members of the majority suggested the result might be different for detainees "held without assignment to the general jail population and without substantial contact with other detainees." *Id.* at 1522–23 (Kennedy, J.); *see also id.* at 1523 (Roberts, C.J., concurring); *id.* at 1524 (Alito, J., concurring).

205. *Id.* at 1515 (Kennedy, J.).

206. *See id.* at 1525 (Breyer, J., dissenting).

207. *See, e.g.*, Fabio Arcilla, Jr., *GPS Tracking Out of Fourth Amendment Dead Ends:* United States v. Jones *and the* Katz *Conundrum*, 19 N.C. L. Rev. 1 (2012); Jim Harper, *Escaping Fourth Amendment Doctrine After* Jones*: Physics, Law, and Privacy Protection*, 2012 CATO SUP. CT. REV. 219; Kerr, *supra* note 9; Arnold H. Loewy, United States v. Jones: *Return to Trespass—Good News or Bad*, 82 MISS. L.J. 879 (2013); Erin Murphy, *Back to the Future: The Curious Case of* United States v. Jones, 10 OHIO ST. J. CRIM. L. 325 (2012); *Caren Myers Morrison, The Drug Dealer, The Narc, and the Very Tiny Constable: Reflections on United States v. Jones*, 3 CALIF. L. REV. CIRCUIT 113 (2012), *available at* http://www.californialawreview.org/assets/circuit/Morrison_3-113.pdf.

208. *See, e.g.*, Julian Simcock, Note, Florence, Atwater, *and the Erosion of Fourth Amendment Protections for Arrestees*, 65 STAN. L. REV. 599, 602 (2013) (noting that *Florence* "has been the subject of little attention by scholars").

209. *See, e.g.*, Sharon Dolovich, *Teaching Prison Law*, 62 J. LEGAL EDUC. 218, 221–22 (2012).

sensitivities of the person being searched,[210] whereas the surveillance in *Jones* implicated the very "relationship between citizen and government" in a "democratic society."[211]

The relationship between citizen and government in a democratic society might also be thought implicated by the exercise of power inherent in the act of forcing a prisoner (or a student at a public school) to strip naked and submit to official inspection. All the more so given the racially skewed nature of incarceration[212] (and, for that matter, school discipline[213]) in the United States. If the ultimate fear is O'Brien's vision of "a boot stepping on a human face . . . forever,"[214] it is not clear that widespread GPS monitoring moves us farther along that path than routine strip searches. Seeing strip searches as more than just traumatic, though, requires a way to conceptualize their less immediate harms: their "symbolic function of reaffirming . . . shame, and lack of status";[215] the way they can cultivate a politically enervating sense of "humiliation and helplessness";[216] and, perhaps most importantly, the way they can build habits of dehumanization and brutality in the institutions and officials carrying out the searches. One way to conceptualize these dangers is through a theory of privacy, but not a theory of privacy that focuses first and foremost on control over information. An information-based theory of privacy will similarly be of little use in understanding the hazards, beyond injured sensibilities, of aggressive stop-and-frisk police tactics, or of traffic stops and vehicle searches that uncover nothing of interest.[217]

---

210. *See, e.g.*, *Florence*, 132 S. Ct. at 1524 (Alito, J., concurring); *id*. at 1526 (Breyer, J., dissenting).

211. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

212. *See, e.g.*, WILLIAM J. STUNTZ, THE COLLAPSE OF AMERICAN CRIMINAL JUSTICE 41–59 (2011).

213. *See, e.g.*, Michael Pinard, *From the Classroom to the Courtroom: Reassessing Fourth Amendment Standards in Public School Searches Involving Law Enforcement Authorities*, 45 ARIZ. L. REV. 1067, 1117–18 (2003).

214. GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949).

215. Daphne Ha, Note, *Blanket Policies for Strip Searching Pretrial Detainees: An Interdisciplinary Argument for Reasonableness*, 79 FORDHAM L. REV. 2721, 2740 (2011) (quoting RUSSELL P. DOBASH, R. EMERSON DOBASH & SUE GUTTERIDGE, THE IMPRISONMENT OF WOMEN 204–05 (1986)); *cf.* ERVING GOFFMAN, ASYLUMS 32, 130, 137 (1961) (discussing strip searches and the lack of physical privacy in mental hospitals and by extension in other "total institutions").

216. Ha, *supra* note 215, at 2740.

217. *See* CHARLES R. EPP, STEVEN MAYNARD-MOODY & DONALD HAIDER-MARKEL, PULLED OVER: HOW POLICE STOPS DEFINE RACE AND CITIZENSHIP (2014); Janice Nadler, *Consent, Dignity, and the Failure of Scattershot Policing*, *in* THE CONSTITUTION AND THE FUTURE OF CRIMINAL JUSTICE IN AMERICA 93, 102–03 (John T. Parry & L. Song Richardson eds., 2013); Tom R. Tyler, Jeffrey Fagan & Amanda Geller, Street Stops and Police Legitimacy: Teachable Moments in Young Urban Men's Legal Socialization (Jan. 2014) (unpublished manuscript), *available at* http://web.law.columbia.edu/sites/default/files/microsites/tax-policy/files/LTW/police_stops_and_legitimacy_january_22_2014.pdf.

A non-informational theory of privacy is not the only way to get purchase on these kinds of harms. They can be described, for example, simply as assaults on dignity. In fact, dignity is precisely the language most often used by judges and scholars trying to capture what makes strip searches so extraordinarily violative.[218] It is commonly employed, as well, to describe the non-informational infringements associated with investigatory stops.[219] But dignity is an even vaguer term than privacy, and it lacks the connotations of enclothement, sanctuary, and sovereignty that I have been suggesting we may wish to recover. There is a long tradition of suggesting that privacy is a form of dignity, or that privacy is important in part because it protects dignity;[220] I will argue below that this tradition has a good deal to teach us. But dignity can be undermined in ways that have little to do with privacy, however broadly conceived: name-calling, mockery, or open expressions of contempt, for example. The language of privacy seems useful in identifying a particular kind of threat to dignity.

For similar reasons, it does not seem sufficient to describe the distinctive injury in a strip search or in a particularly aggressive investigatory stop as an attack on "trust"[221] or "security."[222] Violations of privacy can plainly undermine trust, and certain forms of privacy may even be a "necessary context" for trust.[223] But trust can be damaged without infringing privacy: by breaking a promise, say. And asserting, as some scholars have, that the Fourth Amendment protects "security" raises the obvious question, security of *what*? Jed Rubenfeld answers, plausibly, that the Fourth Amendment should be read to promise the security of "personal life"—i.e., of "all those domains of interaction in which people are outside the public sphere."[224] But that sounds like a kind of privacy: it sounds like a reference to what has more often been described as the "private sphere." Just as the language of privacy seems useful in describing a specific way in which dignity can be assaulted, it can be helpful in identifying distinctive threats that, say, a strip search or an aggressive pat down poses to trust and security. To do so convincingly, though, it cannot focus first and foremost on data flows.

---

218. *See, e.g.*, Florence v. Bd. of Chosen Freeholders, 132 S. Ct. 1510, 1527 (2012) (Breyer, J., dissenting); Josh Bowers, *Probable Cause, Constitutional Reasonableness, and the Unrecognized Point of a "Pointless Indignity"*, 66 STAN. L. REV. 987, 1018 (2014); Ha, *supra* note 215, at 2740.

219. *See, e.g.*, Nadler, *supra* note 217; Stuntz, *supra* note 119, at 1273.

220. *See, e.g.*, Bloustein, *supra* note 62; Gavison, *supra* note 34, at 455; Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 1008 (1989); Post, *supra* note 112, at 2092–94; *cf.* Whitman, *supra* note 36, at 1161 (arguing that "[c]ontinental privacy protections are, at their core, a form of protection of a right to *respect* and *personal dignity*").

221. Sundby, *supra* note 23.

222. Clancy, *supra* note 24; Rubenfeld, *supra* note 8, at 104.

223. Fried, *supra* note 26, at 478.

224. Rubenfeld, *supra* note 8, at 128, 133.

III.
REIMAGINING PRIVACY

If defining privacy as control over data flows seems too reductive (as well as too broad[225]), how *should* we think about privacy? One way to begin answering that question is to identify elements that a helpful conception of privacy should include, elements that are missing from an account of privacy that focuses only on control over data flows. I have gestured at some of these elements already: the connection between privacy and a sense of enclothement, the familiar (if now less ubiquitous) intuition that privacy resides in a "zone" or "sphere" of personal sovereignty, and the notion of privacy as a refuge or sanctuary. These three elements are linked: the zone of privacy has often been defended as a place of retreat, and there is a long tradition of thinking that the body itself is at the core of the zone of privacy. I want to say a bit more regarding these linked intuitions about privacy, and I also want to suggest other elements worth incorporating into a reconstructed conception of privacy, elements having to do with the nature and purpose of privacy rather than the content of privacy.[226] In the latter regard, I will draw on Robert Post's idea that privacy is not, strictly speaking, something that people *have* but rather a way that people treat each other, a form of respect, a set of "civility rules"[227]; and I will suggest that privacy violations are harmful not solely because of their effects on the victims, but also, and maybe mostly, because of the habits and ways of thinking they engrain in the violators. Finally, after discussing the elements to be brought back into privacy, I will try to formulate a conception of privacy that incorporates those elements, and discuss how it might inform and improve discussions about government searches and seizures.

A. Privacy and Refuge

The notion that each of us needs "a private enclave"[228]—locations and aspects of our lives that are shielded from public scrutiny—may be a product of modernity, but it is so deeply entrenched that it has become part of what it means for a life to be well led and for a society to be well constituted.[229] That is why even David Brin, the influential enthusiast for a "transparent society," warns that we will always need "some zone of sanctuary where we can feel unobserved . . . [s]ome corner where our hearts can remain forever just our own."[230] He is echoing the thoughts and cadences of Judge Jerome Frank, who

225. *See supra* text accompanying notes 191–92.

226. Regarding these distinctions, see INNESS, *supra* note 34.

227. Post, *supra* note 220, at 1008–09; *see also id.* at 959; Post, *supra* note 112, at 2096–97.

228. *E.g.*, Murphy v. Waterfront Comm'n, 378 U.S. 52, 55 (1964) (quoting United States v. Grunewald, 233 F.2d 556, 581 (2d Cir. 1956) (Frank, J., dissenting in part), *rev'g* 353 U.S. 391 (1957)).

229. *See, e.g.*, Galison & Minow, *supra* note 39, at 258.

230. BRIN, *supra* note 104, at 269–70; *see supra* text accompanying notes 104–09.

wrote, in language that the Supreme Court later adopted in a precursor to *Katz v. United States*, that a "sane, decent, civilized society must provide some . . . oasis, some shelter from public scrutiny, some insulated enclosure, some enclave, some inviolate place . . . ."[231] The private sphere is valued for reasons both psychological and political.[232] The psychological reasons have to do with an individual's need for solitude—"a room, just for ourselves, at the back of the shop" where "[the] soul . . . [can] turn in on herself"[233]—and with the necessary conditions for intimacy. The political significance of the private sphere is connected to the idea of limited government; it became especially salient in the middle decades of the twentieth century, when the cardinal political imperative became the avoidance of totalitarianism, a "contrast-model"[234] often defined in large part precisely by the elimination of the private sphere.[235]

To say that there should be a private sphere is not to say where it should be located, but there is a long tradition of centering that sphere around the home and the body.[236] The home is what Judge Frank had in mind when he wrote about an "oasis" and "shelter from public scrutiny"[237] (although not when he wrote later about the need for a "private enclave" where an individual "may lead a private life"[238]), and it is what Brin has in mind when he speaks of a "zone of sanctuary" or "bedroom privacy."[239] The home and the body are not arbitrary choices as the foci of privacy. The home is a natural site of seclusion and intimacy; some people go to the woods to be alone, but most of us, most of

231. Silverman v. United States, 365 U.S. 505, 511 n.4 (1961) (quoting United States v. On Lee, 193 F.2d 306, 315–16 (2d Cir. 1951) (Frank, J., dissenting), *aff'd*, 343 U.S. 747 (1952)).

232. *Cf.* OBIKA GRAY, DEMEANED BUT EMPOWERED: THE SOCIAL POWER OF THE URBAN POOR IN JAMAICA 95–96 (noting the use of the "refuge" of "exilic space" by Jamaican urban poor both to build "repertoires of survival" and to "exert a social power").

233. MICHEL DE MONTAIGNE, *On Solitude*, *in* ON SOLITUDE 1, 7 (M. A. Screech trans., 1991).

234. William E. Connolly, *The Challenge to Pluralist Theory*, *in* THE BIAS OF PLURALISM 3, 22–24 (William E. Connolly ed., 1969).

235. *See, e.g.*, United States v. Grunewald, 233 F.2d 556, 581–82 (2d Cir. 1956) (Frank, J., dissenting in part) (calling the "right to a private enclave" the "hallmark of our democracy" and noting that "[t]he totalitarian regimes scornfully reject that right" and "seek to convert all that is private into the totally public . . . a la Orwell's terrifying book, '1984'"); *but cf.* BETTS, *supra* note 171, at 3 (suggesting that what atrophied in East Germany was not the private sphere but the "public sphere of open debate and genuine civil society").

236. *See, e.g.*, SUK, *supra* note 22, at 1–8, 109–11; Linda J. McClain, *Inviolability and Privacy: The Castle, the Sanctuary, and the Body*, 7 YALE J.L. & HUMAN. 195 (1995).

237. United States v. On Lee, 193 F.2d 306, 315 (2d Cir. 1951) (Frank, J., dissenting), *aff'd*, 343 U.S. 747 (1952)). When the Supreme Court quoted and adopted Judge Frank's language in *On Lee*, it did so in support of the proposition that "[a]t the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from governmental intrusion," *Silverman*, 365 U.S. at 511 & n.4—a proposition it has since repeatedly reaffirmed, most recently in Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013).

238. *Grunewald*, 233 F.2d at 581–82 (Frank, J., dissenting in part) (discussing the Fifth Amendment privilege against compelled self-incrimination).

239. *See* BRIN, *supra* note 104, at 269–70.

the time, go home. If there is to be a place of repose, a place where we are allowed to be alone with our thoughts or with each other, it makes sense for it to be the home—partly because if it were someplace else, we would likely want to *make* that place our home. If the home is not a place of repose, a place where we can be ourselves, it is hard to imagine where such a place might be found. Something similar might be said about the body, "the most basic vehicle of selfhood."[240] Notions of bodily modesty are culturally conditioned and vary widely, but the core idea that an individual's body is not public property, that the individual should control access to his or her body, runs deep and is likely universal. If our bodies are not our own, it is hard to imagine that anything is.

There are three further points worth making about the idea of a private sphere, regardless where its boundaries are drawn. First, the sanctuary to be found in the private sphere cannot be absolute. There is a tendency to talk of the "sanctity" and "inviolability" of the home and the body,[241] but language of that kind cannot be taken literally. It has never been the law, and could never be the law, that people can do whatever they want in their own homes and with their own bodies or that searches of homes or of bodies are categorically forbidden. Wherever it is located, the private sphere cannot be a zone the law can never penetrate, a zone from which the public is forever excluded. The right to repose within the sphere of privacy, the "right to be let alone," is necessarily qualified. If there is a sphere of privacy, it is a sphere to which the public has *less* access: sufficiently less to make it, meaningfully, a place of repose, a place where we can be ourselves.

Second, to say that there is a sphere of privacy is necessarily to say that there is a space outside that sphere, a space where the public has *more* access to the individual, a space where the individual has *less* of a "right to be let alone." For roughly half a century, the idea that privacy against government searches should be tied to particular locations, and in particular to the home, has been thought old-fashioned and overly formalistic. The Supreme Court famously declared in *Katz v. United States* that the Fourth Amendment "protects people, not places,"[242] and subsequent decisions linking privacy protections to the home have been criticized as inconsistent with that promise—a "return to the pre-*Katz* world."[243] The boundaries of a "zone of sanctuary" will inevitably seem arbitrary, at least at times, and its very existence will make infringements of privacy outside the zone seem more tolerable. So there are disadvantages to understanding privacy in this way. There are also advantages, though, and chief among these is that the idea of a sanctuary or refuge responds to deep and

240. Gerety, *supra* note 72, at 266.
241. *See* McClain, *supra* note 236.
242. 389 U.S. 347, 351 (1967).
243. David Cole, *Scalia's Kind of Privacy*, THE NATION, July 23, 2001, at 6 (discussing Kyllo v. United States, 533 U.S. 27 (2001)).

longstanding intuitions about psychological and political imperatives in the modern world.

Third and finally, any credible articulation of a sphere of privacy must address the problem of private violence. The primary reason that privacy—and particularly the idea of a realm of privacy centered around the home—fell into such disfavor with feminists in the late twentieth century was not that the boundaries of the private sphere seemed arbitrary, or that dividing the world into public and private spheres seemed too binary and formalistic. It was that the private realm did not seem much of a refuge or sanctuary to victims of domestic violence.[244] Because the protection that the private sphere provides can never be absolute, there are an endless series of decisions to be made about precisely how it operates: whether, for example, the police can enter a family home against the husband's objections but with the wife's consent.[245] Those decisions and how they are justified will help determine both the value of the sphere of privacy and its costs.[246]

B. Privacy and Civility

Post usefully describes privacy not as a thing that people have but as a set of "social norms that define the forms of respect that we owe to each other," norms that are part of "the decencies of civilization."[247] One implication of this view is that privacy is relational: the privacy that you have, want, or need vis-à-vis me may differ from the privacy that you have, want, or need vis-à-vis a third party. That is one reason why the Supreme Court has been wrong to declare that an individual can have no "legitimate expectation of privacy" in anything shared voluntarily with someone else[248]—and one reason the Court has been right to ignore that principle when it protects, for example, the privacy of a telephone call.[249] It is one reason the European Convention on Human Rights is wise to speak not of an individual's "right to privacy" but of a "right to *respect* for his private . . . life."[250]

---

244. *See, e.g.*, SUK, *supra* note 22, at 4–8, 125–27.

245. *See* Georgia v. Randoph, 547 U.S. 103 (2006) (answering no, absent an imminent danger of domestic violence or other extenuating circumstances).

246. *See, e.g.*, Reva B. Siegel, *"The Rule of Love": Wife Beating as Prerogative and Privacy*, 105 YALE L.J. 2117, 2150–74 (1996).

247. Post, *supra* note 112, at 2092–93; *see also* Post, *supra* note 220, at 1008–09; *cf.* BOYD, *supra* note 179, at 58 (suggesting that for many adolescents privacy "is more a matter of social norms and etiquette than technical access").

248. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).

249. *Cf. Smith*, 442 U.S. at 749 (Marshall, J., dissenting) (arguing that privacy "is not a discrete commodity, possessed absolutely or not at all"); *supra* text accompanying note 11 (discussing Justice Sotomayor's suggestion that the third-party doctrine in Fourth Amendment law should be reconsidered).

250. EUR. CONV. HUM. RTS., art. 8, § 1.

The relational nature of privacy also suggests that infringements of privacy may affect not just the victim but also the infringer. It is customary to reason that privacy matters either for non-consequentialist reasons, usually pertaining to the deontological value of dignity, or because of the harms suffered by people whose privacy is not respected, in particular the chilling effects on personality development, intimate relationships, and uninhibited discourse.[251] That leaves out the effects of privacy violations on the violators, the ways in which violating privacy can train individuals and organizations in habits of dehumanization and depersonalization. Those effects may be some of the most important reasons to care about privacy, particularly given the surprisingly weak evidence for the chilling effects of privacy violations on their victims.[252]

Philip Zimbardo, who designed and supervised the infamous Stanford Prison Experiment, reports that the students assigned to be "guards" assumed their roles slowly "and with considerable hesitation and some awkwardness";[253] the depersonalization and dehumanization that transformed these students into "perpetrators of abuse" was a gradual process.[254] Privacy violations, and particularly strip searches, seem to have played a significant role in that process. At the experimenters' instructions, the guards had the students assigned the role of "prisoners" strip and stand naked for inspection during their initial "intake."[255] Zimbardo was struck by the fact that "[w]ithout any staff encouragement" some of the guards immediately began to mock the size and appearance of the prisoners' genitals.[256] Further privacy intrusions were built intentionally into the experiment. The prisoners were "allowed no underwear, so when they ben[t] over their behinds show[ed],"[257] and Zimbardo told the guards that the prisoners were to have "no privacy at all": there would be "constant surveillance," so that "nothing [the prisoners did would] go unobserved."[258] On the second day of the experiment, when some of the prisoners tore numbers from the fronts of their uniforms as a protest against prison conditions, "[t]he guards immediately retaliate[d] by stripping each of them stark naked until their numbers [were] replaced."[259] Not only had privacy violations helped the guards to internalize their roles and depersonalize the inmates, but the guards had internalized the use of privacy violations as a mechanism of debasement and status reinforcement.

---

251. *See, e.g.*, INNESS, *supra* note 34, at 23–24, 95–97.

252. *See supra* notes 165–86 and accompanying text.

253. PHILIP ZIMBARDO, THE LUCIFER EFFECT: UNDERSTANDING HOW GOOD PEOPLE TURN EVIL 54 (2007); *see also id.* at 53–54, 56.

254. *Id.* at 56.

255. *Id.* at 40.

256. *Id.*

257. *Id.*

258. *Id.* at 55.

259. *Id.* at 60.

The role that privacy violations played in the process of dehumanization and depersonalization in the Stanford Prison Experiment appears to reflect a common phenomenon in real-life custodial institutions. Strip searches serve "a symbolic function of reaffirming imprisonment, shame, and lack of status."[260] The traumatizing effects of strip searches on inmates—the sense of humiliation, helplessness, and degradation that the practice can cause—are well documented.[261] Too little attention, though, has been paid to the effects of those searches on the guards who carry them out and the institutions where they are conducted, the ways in which "prisoners are dehumanized in the eyes of prison officials" who preside over strip searches and related privacy violations.[262] It is not surprising that the torture of prisoners at Abu Ghraib was accompanied by rampant and intentionally degrading strip searches and by interrogations conducted while prisoners were forced to remain naked. Nor should it be surprising that military investigators later concluded that at least in some cases the "tone and environment" surrounding these practices were "the causative factor that set the stage" for worse abuses.[263]

This is only anecdotal evidence. And we know even less about the effects of intrusive surveillance, as opposed to strip searches, on those who carry it out. But the evidence we do have gives reason to suspect that that the indignities associated with privacy violations affect the monitors as much as the monitored, if not more so—that routinely disregarding the "social norms" and "decencies" of privacy can lead organizations and their employees to dehumanize and depersonalize the people they search or surveil.[264] And although the evidence to support that intuition is anecdotal and fragmentary, it is considerably stronger than the evidence for the stultification thesis, which is a fixture of privacy discussions and, as we have seen, part of the reason those discussions have become increasingly dominated by concerns about data flows.

---

260. RUSSELL P. DOBASH, R. EMERSON DOBASH & SUE GUTTERIDGE, THE IMPRISONMENT OF WOMEN 205 (1986); *see also, e.g.*, JAMES GILLIGAN, VIOLENCE: OUR DEADLY EPIDEMIC AND ITS CAUSES 152–53 (1996).

261. *See, e.g.*, Ha, *supra* note 215, at 2740; Jude McCulloch & Amanda George, *Naked Power: Strip Searching in Women's Prisons*, *in* THE VIOLENCE OF INCARCERATION 107 (Phil Scraton & Jude McCulloch eds., 2009).

262. Sharon Dolovich, *Cruelty, Prison Conditions, and the Eighth Amendment*, 84 N.Y.U. L. REV. 881, 931–32 (2009).

263. Maj. Gen. George R. Fay, *AR 15-6 Investigation of the Abu Ghraib Detention Facility and 205th Military Intelligence Brigade*, *in* INVESTIGATION OF INTELLIGENCE ACTIVITIES AT ABU GHRAIB 6, 57 (2004); *see also* AIDAN DELGADO, THE SUTRAS OF ABU GHRAIB 153–54 (2007).

264. That may be part of the story of FBI counterintelligence activities in the 1960s, which often progressed from monitoring and infiltrating "subversive" groups to intentionally harassing and disrupting them. *See, e.g.*, DAVID CUNNINGHAM, THERE'S SOMETHING HAPPENING HERE: THE NEW LEFT, THE KLAN, AND FBI COUNTERINTELLIGENCE 79–145 (2004).

C. Toward a Different Conception of Privacy

We can now begin to sketch an alternative conception of privacy, a conception aimed at recovering what is lost when privacy is defined as control over the use and dissemination of information, a conception we might call "privacy as refuge." That conception should be informed by the intuitions connecting privacy with enclothement, with sanctuary, and with a zone of personal sovereignty. It should help make sense of the relational nature of privacy, the connection between privacy and civility, and the effects of privacy violations on the violators. And it should equip us to think sensibly about reconciling privacy with other imperatives, including protection against domestic violence.

With these desiderata in mind, we can provisionally define privacy as respect for a personal sphere shielded, but not completely immune, from public inspection and regulation. We can agree with Justice Blackmun that this sphere is defined partly by places (especially the home and the body) and partly by activities (especially those that relate to intimacy and self-definition).[265] We can say that privacy is not so much a thing or quantity that someone has, but rather that it resides in the respect that others, including governmental officers, show for an individual's sphere of personal sovereignty. Violations of that respect are important not just as a matter of principle but because of the tangible effects they can have both on the victim's sense of security and peace of mind and, perhaps more importantly, on the habits and ways of thinking of the individuals and organizations responsible for the violations. Privacy violations can train violators to depersonalize and dehumanize the individuals with whom they deal, and those are particularly dangerous habits and ways of thinking for governmental officers and agencies, because of the tools of coercion and violence they can lawfully employ. Finally, we can take note of a tension in this conception of privacy: the personal sphere draws its significance in part from the interpersonal interactions it protects, but those interactions can take forms that are abusive and that the public has a strong interest in detecting, interrupting, and punishing.

We should immediately note two ways in which it may be appropriate to limit our ambitions for this conception of privacy. First, concerns falling outside privacy as refuge may play important roles in determining whether a governmental search or seizure should be deemed "unreasonable" and therefore unconstitutional—or whether, even if constitutional, a particular law enforcement tactic should nonetheless be forbidden or restricted. Privacy should play a large role—maybe a larger role than any other interest—in determining the proper bounds on government searches and seizures, but it should not be the beginning and end of that inquiry. Second, as a practical matter the conception of privacy as control over information is not going away,

265. Bowers v. Hardwick, 478 U.S. 186, 203–07 (1986) (Blackmun, J., dissenting).

and that may be for the best. The concerns addressed by that rival conception are genuine and growing rapidly. There would be something to be said for addressing those concerns using some rubric other than privacy, but at this point the terminological choice has been made and is unlikely to be reversed. The two conceptions of privacy can coexist, and the dialectic between them might even prove beneficial: if privacy remains an "essentially contested concept," then the conflict between these two conceptions could be a productive way to remind ourselves, periodically, of the underlying values at stake.

That depends, though, on whether privacy as information control can be kept in its place: as only one conception of privacy, and a conception with some serious shortcomings. It should be apparent by now why privacy as refuge avoids some of the problems associated with defining privacy in terms of data flows.

First, unlike privacy as information control, privacy as refuge helps to highlight some of what is special about government searches and why someone concerned about privacy should care about the rules of criminal procedure. The government may not collect more information about us than corporations, but it can and does demand access that is denied to the commercial sector: access to the insides of our homes, and access to our bodies. That means that governmental searches can deny refuge in a way that commercial searches cannot. Beyond that, the coercive powers of the government make it a matter of special concern when its agencies and officers are trained, through privacy violations, in habits of depersonalization or dehumanization.

Second, privacy as refuge explains, as privacy as information control cannot, how privacy is connected to larger issues in criminal justice, and not just criminal justice for the rich. Much (although obviously not all) of the harm of incarceration has to do not with restrictions on movement but with the thorough denial of privacy: not privacy in the sense of control over information, but privacy in the sense of a zone of personal retreat. Much (but not all) of the indignity inflicted by aggressive stop-and-frisk policing has to do with violations of personal space and bodily privacy. And the brutalization associated with invasions of privacy connects in straightforward ways with concerns about violence at the hands of prison guards and police officers—but only if privacy is understood as centered around a zone of personal retreat, and not control over information.

Third, defining privacy as respect for a personal sphere makes clear why privacy should not be written off as dead or dying. Vastly more information is collected about us than ever before. That is undeniably cause for great concern and properly the focus of new legal protections. But most of us still have a place we can go where we are shielded from public scrutiny and government surveillance, and most of us still have parts of our lives we keep to ourselves or share only with our intimates. Those sanctuaries are worth protecting.

Furthermore, if privacy consists in respect shown for those zones of retreat, and not just in the zones themselves, then even after private snoopers invade an individual's privacy, there is a further and distinct injury if government officers follow suit.

Fourth, a conception of privacy anchored in respect for zones of personal refuge helps to avoid the circularity the Supreme Court has encountered in linking Fourth Amendment protection to "reasonable expectations of privacy." An infringement is not necessarily reasonable simply because it is lawful. Some reference to common norms is unavoidable in determining what counts as disrespecting a zone of privacy: it depends on what boundaries "we are socialized to experience . . . as essential prerequisites of our identity and self-respect."[266] But it is not all a matter of convention. If privacy consists in respect for a domain of personal sanctuary, then part of what we must ask, in determining the proper bounds of the private sphere, is whether excluding certain areas or aspects of life from that sphere would prevent it from serving as a meaningful refuge.

D. Privacy as Refuge, Applied

What difference might it make for policing and criminal procedure if we thought about privacy along the lines I have just proposed—as respect for zones of refuge, rather than as control over information? I want to suggest some partial, tentative answers to that question by briefly discussing five categories of intrusions: searches of the home, strip searches, investigatory stops and frisks, informants, and electronic surveillance.

1. Home Searches

There is a long history of providing heightened protections against searches of the home. At the "very core" of the Fourth Amendment, the Supreme Court has said repeatedly, sits "the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[267] The special treatment of the home and the reduced level of protection elsewhere have often been criticized as old-fashioned, formalistic, and class-biased, but if privacy is understood as a zone of refuge, then treating home searches as exceptionally threatening makes sense. The main reason it makes sense is not, as the Supreme Court sometimes suggests, that it has the pedigree of tradition,[268] but that the home is the paradigmatic place of "retreat." Invasions

266. Post, *supra* note 112, at 2094.

267. *E.g.*, Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013) (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

268. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001) (explaining that "in the case of the search of the interior of homes . . . there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*").

of the home are therefore especially threatening to the individual's zone of refuge.

At the same time, if the special status of the home in Fourth Amendment law is instrumental—if the home is valued because it is a refuge, and not simply because it is the home—then it seems important to ask how some of the privacy that homes provide to the fortunate can be extended to the less fortunate. Some people do not have homes. Some people have homes that do not function as zones of refuge: they share their homes with abusers, or their homes are simply too crowded or uncomfortable. In large part this is an agenda for social welfare policy—in particular, for housing policy and efforts to combat domestic violence—but it should also inform the law and policies regulating government searches and seizures. Everyone should have a home that functions as a refuge. Until they do, though, search-and-seizure law might profitably take into account the ways in which policing can enhance or threaten zones of refuge outside of the home. It might give reason, for example, to provide greater protection against some searches of vehicles. It might also have implications for the regulation of stop-and-frisk tactics, a matter to which I will return below.

Valuing the home as an instrumentality—as a refuge—might also require rethinking cases in which the interests of co-residents of a home seem to be in conflict. In *Georgia v. Randolph*,[269] for example, the Supreme Court confronted the following question: If one resident of a house invites the police in, but another resident objects, may the police enter? The Court said no, unless the police have a warrant or there are "exigent circumstances."[270] The Court tried to justify this result by appealing to "widely shared social expectations" regarding the behavior of "a caller standing at the door of shared premises."[271] That was unconvincing, in part because a police officer is obviously not just another "caller," and in part because, as the dissent pointed out, it was "entirely atypical" for any kind of "caller" to be invited in by one co-resident and told to stay out by another.[272] The dissent's reasoning, though, was even less convincing. The dissent reasoned that "[t]he Fourth Amendment protects privacy," and that therefore "[i]f an individual shares information, papers, *or places* with another, he assumes the risk that the other person will in turn share access to that information or those papers *or places* with the government."[273] But that was a non sequitur. Individuals assume the risks that the law makes them assume, and the question in *Randolph* was, or should have been, whether making cohabitants assume this particular risk raised an undue threat to

269. 547 U.S. 103 (2006).

270. *Id.* at 122–23.

271. *Id.* at 111, 113.

272. *Id.* at 127 (Roberts, C.J., dissenting). On the rhetorical uses of social conventions in *Randolph*, see SUK, *supra* 22, at 112–25.

273. *Randolph*, 547 U.S. at 128 (Roberts, C.J., dissenting).

privacy. Answering that question required an examination of how different outcomes would affect, in practice, the ability of shared homes to operate as places of retreat—an examination carried out neither by the majority in *Randolph* nor by the dissent.

2. Strip Searches

The triumph of the information-based conception of privacy has had a particularly striking effect on the way that strip searches are discussed. Strip searches were once the paradigmatic privacy violation: other violations of privacy were often described, metaphorically, as a kind of denuding.[274] But when privacy is understood first and foremost as control over information, strip searches no longer seem like an especially severe infringement—except perhaps in the way that they injure a certain set of arbitrary, socially conditioned sensibilities. Judges increasingly have difficulty even knowing what a strip search *is*. Is forcing a prisoner to disrobe especially violative only if the guards touch him?[275] Has a thirteen-year-old girl undergone a "strip search" if she is allowed to keep her undergarments on and is merely forced to pull them away from her body?[276] The definitional confusion is a byproduct of conceptual uncertainty. Why is the information disclosed by disrobing particularly important? And if the privacy invaded by a strip search does not have to do with information, what does it concern?

The sense persists, though, that there is something distinctively violative about a strip search—and that the violation has to do with privacy. Simply saying that this is a different kind of "privacy" than the "privacy" threatened by electronic surveillance is unsatisfactory; it amounts to saying that the same word refers to two different things, which bear at most a "family resemblance" to each other. That is possible, but it does not fit the longstanding intuition that these things are more closely related, that a strip search is not a peculiar kind of privacy violation but a *paradigmatic* privacy violation. The most convincing explanation of that intuition is that the body is so closely linked to the self that it stands at or near the center of any plausibly sketched zone of personal sovereignty.

This means it is right to treat strip searches as particularly serious and particularly worrisome infringements of privacy. It also means there are strong grounds for concern about the effects of strip searches—especially when conducted routinely or cavalierly—not just on the people being searched but on the officers and organizations doing the searching. Strip searches can not only send a signal of disrespect and humiliation to their victims, they can train the

274. *See supra* notes 59–62 and accompanying text.
275. *See supra* notes 201–05 and accompanying text.
276. *See supra* note 200 and accompanying text.

searchers and their employers to depersonalize and dehumanize the individuals in their charge.[277]

3. Investigatory Stops and Frisks

Conceiving privacy as protecting a sphere of personal sovereignty—non-absolute but nonetheless vital—suggests that investigatory stops and frisks should be understood as raising concerns in part because of the ways in which they intrude on privacy. A stop itself, even without a frisk, is a kind of violation of privacy, because for most of us the zone of personal sovereignty that we prize includes the ability to go about our ordinary affairs—to move our bodies around—without arbitrary interference from the state. A frisk, which amounts to tactile exploration of the subject's body, is a still greater infringement of privacy; it is the tactile analog of a visual strip search. (Recall that the Supreme Court found the term "strip search" imprecise in *Florence* in part because a search involving touching was more invasive than a purely visual search.)[278] Thinking about stops and frisks in this way may help us to remember what the Supreme Court itself stressed when it conditioned use of the stop-and-frisk tactic on specific, articulable suspicion: that the tactic is not a "petty indignity" but "a serious intrusion upon the sanctity of the person."[279] And understanding stops and frisks as infringements of privacy, akin in important respects to strip searches, should lead us to worry about the symbolic significance of indiscriminate and unnecessarily aggressive use of the stop-and-frisk technique—the messages that it can send not only to suspects, but also to the officers and law enforcement organizations carrying out these seizures and searches.[280]

4. Informants

The reduction of privacy to informational privacy has made it harder to appreciate some of the unique threats posed by the widespread use of informants. Informants are not just another means of collecting information; their use can invade and corrode friendships, intimate relationships, and communities of trust.[281] Even more so than searches of the home, informants can endanger the very existence of a personal sphere, a zone of retreat. Winston Smith could hide in a recess of his apartment, out of sight of the telescreen, but he could not survive in solitude. What did him in were the spies he

277. *See supra* notes 253–63 and accompanying text.

278. *See supra* note 205 and accompanying text.

279. Terry v. Ohio, 392 U.S. 1, 17 (1968).

280. *See, e.g.*, EPP, MAYNARD-MOODY & HAIDER-MARKEL, *supra* note 217, at 5–6, 134–51.

281. For a thoughtful discussion, see NATAPOFF, *supra* note 172, at 116–19; *see also supra* note 171 and accompanying text. Natapoff points out that the widespread use of informants may be particularly harmful in poor, inner-city communities, where "social networks are more disorganized and people's lives and spaces are less private." NATAPOFF, *supra* note 172, at 117.

unknowingly made a part of his life—and, even more so, his own coerced transformation into an informant. That aspect *of Nineteen Eighty-Four* reflected, of course, what Orwell and so many others saw as an especially frightening and destructive tactic of state control in the totalitarian societies of mid-twentieth century Europe.

The use of informants is notoriously among the least regulated of law enforcement tactics in the United States.[282] Recognizing the distinctive threats that informants pose to privacy could be the first step in bringing informants under more sensible control, and that recognition will itself be more likely if privacy is understood as a zone of refuge, rather than a set of restrictions on data flows.

5. Electronic Surveillance

The prevailing, information-centered conception of privacy is widely thought to be well-suited to addressing the geometrically proliferating ways in which our movements, transactions, and conversations are subject to electronic monitoring. This perception is one of the reasons why the information-centered conception of privacy has become so dominant. Ironically, though, reducing privacy to informational privacy has hindered sensible thinking about the proper legal limits on government surveillance in the information age. The problem is that so much information is being collected and collated in so many different places, corporate as well as governmental, and that increasingly these data flows seem not only commonplace but a central part of everyday life. We need some way to distinguish the data flows that are most problematic, and this is precisely what focusing on information alone cannot provide. Surveillance tactics are sometimes challenged or defended based on the amount of information they amass, but that is rarely convincing: in part because the background flood of information makes it hard to assess how much information should count as a lot, and in part because it seems clear that some data should matter more than others. Sometimes it is suggested that surveillance techniques should matter only if and to the extent that they gather "personal" information, but this raises the question of what should count as "personal." As I have suggested earlier, that amounts to another way of asking what should be private.

I have argued that privacy should be understood as respect for a sphere of individual sovereignty partially shielded from public scrutiny and regulation. Electronic surveillance impinges on privacy, understood in this manner, to the extent that it is inconsistent with respect for that sphere. Because the sphere is socially constructed, what counts as disrespect for it will also be, to a great

282. *See, e.g.*, NATAPOFF, *supra* note 172, at 45–67. For a useful comparative perspective, see Jacqueline Ross, *Undercover Policing and the Shifting Terms of Scholarly Debate: The United States and Europe in Counterpoint*, 4 ANN. REV. L. & SOC. SCI. 239 (2008).

extent, a matter of convention; this is why it has made a certain amount of sense for the Supreme Court to define "reasonable expectations of privacy"[283] as those that "society is prepared to recognize as reasonable."[284] But it is not all a matter of convention. For example, it is difficult to imagine any delineation of the private sphere that does not include a space for intimacy: not just for physical intimacy, but for expressing thoughts and feelings to oneself and to one's intimate acquaintances without sharing them with the world.[285] Some forms of electronic monitoring seem inconsistent with respect for any such space. Unfettered eavesdropping on public telephone booths (when there were public telephone booths) fell into that category; that is why the Supreme Court was right to say that to disrespect the privacy of telephone booths was "to ignore the vital role that the public telephone has come to play in private communication."[286]

Assessing which kinds of electronic surveillance are most threatening to privacy as refuge is a complicated task. I will not pursue it here. I do want, though, to make a few preliminary points about that assessment.

First, a simple distinction between "identifying" and "anonymous" data, or between "message" and "metadata," is likely to prove of only limited help. Advances in data analysis make truly "anonymous" data increasingly rare,[287] and it is far from obvious that a sphere of privacy can function effectively as a zone of retreat if it does include some protection not only for what we say to others, but also who we speak with, when we speak with them, how frequently, and for how long.

Second, assessing the privacy impact of any particular form of electronic monitoring requires some consideration of what spaces of retreat it leaves untouched. Public telephones circa 1967 played a "vital role . . . in private communication," and eavesdropping on phone booths was a serious violation of privacy, in part because many Americans had no realistic alternative to relying on pay phones in maintaining a range of private relationships.[288] Technologies of social interchange today are more varied, and sorting out which venues are "vital" to the preservation of a personal sphere is accordingly more difficult, but it is no less important.

Third, technological advances can alter the degree to which particular forms of electronic surveillance threaten the existence of a private sphere. New technologies can create new forms of private interaction, but they can also render existing forms of surveillance more troubling. That is particularly true of advances in automated data analysis, which, as I noted earlier, have the

283. Katz v. United States, 389 U.S. 347, 362 (1967) (Harlan, J., concurring).
284. Oliver v. United States, 466 U.S. 170, 191 (1984).
285. *See, e.g.*, INNESS, *supra* note 34, at 74–94.
286. *Katz*, 389 U.S. at 352 (1967).
287. *See generally* Ohm, *supra* note 89.
288. *Katz*, 389 U.S. at 352 (1967).

potential to turn being passively recorded (on the Internet or on the sidewalk) into being actively watched.[289]

Fourth and finally, privacy is not everything. There are good reasons other than privacy to be concerned about government surveillance, and there are plenty of ways for a search or seizure to be "unreasonable" other than impinging too severely on privacy. Information is power, and keeping reasonable restraints on governmental power is an imperative for any liberal democracy—wholly aside from whether that power is accumulated or exercised in ways that impinge on privacy. Nonetheless privacy is worth protecting. It is not meaningless, it is not dead, and it is not all about information.

289. *See supra* note 189 and accompanying text.