1984 is So Last Century: Privacy and Policing in the Information Age

(or, Too Much Information: How Not to Think About Privacy and the Fourth Amendment)

David Alan Sklansky*

[August 23, 2013]

Privacy has long been understood to be the core concern of search-and-seizure law, and—especially in the wake of recent disclosures about surveillance by the National Security Agency—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." If it did, the action was unconstitutional unless it was itself "reasonable," which generally meant that it had to be based on probable cause and carried out pursuant to a warrant, unless it fell within a judicially defined exception to one or both those requirements.

The consensus has unraveled. Complaints about the disarray of Fourth Amendment law deserve to be greeted with skepticism: law professors have been saying for decades that search and seizure law is a mess, and for most of that time the complaints have seemed overwrought. Fourth Amendment law has been more predictable and better ordered than many other fields of jurisprudence—sufficiently well-defined to be applied, generally with confidence, by police officers with minimal legal training. But the disarray in search-and-seizure law today is not simply a matter of doctrinal confusion, although there is plenty of that—more, probably, than at any time since the 1960s. The uncertainty extends to the underlying philosophy of search and seizure law, and in particular to the idea that the job of the Fourth Amendment should be to protect privacy. That idea, in turn, has been put into doubt by uncertainty about how important privacy is, about whether the Fourth Amendment can be of much help in protecting it, and, even more fundamentally, about how privacy itself can be best be defined, and whether it can be defined at all.

---

* Yosef Osheawich Professor of Law, University of California, Berkeley. I thank Hamilton Jordan Jr. and Corey Laplante for research assistance, and Martha Minow, Melissa Murray, Pamela Samuelson, and Jennifer Urban for helpful guidance.

The sources of the doctrinal disarray, widely familiar to legal scholars, are twofold. First, the exceptions to the warrant and probable cause requirements have proliferated and in some cases grown so open-ended that the Supreme Court now treats the 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. 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 had 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 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.[1] 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,"[2] 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 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.[3] Justice Alito, writing for a four-Justice minority, adhered to the longstanding, consensus view that the Court had in fact done away with the trespass test, and for good reason, in *Katz v. United States*,[4] the source of the "reasonable expectations of privacy" approach.[5] But Justice Alito also criticized the circularity and subjectivity of the *Katz* test (echoing complaints long voiced by scholars and by other members of the Court[6]), and he suggested that legislatures are better than suited

[1] 132 S. Ct. 945 (2012).
[2] United States v. Knotts, 460 U.S. 276, 281 (1983).
[3] *Jones*, 132 S. Ct. at 950-53.
[4] 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. Florence v. Jardines, 133 S. Ct. 1409, 1414 (2013).
[5] *Jones*, 132 S. Ct. at 959-60 (Alito, J., concurring in the judgment).
[6] *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

than courts to develop protections against new technologies that threaten privacy.[7] And he departed from the conventional understandings of *Katz* in reasoning that satellite monitoring of vehicles movements on public highways *does* infringe on "reasonable expectations of privacy," depending on how long it continues: in *Jones*, it lasted four weeks, and Justice Alito thought that crossed the line, at least for "most offenses."[8] Justice Scalia, in turn, criticized the concurrence out for introducing "novelt[ies]" and "thorny problems" of line-drawing into Fourth Amendment jurisprudence, but even he conceded that those problems might need to be faced in any event as soon the Court confronted a satellite monitoring case like *Jones* but not involving 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 "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, 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.

The doctrinal disarray, though, 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

---

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, No. 12-207, slip op. at 24-25 (June 3, 2013). "Reasonable expectations of privacy" can be defined by social norms rather than legal rules, *see, e.g.*, Rubenfeld, *supra*, at 107, but then *Katz* test runs into a different kind of circularity: the tendency over time for people to become accustomed to violations of privacy. *See infra* notes 92-100 and accompanying text.

[7] *Jones* at 962-63 (Alito, J., concurring in the judgment).

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

[9] *Id.* at 953-54 (opinion of the Court). 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] *Id.* 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.

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 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 considerable 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 seem these days 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. The threats that law enforcement poses to privacy seem dwarfed not just by commercial threats to privacy but also by concerns about other, more pressing threats posed by law enforcement: racial profiling, police violence, and mass incarceration. "Privacy scholars" by and large are 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." There is a growing sense among scholars in both camps, moreover, that any needed protection against government infringements on privacy is more likely to come from statutes and regulations than from courts and case law.

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, in part in work by legal scholars and other academics. 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 variants of this idea. One is conceptual, one is empirical, and the third 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 means too many different things; we would do better just to replace any invocations of privacy with invocations of whatever underlying value the term is standing in for: bodily autonomy, or control over how information about oneself is used, 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]

---

[12] *See* Polly Springer, *Sun on Privacy: 'Get Over It,'* Wired.Com, Jan. 26, 1999, available at www.wired.com (quoting Scott McNealy).

[13] *See, e.g.*, Michael Arrington, *OK You Luddites, Time to Chill Out on Facebook Over Privacy*, Techcrunch, Jan. 12, 2010, available at techcrunch.com (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").

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 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 particular idea about 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 that this is an important value 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 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.[14]

Part I of this article will discuss the arguments for untethering 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. Part III sketch a different understanding of privacy and explore its implications for Fourth Amendment law, drawing lessons from the earlier parts of the article.

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 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

[14] In a separate paper, I plan to challenge two other increasingly common ideas about privacy and the Fourth Amendment: that any protections needed against government infringements of privacy in the Information Age are best developed outside of the courts and outside of constitutional law; and that the various puzzles encountered when thinking about privacy and the Fourth Amendment can solved or circumvented through some kind of invocation of the past: either a focus on the text of the Fourth Amendment, or the study of its history, or simply an effort to "preserv[e] . . . that degree of privacy against government that existed when the Fourth Amendment was adopted."[14] Jones v. United States, 132 U.S. at 950 (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

famously argued in *Olmstead v. United States*[15] that the Fourth Amendment protected against any "unjustifiable intrusion by the government upon the privacy of the individual," but he wrote in dissent.[16] Even the majority opinion in *Katz v. United States*[17]—the decision generally thought to have vindicated Justice Brandeis's position in *Olmstead*[18]—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."[19] But a concurring opinion in *Katz* explicitly tied Fourth Amendment protections to "reasonable expectations of privacy"[20]—i.e., to "actual" expectations of privacy "that society is prepared to recognize as reasonable"[21]—and the Court soon embraced that formulation and made it the centerpiece of its search-and-seizure jurisprudence.[22] 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.[23]

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: by the sense that if the Fourth Amendment protects only privacy, there soon will be little left for it to protect.[24] But most of them also think there are and always have been more important values at stake when assessing government searches and seizures.[25] 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

---

[15] 277 U.S. 438 (1928).

[16] *Id.* at 478 (Brandeis, J., dissenting).

[17] 389 U.S. 347 (1967).

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

[19] 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).

[20] 389 U.S. at 362 (Harlan, J., concurring).

[21] *Id.* at 361.

[22] *See* Terry v. Ohio, 392 U.S. 1, 9 (1968); Sklansky, *supra* note 18, at 254.

[23] *See, e.g.*, JEANNIE SUK, AT HOME IN THE LAW: HOW THE DOMESTIC VIOLENCE REVOLUTION IS TRANSFORMING PRIVACY 124 (2009).

[24] *See, e.g.*, Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309 (2012); Rubenfeld, *supra* note 6, 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).

[25] *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 U.C.L.A. L. REV. 1 (2009); Rubenfeld, *supra* note 6, at 103-04, 108; Sundby, *supra* note 24, at 1777-83.

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 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 in keeping with 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.[26] 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.[27] Scholars and popular writers alike linked totalitarianism with an absence of privacy; it became common, even ubiquitous, to cite Orwell's *Nineteen Eighty-Four* for what life would look like if attacks on privacy were not resisted.[28] The 1960s were also, of course, when the Supreme Court began to protect intimate autonomy under the rubric of a penumbral right to privacy.[29]

---

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

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

[28] *E.g.,* PACKARD, *supra* note 26, 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, e.g.*, ALAN F. WESTIN, PRIVACY AND FREEDOM 4, [*] (1970); Neil M. Richards, *The Dangers of Surveillance*, [*] HARV. L. REV. [*], [*] (forthcoming 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 [*]; 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.

[29] *See* Griswold v. Connecticut, 381 U.S. 479, 484-86 (1965).

Assaults on privacy were seen in many places in the 1960s: not just in government surveillance and in regulations of intimate association, but in the employment screening, both public and private; in workplace monitoring; in loyalty oaths and polygraphy; in personality testing of schoolchildren; in investigations by insurance companies and credit bureaus; in the encroaching noise and commotion of urban life; and in the introduction of additives to foods and drinking water.[30] 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.[31]

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 there 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."[32] Prosser disputed the existence of a comprehensive "right of privacy" in tort law[33], much as Justice Stewart later claimed there was no broad "right to privacy" in constitutional law. 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.

A broader challenge began to be mounted in the 1970s. The philosopher Judith Jarvis Thompson argued in a particularly influential essay that the whole idea of moral right to privacy was invariably "derivative" of other, more basic claims, and that clear thinking would be advanced by dropping the rhetoric of privacy out of the argument.[34] By the 1980s this kind of skepticism or "reductionism" was common in scholarly treatments of privacy.[35] 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."[36] The

---

[30] *See, e.g.,* BRENTON, *supra* note *supra* 26; PACKARD, *supra* note 26.
[31] *See* Roe v. Wade, 410 U.S. 113 (1973).
[32] William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383, 422 (1960).
[33] 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).
[34] Judith Jarvis Thompson, *The Right to Privacy*, 4 PHILOS. & PUB. AFF. 295, 313 (1975).
[35] Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421 (1980); *see also* JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 21, 39 n.1 (1996).
[36] Colin Bennett & Rebecca Grant, *Introduction*, *in* VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE (Colin Bennett & Rebecca Grant eds., 1999); *see also, e.g.*, Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335 (1992); Peter Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 951, 975 (2006); Diane L.

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.[37] "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."[38]

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,"[39] lacking any "'essential' or 'core' characteristics."[40] 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."[41] 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."[42] Privacy, Solove suggests, is one of those concepts, consisting in "many different yet related things"[43]—things that share, in Wittgenstein's terminology, a "family resemblance."[44]

Wittgenstein was more radical than Solove makes him out to be,[45] 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."

Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 299 (1983).

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

[38] *Id.* at 1221.

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

[40] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 8 (2008). For examples of Solove's influence, see Crocker, *supra* note 25, 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); Richard B. Bruyer, *Privacy: A Review and Critique of the Literature*, 43 ATLA. L. REV. 553 (2006); Leslie Meltzer Henry, *The Jurisprudence of Dignity*, 160 U. PA. L. REV. 170, 188-89 (2011).

[41] SOLOVE, supra note 40, at 10-11.

[42] SOLOVE, supra note 40, at 9 (citing LUDWIG WITTGENSTEIN, PHILOSOPHICAL INVESTIGATIONS (G. E. M. Anscombe trans., 3d ed. 1958)).

[43] *Id.*

[44] WITTGENSTEIN, *supra* note 42, at ¶ 67.

[45] *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 CAL. 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").

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 regulation: "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 necessarily will differ in some ways 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.'"[46] 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."[47] 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 departs 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"[48] He was advancing an anti-essentialist theory of language: words generally could be understood, he suggested, only by looking at how they were used.[49] The meaning of the word "game," for example, consisted for Wittgenstein in the things for which people used that term as a referent.[50] 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."[51] 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.[52] It is instructive, though, that scholars who study games as games, not just as an illustration of

---

[46] SOLOVE, supra note 40, at 13

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

[48] Henry, *supra* note , at 188.

[49] *See* WITTGENSTEIN, *supra* note 42, 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 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).

[50] *See id.* at ¶ 69.

[51] *Id.* at ¶¶ 66-67.

[52] *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);

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.[53]

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. [54] 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 treating dropping the language of privacy, or treating it 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.[55]

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.[56] Some words really may be so vague that they impede careful

---

Kent Greenawalt, *Religion as a Concept in Constitutional Law*, 72 CAL. 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). Wittgenstein and his evocative concept of "family resemblances," have also made their way into court opinions. *See, e.g.*, Empress Casino Joliet Corp. v. Balmoral Racing Club, Inc., 651 F.3d 722, 728 (7th Cir. 2011); Ortiz v. Bank of America, 547 F. Supp. 550, 568 n.27 (E.D. Cal. 1982); Taggart v. State, 822 P.2d 243, 248 (Wash. 1992).

[53] *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 RULES OF PLAY: GAME DESIGN FUNDAMENTALS 72, 82 (2004); SUITS *supra* note 47. Bernard Suits, who put forward and defended 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 47, at 21 (quoting WITTGENSTEIN, *supra* note 42, at ¶ 66). Suits called Wittgenstein's "family resemblance" approach to language "an Idol of the Academy" that prejudiced it against any efforts at definition; in contrast, he suggested, "the man in the street . . . is a working essentialist." SUITS *supra* note 47, at 172. Despite Wittgenstein's popularity among legal scholars, in practice most of them probably are "working essentialists," too, precisely because definitions are such a natural tool of normative work.

[54] 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).

[55] In this regard see Ruth Gavison's helpful discussion of privacy "reductionism" in Gavison, *supra* note 35, at 460-67.

[56] 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

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.[57] Others have a similar view of "equality" as a legal or political ideal.[58] I think they are wrong about those concepts,[59] 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 proof is in the eating: 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."[60] References to the realm or sphere or domain of privacy, with their connotations both of sovereignty and physical space,[61] were ubiquitous in legal, popular, and philosophical discussions of privacy in the 1960s and 1970s; they are still common, although less so, today.[62] 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

---

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 47, 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, [*] (2010).

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

[58] *See* Peter Westen, *The Empty Idea of Equality*, 95 HARV. L. REV. 537 (1982).

[59] *See* DAVID ALAN SKLANSKY, DEMOCRACY AND THE POLICE 10, 102-04 (2008).

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

[61] *See, e.g.*, INNESS, *supra* note 35, 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").

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

to privacy rose rapidly to prominence. Vance Packard called his best-selling expose of threats to privacy *The Naked Society*, and it was common to refer to describe privacy violations as leaving the victim "naked before the world."[63]

The conjunction of these two connotations—sovereign space and enclothement—suggests that privacy, at least as 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 another question, of course, whether a precise definition can be formulated that captures the intuitions suggested by 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.

They 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. And this is the second of the three closing points I wanted to make about whether the concept of privacy has any content. Despite the popularity of Solove's suggestion that privacy is a diversity things without any common essence, most discussions of privacy today—certainly most discussions by people who think of themselves as "privacy scholars"—does treat privacy as having a core meaning. The core meaning of privacy 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,"[64] but the taxonomy of privacy that he proposes is, he says, "arranged . . . around a model that begins with the data subject,"[65] and fourteen of the sixteen topics in his taxonomy pertain, by his own analysis, to "information collection," "information processing," or "information dissemination."[66] 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.

---

[63] 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 26, at 11 (warning that every decrease in privacy "denudes us further still"); WESTIN, *supra* note 28, 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 (1979).

[64] SOLOVE, *supra* note 40, at 24-29.

[65] *Id.* at 103.

[66] *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.

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,[67] but today it has taken over. Control over data flows has become "the cornerstone of our modern right to privacy."[68] This conception of privacy is sometimes traced back to Alan Westin's 1970 book, *Privacy and Freedom*. Westin's ideas about privacy were textured. Much of his book treated privacy as kind of withdrawal or isolation from society.[69] For example, he described privacy as having "four basic states"—"solitude, intimacy, anonymity, and reserve"[70]—and he suggested that "[e]ither too much or too little privacy can create imbalances which seriously jeopardize the individual's well-being."[71] 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."[72] Within a decade this became perhaps the most widely cited definition of privacy among scholars,[73] on its way toward becoming "a dogma of contemporary jurisprudence."[74] When Westin died in 2013, this definition of privacy was what he was chiefly remembered for. As one scholar explained to the New York *Times*, Westin "transformed the privacy debate by defining privacy as the ability to control how much about ourselves we reveal to others."[75]

Later I will argue that reducing privacy to informational privacy is a bad idea, but for now my claims are more modest. Despite the nods toward anti-essentialism in much modern scholarship about privacy, there is in fact a unified conception of privacy

---

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

[68] Margalit Fox, *Alan F. Westin, Who Transformed Privacy Debate Before the Web Era, Dies at 83*, N.Y. TIMES, Feb. 23, 2013, at A17 (quoting Marc Rotenberg, Executive Director of the Electronic Privacy Information Center); *see also, e.g.*, Schwartz, *supra* note 28, 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").

[69] 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, *An Interview With Herbert Marcuse*, PSYCHOL. TODAY, Feb. 1971, at 37-38.

[70] WESTIN, *supra* note 28, at 31.

[71] *Id.* at 40.

[72] *Id.* at 7. For an earlier version of this idea, see Fried, *supra* note 27, at 483 (defining privacy as "control over information about oneself").

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

[74] 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. A decade a half later Pamela Samuelson noted that "[t]he idea of legal protection for personal data resonates so little with the 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 67, at 752-53. There would be no such difficulties today.

[75] Fox, *supra* note 68 (quoting Professor Jeffrey Rosen).

underlying and shaping most of that scholarship, as well as more and more discussions outside academia. It is the conception of privacy as control over personal information.[76] 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.

The third and last point I want to make in closing about the meaningfulness of the concept of privacy is this: it may be helpful and important to try to define privacy even if the definition remains elusive. 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" (i.e., 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 be faithful to or understanding the merit of some generally agreed upon exemplars or paradigmatic cases.[77] Gallie's principal examples were "work of art," "democracy," and "a Christian life." I will argue later in this article that privacy may in fact be "essentially contested concept" in Gallie's sense. Even it is not, though, we should remain open to the possibility that, for reasons related to but not identical to the ones Gallie 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

---

[76] *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"); Natash Singer, *An American Quilt of Privacy Laws, Incomplete*, N.Y. TIMES, Sunday Business, Mar. 31, 2013, at 1 (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. [*], [*] (2013) (arguing that Fourth Amendment law should take guidance from scholarship on "information privacy law").

[77] W.B. Gallie, *Essentially Contested Concepts*, 56 PROC. ARISTOTELIAN SOC'Y 167 (1955-56), *reprinted in* THE IMPORTANCE OF LANGUAGE 121, 135 (Max Black ed., 1962). For helpful discussions of Gallie's argument, see WILLIAM E. CONNOLLY, THE TERMS OF POLITICAL DISCOURSE 10-44 (1974); Jeremy Waldron, *Vagueness in Law and Language: Some Philosophical Issues*, 82 CAL. L. REV. 509, 529-34 (1994).

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 privacy around 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.[78] 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.[79] They are joined by a growing number of audio sensors[80] and, of course, by the explosion of cameras on mobile telephones, and perhaps soon in eyeglasses.[81] Police departments are making increasing use of cameras mounted on aerial drones; in the near future that technology will almost certainly used much more widely, and not just by the police.[82] And mobile telephones track their users' locations even when their cameras and microphones are turned off.[83]

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 more powerful.[84] Video images from far-flung camera systems are stitched together;[85] license plates photographed by

---

[78] *See, e.g.*, JAMES B. RULE, PRIVACY IN PERIL (2007).

[79] *See, e.g.*, SIMON CHESTERMAN, ONE NATION UNDER SURVEILLANCE: A NEW SOCIAL CONTRACT TO DEFEND FREEDOM WITHOUT SACRIFICING LIBERTY 145-54 (2011); Ariel Kaminer, *Has the Big Apple Become the Big Eyeball?*, N.Y. TIMES, May 7, 2010, at A1.

[80] *See, e.g.*, Kashmir Hill, *Public Buses That Listen to Passengers' Conversations Have Been Around for Five Years*, Forbes.com, Dec. 11, 2012, available at www.forbes.com; Chris Matyszczyk, *Is Your Bus Bugged for Sound?*, CNET.com, Dec. 12, 2012, available at news.cnet.com; Candy Thompson, *MTA Recording Bus Conversations to Eavesdrop on Trouble*, Baltimore SUN, Oct. 17, 2012, at [*].

[81] *See, e.g.*, Charles Arthur, *Google Glass: Is it a Threat to Our Privacy?*, GUARDIAN, Mar. 6, 2013, available at www.guardian.co.uk.

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

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

[84] *See, e.g.*, Steve Lohr, *The Age of Big Data*, N.Y. TIMES, Sunday Review, Feb. 1, 2012, at 1.

[85] This is why the term "closed-circuit" is "[a]lready … misleading." CHESTERMAN, *supra* note 79, at 147.

surveillance cameras are automatically read, identified, and tracked;[86] automated facial recognition is crude but getting steadily more accurate.[87] Store purchases—and, increasingly, other behaviors while shopping—are tracked and cross-referenced.[88] Online clicks are compiled and analyzed. Medical records, school transcripts, and credit reports are increasingly accessible.[89] Merging separate databases makes it difficult if not impossible to maintain the anonymity of any records.[90] The federal government is said to be constructing a vast data facility "to sort all of the trillions of words and thoughts and whispers captured in its electronic net."[91]

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.[92] 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 New York *Times* described this as "a crime-fighting experiment that civil libertarians call Orwellian."[93] 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—privacy concerns were not mentioned.[94] So

---

[86] *See, e.g.*, *id.* at 147; Julia Angwin & Jennifer Valentino-Devries, *New Tracking Frontier: Your License Plates*, WALL STREET JOURNAL, Sept. 29, 2012, at [*]; Shawn Musgrave, *Licene Plate-Reading Devices Fuel Privacy Debate*, Boston GLOBE, Apr. 9, 2013, at [*]; Robert Patrick, *Police Cameras Gobbling Up Driver Data in St. Louis*, St. Louis POST-DISPATCH, Nov. 26, 2012, at [*]; Eric Roper, Minneapolis STAR TRIBUNE, Aug. 10, 2012, at [*]; Ali Winston, *Police Tracking of Cars on Rise*, S.F. CHRON., June 26, 2013, at A1.

[87] *See* Charlie Savage, *Facial Scanning is Making Gains in Surveillance*, N.Y. TIMES, Aug. 21, 2013, at A1; Natasha Singer, *Facial Recognition Makes the Leap from Sci-Fi*, N.Y. TIMES, Nov. 13, 2011, at [*].

[88] *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, Magazine, Feb. 19, 2012, at 30.

[89] CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT [*] (2007).

[90] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1201 (2010).

[91] James Bamford, *The Black Box*, WIRED, Apr. 2012, at 78, 81.

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

[93] Nick Ravo, *Police Install Cameras in Washington Sq. Park*, N.Y. TIMES, Jan. 2, 1998, at [*]; *cf., e.g.*, Andrea Estes, *Smile! You're on "Traffic Camera,"* Boston HERALD, Dec. 15, 1994, at 1 (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*").

[94] *See More Cameras for New York City Streets*, N.Y. TIMES, Mar. 2, 2013, at A16.

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.[95] 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."[96] Today public surveillance cameras in the United States are commonplace, just as in Britain.[97] In the wake of the bombings at finish line of the 2013 Boston Marathon, no one thought it remarkable, let alone troubling, that law enforcement officials could quickly find video records of the suspects walking along the sidewalk.[98] 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."[99] There is a downward creep in what strikes us as creepy.[100]

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,[101] 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

---

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

[96] Jeffrey Rosen, *A Cautionary Tale for a New Age of Surveillance*, N.Y. TIMES, Magazine, Oct. 7, 2001, at [*], [*].

[97] *See, e.g.*, SLOBOGIN, *supra* note 89, 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").

[98] *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.

[99] 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 Panopticism*, N.Y. TIMES, July 12, 2013, at A25 (noting with dismay that "[t]The revelations 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").

[100] 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).

[101] *See supra* notes 12 & 13.

long as 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."[102] Bennett Capers agrees: "Quite simply, we have become a surveillance state."[103] What we need, Paul Ohm explains, is a Fourth Amendment for "a world without privacy."[104]

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 is 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*,[105] has become something of a touchstone for death-of-privacy predictions[106]—foresees or would welcome a world without *any* kind of privacy. "It is 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.[107] Still, he insists that ways can and must be found to protect what he calls "bedroom privacy"[108]:

> [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 age, when camera-bearing robots may swarm the skies, we will all need . . . some zone of sanctuary where can feel unobserved. Some corner where our hearts can remain forever just our own.[109]

Brin explicitly links this kind of privacy with traditional protections of the home and the venerable legal concept of "curtilage."[110] I will have more to say about that linkage later.[111] 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.

---

[102] Rubenfeld, *supra* note 6, at 118.
[103] I. Bennett Capers, *Crime, Surveillance, and Communities*, [*] FORDHAM URB. L.J. [*], [*] (forthcoming 2013).
[104] Ohm, *supra* note 24, at 1310; *cf.* Sundby, *supra* note 24, at 1758 (suggesting the need to adapt the Fourth Amendment to "a non-private world").
[105] DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (1998).
[106] *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 24, at 1313.
[107] BRIN, *supra* note 105, at 8-9.
[108] *Id.* at 269.
[109] *Id.* at 269-70.
[110] *See id.* at 270.
[111] *See infra* text accompanying notes 221-237.

Actually, the privacy widely thought to be dead or dying is not just informational privacy but 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."[112] But of course we never did.[113] 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 are 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. Even informational privacy is not dead, unless we mean by informational privacy the ability to keep our secrets *completely* secret. And that 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.[114] 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 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 about *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 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 on that control come not the government but from private entities. Police departments matter less than retailers, credit bureaus, and internet service providers.[115] Even law enforcement officials

---

[112] Sundby, *supra* note 24, at 1759 (emphasis added).
[113] *See* Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2090-91 (2001).
[114] *See, e.g.*, Rubenfeld, *supra* note 6, at 110-15; *cf. supra* text accompanying note 11 (discussing Justice Sotomayor's suggestion that the third-party docrine in Fourth Amendment should be reconsidered).
[115] *See, e.g.*, COHEN, *supra* note 92, 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).

increasingly rely on information collected and collated by private companies.[116] 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.[117]

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.[118] 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 routine encounters between law enforcement agents and suspects. Neither of those sets of concerns relate directly to control over personal information.[119]

Not only that, but the threats that police investigations do pose to informational privacy—the compelled disclosures inherent in the search of a home or a computer, say—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, in part because 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."[120] 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 the privacy safeguarded by the Fourth Amendment.[121] 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 on line, and it makes informational privacy even more of a rich person's concern.

For all of these reasons, protecting privacy seems like something of diversion to many scholars of criminal procedure. The police are an increasingly marginal part of the overall threat to privacy, and privacy is tangential to the most important threats the police do pose. 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

---

[116] *See, e.g.*, Angwin & Valentino-Devries, *supra* note 86, at [*]; Galison & Minow, *supra* note 40, at 265; Ohm, *supra* note 24, at 1311, 1321; Winston, *supra* note 86, at A8.
[117] *See* William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016 (1995).
[118] Rubenfeld, *supra* note 6, at 118.
[119] *Id.* at 1021-22.
[120] William J. Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 GEO. WASH. L. REV. 1265, 1289 (1999).
[121] *See id.*

law—called "privacy-as-secrecy."[122] Stuntz was careful to point out that "[t]here is another kind of privacy protected in criminal procedure law," focused on "preventing invasions of dignitary interests, as when a police officer publicly accosts someone and treats him as a suspect."[123] 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."[124] But "[t]his other 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."[125] 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.[126] At least at first blush, there is a good deal less reason to expect a unitary of 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 increasingly difficult to defend. All of which raises the question whether privacy *should* mean informational privacy, and if not what it should mean instead.

---

[122] Stuntz, *supra* note 117, at 1021-22.
[123] *Id.* at 1021.
[124] *Id.*
[125] *Id.* at 1021-22.
[126] *See, e.g.*, AKHIL REED AMAR, THE CONSTITUTION AND CRIMINAL PROCEDURE: FIRST PRINCIPLES [*] (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).

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 useful 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 scholars of criminal procedure, 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.[127] 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.[128] For critics of these decisions, including some members of the Court, and even for 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.[129] 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.[130]

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."[131] The "sphere" of privacy described by James Fitzjames Stephen, for example, was the sphere "within which law and public opinion re intruders likely to do more harm than good," a sphere the included "the internal affairs of a family" and "the relations of love or

---

[127] *See supra* notes 34-35 and accompanying text.

[128] *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).

[129] *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).

[130] *See, e.g.*, Henkin, *supra* note 129, 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 Amendment: Privacy and the Police Use of Spies, Secret Agents, and Informers*, 1976 AM. BAR FOUND. RES. J. 1193, 1206.

[131] INNESS, *supra* note 35, at 64.

friendship."[132] 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.[133] Alan Westin's suggestion, that privacy had to do with controlling the circulation of personal information, fit the bill.[134] 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 should receive official recognition by the state. Debates over same-sex marriage has been debates about equality, not privacy.[135]

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.[136] 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.[137] 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 polarizations, that Critical Legal Studies often took as its primary target.[138] 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.

---

[132] STEPHEN, *supra* note 60, at 107-08.

[133] *See, e.g.* Sundby, *supra* note 24, 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, for example, INNESS, *supra* note 35, at 23, 56-73.

[134] *See, e.g.*, Stone, *supra* note 130, at 1207 n.49. The idea that privacy consisted in control over personal information did not originate with Westin, but it became closely identified with him. *See supra* notes 69-75 and accompanying text.

[135] *See, e.g.*, United States v. Windsor, No. 12-307 (U.S. Mar. 27, 2013).

[136] *See*, *e.g.*, DEBORAH COHEN, FAMILY SECRETS: SHAME AND PRIVACY IN MODERN BRITAIN 244-46 (2013); SUK, *supra* note 23, at 4-8, 125-27.

[137] *See, e.g.*, Frank Michaelman, *Law's Republic*, 97 YALE L.J. 1493, 1533-36 (1988).

[138] *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").

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, the branch of applied mathematics based on the idea that information can be quantified as the opposite of randomness, 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, and then became a kind of conceptual touchstone for academics of all stripes, much as Newtonian physics and Darwinian evolution had done earlier.[139] 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.[140] 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 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."[141] It is axiomatic in all of these discourses that people under surveillance become more guarded about what they say and do, less trustful and playful, more fearful and conformist.[142] Vance Packard warned in 1964 that surveillance "breeds not only sameness but a watchfulness completely untypical of the

---

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

[140] *See id.*

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

[142] *See, e.g.*, ANDREWS, *supra* note 92, at 55-57; Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083, 1102-04 (2002);

exuberant, free-wheeling American so commonly accepted as typical of this land in earlier decades."[143] 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."[144] By 1971, though, Justice Harlan thought "authority [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."[145] He warned that informants carrying hidden microphones could "smother that spontaneity—reflected in frivolous, impetuous, sacrilegious, and defiant discourse—that liberates daily life."[146] Justice Harlan's opinion was widely quoted, invariably with approval,[147] 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 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 development and maintain a particular style of life fade."[148] On this side of the Atlantic, the Daniel Solove notes that surveillance "can lead to self-censorship"[149] and "can inhibit such lawful activities as free speech, free association and other First Amendment rights essential for a democracy."[150] Charles Fried warned as early as 1968 that monitoring makes intimacy impossible and "undermines the subject's capacity to enter into relations of trust,"[151] 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

---

[143] PACKARD, *supra* note 26, at 9-10.
[144] Note, *Anthropotelemetry: Dr. Schwitgebel's Machine*, 80 HARV. L. REV. 403, 408-09 (1966).
[145] United States v. White, 401 U.S. 745, 787 (1971) (Harlan, J., dissenting).
[146] *Id.*
[147] *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 6, at 133-34 (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").
[148] Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707 (1987).
[149] SOLOVE, *supra* note 40, at 108; *see also id.* at 112 (describing the "chilling effects" of surveillance).
[150] DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 27 (2011); *see also* Solove, *supra* note 142, at 1102 (noting that surveillance can "severely constrain democracy and individual self-determination").
[151] Fried, *supra* note 27, at 490.

society celebrates . . . the space people need to deliberate, to try out new ways of acting or different ways of speaking."[152] The 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,"[153] because without informational privacy "we may all be more cautious"; monitoring pushes people's choices toward "the bland and the mainstream"[154] and "chills experimentation with the unorthodox, the unpopular, and the merely unfinished."[155] 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?"[156] Schwartz warns that "[a]s 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."[157] 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."[158] He explains that "[p]eople who know they are under government surveillance will act less spontaneously, more deliberately, less individualistically, and more conventionally."[159] David Gray and Danielle Citron similarly note that monitoring "nudges people toward the benign, mainstream, and institutionally accepted."[160] "Under persistent surveillance," they explain, "people curtail their movements, speech, and engagement with religious, political, and ethnic groups."[161] 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."[162]

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

---

[152] Galison & Minow, *supra* note 40, at 268, 286.
[153] COHEN, supra note 92, at 140, 143, 149.
[154] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000).
[155] *Id.*
[156] Schwartz, *supra* note 28, at 1651-53.
[157] *Id.* at 1656-57.
[158] SLOBOGIN, *supra* note 89, at 92.
[159] *Id.* at 97.
[160] Gray & Citron, *supra* note 76, at [*].
[161] *Id.*
[162] Richards, *supra* note 28, at [*].

consciously or unconsciously on Jeremy Bentham's Panopticon.[163] Nonetheless, as Neil Richards notes, claims about the chilling effects of surveillance ultimately are "empirical."[164] And it is astonishing 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." Two of these—"cultural and literary works" like *Nineteen Eighty-Four* and assertions made by the Supreme Court in First Amendment decisions—amount to different species of turtle. Richards also claims, though, that the stultification thesis is supported by a third set of arguments, "com[ing] from the empirical work of scholars working in the interdisciplinary field of surveillance studies."[165] Alas, 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—is experience in communist states during the Cold War.[168] We have vivid accounts of the way that fear of the state suffused daily life in the Soviet Bloc, and many these accounts suggest that the "assumption of being under surveillance . . . kept people on their guard," fostering a kind of

---

[163] *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 92, 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"); Maria Los, *The Technologies of Total Domination*, 2 SURVEILLANCE & SOC'Y 15, 15-18 (2004). For Foucault's influence on legal scholars studying surveillance, see, for example, SOLOVE, *supra* note 40, at 109; Capers, *supra* note 103, at [*].

[164] Richards, *supra* note 28, at [*].

[165] *Id.* at [*].

[166] *Id.* at [*] (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* Mitrou, *supra* note 166, at 138.

[168] 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 130, at 1195 n.3, 133 n.142.

"self-policing."[169] It is difficult in retrospect, though, to determine how much of the blame for this should be placed with surveillance practices, because the communist states of Eastern Europe, like their fictional counterparts in *Nineteen Eight-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, 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.[170] Secret agents and informants do not just collect information; they do so in a way that dramatically breaches trust and intrudes into intimate confidences.[171] 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 there little empirical support for the stultification thesis, there is a good deal of suggestive evidence throwing it into doubt. 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.[172] "Our growing collective compulsion to document our lives and share them online"[173] strikes many people (particularly if they grew up without the internet) as both reckless and solipsistic.[174] Moreover, there are frequent suggestions that young people do not understand and appreciate the risks they run by posting material about themselves online.[175] That is doubtless true: they are young. And there are reasons to be skeptical of the extravagant claims often made about how social media can improve our lives.[176] Nevertheless, the porous nature of social media and the susceptibility of internet communications to uninvited monitoring are not exactly secrets, even among the young: they "aren't oblivious

---

[169] Maria Los, *Post-Communist Fear of Crime and the Commercialization of Security*, 6 THEORETICAL CRIMINOLOGY 165, 169 (2002); *see also, e.g.*, [*].

[170] *See, e.g.*, Los, *supra* note 169, at 169. 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 (1994 ed.).

[171] *See, e.g.,* ALEXANDRA NATAPOFF, SNITCHING: CRIMINAL INFORMANTS AND THE EROSION OF AMERICAN JUSTICE 116-18 (2009).

[172] *See, e.g.*, CHESTERMAN, *supra* note 79, at 9, 246; JOHN PALFREY & URS GLASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES (paperback ed. 2008).

[173] Jenna Wortham, *Facebook Made Me Do It*, N.Y. TIMES, June 15, 2013, at [*].

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

[175] *See, e.g.*, ANDREWS, *supra* note 92, at 21; PALFREY & GLASSER, *supra* note 172, at 24, 54, 75.

[176] *See, e.g.*, EVGENY MOROZOV, THE NET DELUSION: THE DARK SIDE OF INTERNET FREEDOM (2011).

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 of extensive NSA snooping in 2013 generated a "collective national shrug."[178] And there are precious few signs that lack of confidentiality has 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] but reasons to doubt the stultification thesis are not limited to the young. 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 recordkeeping or intra-governmental communication.[182] That will come as little surprise to anyone who uses e-mail on a workplace network subject to employer monitoring: evidence of self-censorship on such networks is difficult to find.[183] People quickly become accustomed to monitoring and then ignore it. Something similar happens when criminal suspects are recorded, either openly or covertly. 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.[184] And despite Justice Harlan's warning that warrantless, surreptitious recording of conversations by confidential informants "might well smother [the] spontaneity . . . that liberates daily life,"[185] we have now lived with that practice for four decades, and it has had 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, and there are, of course, reasons to worry about the government accumulating too much power and reasons to scrutinize how the government uses the powers it is allowed to amass.[186] Furthermore there some techniques of surveillance—in particular, the widespread use of secret agents

---

[177] PALFREY & GLASSER, *supra* note 172, at 51.
[178] Nagourney, *supra* note 99, at A12.
[179] PALFREY & GLASSER, *supra* note 172.
[180] *See, e.g.*, *id.* 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* NATIONAL ARCHIVES OF CANADA, THE ACCESS TO INFORMATION ACT AND RECORD-KEEPING IN THE FEDERAL GOVERNMENT (2001).
[183] *See* ALASDAIR ROBERTS, BLACKED OUT: GOVERNMENT SECRECY IN THE INFORMATION AGE 215-16 (2006).
[184] *See, e.g.*, David A. Sklansky, *Quasi-Affirmative Rights in Constitutional Criminal Procedure*, 88 VA. L. REV. 1229, 1263-64 & nn.110-111 (2002).
[185] United States v. White, 401 U.S. 745, 787 (1971) (Harlan, J., dissenting).
[186] Points that Neil Richards, among others, has usefully elaborated. Richards, *supra* note 28, at [*]; *see also, e.g.*, James B. Rule, *The Whole World is Watching*, 22 DEMOCRACY 58 (2011).

and undercover informants—can generate paralyzing fear and distrust, if not in isolation than at least when combined with the kinds of authoritarian practices that surveillance can help to make possible. What deserves questioning, though, is the common suggestion that surveillance, simply by 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 (although that is possible), but because it has helped to reinforce the idea that the privacy worth protecting is all about controlling information.

A further 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. For one thing, 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.[187] When we reach a point at which 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 a large part of what makes it worth worrying about. Surveillance is troubling in part because of the power relationships it creates, and in part—possibly—because of the ways in which certain forms of surveillance can violate dimensions of privacy that have to do with things other than data.

B. *What Informational Privacy Misses*

An information-based conception of privacy has genuine attractions. It engages privacy with dramatic and far-reaching changes 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, that privacy was linked in some way 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.

---

[187] *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 Desai, Data Hoarding: Privacy in the Age of Artificial Intelligence (unpublished manuscript, 2013).

There also are more basic problems with defining privacy as control over information: problems so obvious they help to explain why even scholars like Daniel Solove, who think about privacy largely in terms of data flows, resist claiming that that privacy can be reduced to informational privacy.[188] 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.[189] 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.[190] 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.[191] 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.

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 in a sense a paradigmatic violation of privacy, or at least they were, when intrusions into privacy were regularly analogized to forced disrobements.[192] Not surprisingly then, there has long been a sense that strip searches are particularly invasive and require particularly strong justification.[193] That sense lingers today, but the focus on

---

[188] *See, e.g.*, SOLOVE, *supra* note 40, at 21-29.

[189] *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.*

[190] *See id.* at 2090-91; *cf., e.g.*, SOLOVE, *supra* note 40, at 28 (arguing that "[e]ven if the conception [of privacy] is narrowed to include only intimate information, it is still too broad").

[191] *See* INNESS, *supra* note 35, at 56-69; *cf., e.g.*, SOLOVE, *supra* note 40, at 29 (concluding that "conceptions of [privacy as information control] are too narrow," in part "because they reduce tprivacy to informational concerns").

[192] *See supra* notes 60-63 and accompanying text.

[193] *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,"

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 cases in point: 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,[194] but six federal judges had concluded otherwise,[195] and the Court itself thought that the ultimate result was sufficiently unpredictable that school officials should be immune from liability.[196] Justice Thomas, along with three judges of the Ninth Circuit, did not believe that the search of Savana Redding—which involved having her unclothe 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[197], *id.* at 369, 374—should even be described as a "strip search"; they would have reserved that term for a search involving "full" disrobing.[198] Three years after deciding *Redding*, the Court took up the case of an African-American man named Albert Florence. Florence had been strip searched when he was jailed following his arrest on a withdrawn bench warrant; he argued the search was unconstitutional because he had been arrested for a minor offense and there no grounds to suspect that he was concealing contraband.[199] Florence lost: the Supreme Court ruled that the jail could strip search all new prisoners, because that policy "struck a reasonable balance between inmate privacy and the needs of the institution,"[200] at least with respect to prisoners admitted to the general jail population.[201] Again, there was uncertainty even about whether to call what had happened a "strip search." Justice Kennedy's majority opinion called that term "imprecise" and noted that searches in this case were not alleged to have involved "any touching of unclothed areas by the inspecting officer."[202] The Court split 5-4, and there was a sharp dissent,[203] 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

---

and that outside prisons and jails such "deeply intrusive searches" could be justified, if at all, "only to prevent imminent, and serious harm").

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

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

[196] *See* 557 U.S. at 377-79.

[197] *See id.* at 369, 374.

[198] *Id.* at 387 n.1 (Thomas, J., dissenting).

[199] *Florence v. Board of Chosen Freeholders*, 132 S. Ct. 1510 (2012). Florence had been strip searched again six days later, when he was transferred to a different jail. He alleged that on both occasions he been forced to lift his genitals for visual inspection. *See id.* at 1514-15. N

[200] *Id.* at 1523.

[201] 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 (opinion of Kennedy, J.); *see also id.* at 1523 (Roberts, C.J., concurring); *id.* at 1524 (Alito, J., concurring).

[202] *Id.* at 1515 (opinion of Kennedy, J.).

[203] *See id.* at 1525 (Breyer, J., dissenting).

an avalanche of commentary, but Florence's case was largely ignored, both by scholars and by the press.[204]

Some of that neglect may be explained by the fact that Florence was searched when he was jailed. There are lots of special rules for jails and prisons, and judges, scholars, and members of the public generally do not think about those rules as rules that 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 FBI agents and local police officers—lay close to the heart of the practices that have come to be understood as the main threat to privacy today, the aggregation and analysis of data about where people go, who they talk with, what they purchase, and how they live their 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 offending the sensitivities of the person being searched,[205] whereas the surveillance in *Jones* implicated the very "relationship between citizen and government" in a "democratic society."[206]

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 (and, for that matter, school discipline) in the United States. If the ultimate fear is O'Brien's vision of "a boot stepping on a human face . . . forever,"[207] 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"[208]; the way they can cultivate a

---

[204] *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").

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

[206] 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)).

[207] GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949).

[208] 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").

politically enervating sense of "humiliation and helplessness"[209]; 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, in aggressive employment of stop-and-frisk tactics by the police, or in traffic stops and vehicle searches that uncover nothing of interest.[210]

A non-informational theory of privacy is not the only way to 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.[211] It is commonly employed, as well, to describe the non-informational infringements associated with investigatory stops.[212] 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[213]; 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"[214] or "security."[215] Violations of privacy can plainly undermine trust, and certain forms of privacy may even be a "necessary context" for trust.[216] 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 Fourth Amendment should be read to promise the security of "personal life"—i.e., of "all those domains of interaction in which people are

---

[209] Ha, *supra* note 208, at 2740.

[210] *See* Janice Nadler, *Consent, Dignity, and the Failure of Scattershot Policing*, *in* THE CONSTITUTION AND THE FUTURE OF CRIMINAL JUSTICE IN AMERICA [*], [*] (L. Song Richardson & John T. Parry eds., forthcoming 2013).

[211] *See, e.g.*, *Florence*, 132 S. Ct. at 1527 (Breyer, J., dissenting); Ha, *supra* note 208, at 2740.

[212] *See, e.g.*, Nadler, *supra* note 210; Stuntz, *supra* note 120, at 1273.

[213] *See, e.g.*, Bloustein, *supra* note 63; Gavison, *supra* note 35, at 455; Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 1008 (1989); Post, *supra* note 113, at 2092-94; *cf.* Whitman, *supra* note 37, at 1161 (arguing that "[c]ontinental privacy protections are, at their core, a form of protection of a right to *respect* and *personal dignity*").

[214] Sundby, *supra* note 24.

[215] Clancy, *supra* note 25; Rubenfeld, *supra* note 6, at 104.

[216] Fried, *supra* note 27, at 478.

outside the public sphere."[217] 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.

III. RECONSTRUCTING PRIVACY

If defining privacy as control over data flows seems too reductive (as well as too broad[218]), 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 trying to incorporate in a reconstructed conception of privacy, elements having to with the nature and purpose of privacy rather than the content of privacy.[219] 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"[220]; and I will suggest that privacy violations are harmful not solely, or perhaps even primarily, 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 incorporating 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"[221]—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.[222] That is why even David Brin, the influential enthusiast for

---

[217] Rubenfeld, *supra* note 6, at 128, 133.
[218] *See supra* text accompanying notes 189-190.
[219] Regarding these distinctions, *see* INNESS, supra note 35.
[220] Post, *supra* note 213, at 1008-09, *see also id.* at 959; Post, *supra* note 113, at 2092-94.
[221] *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'd*, 353 U.S. 391 (1957)).
[222] *See, e.g.*, Galison & Minow, *supra* note 40, at [*].

a "transparent society," warns that we will always need "some zone of sanctuary where can feel unobserved . . . [s]ome corner where our hearts can remain forever just our own."[223] He was echoing the thoughts and cadences of Judge Jerome Frank, who wrote, in language later adopted by the Supreme Court 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. . . ."[224] The private sphere is valued for reasons both psychological and political. 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"[225]—and with the necessary conditions for intimacy. The political significance of the private sphere is connected with 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 system of social organization defined in large part precisely by the elimination of the private sphere.[226]

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.[227] The home is what Judge Frank had in mind when he wrote about an "oasis" and "shelter from public scrutiny"[228] (although not when he wrote later about the need for a "private enclave" where an individual "may lead a private life"[229]), and it is what Brin has in mind when he ties his "zone of sanctuary" (which he calls "bedroom privacy") to the home and its curtilage.[230] 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 the woods to be alone, but most of us, most of the time, go home. If there is to be a place of repose, a place where we are allowed to alone with or 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

---

[223] BRIN, *supra* note 105, at 269-70; *see supra* text accompanying notes 105-110.

[224] 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)).

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

[226] *See, e.g.*, Grunewald, 233 F.2d at 582 (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'").

[227] *See, e.g.*, SUK, *supra* note 23, 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).

[228] *On Lee*, 193 F.2d at 315-16 (Frank, J., dissenting). 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).

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

[230] *See* BRIN, *supra* note 105, at 269-70.

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."[231] Obviously 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.[232] 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,[233] 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. It has never been the law, and could never be the law, that searches of homes or of bodies are categorically forbidden. Wherever it is located, the private sphere cannot be a zone where the law can never reach, 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,"[234] and subsequent decisions linking privacy protections to the home have been criticized as inconsistent with that promise—a "return to the pre-*Katz* world."[235] The boundaries of a "zone of sanctuary" will inevitably seem arbitrary, at least at times, and its very existence will make infringements on 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 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 closing decades of the twentieth century was not that the boundaries of the private seemed

---

[231] Gerety, *supra* note 73, at 266.
[232] [*]
[233] *See* McClain, *supra* note 227.
[234] 389 U.S. 347, 351 (1967).
[235] David Cole, *Scalia's Kind of Privacy*, NATION, July 23, 2001, at 6 (discussing Kyllo v. United States, 533 U.S. 27 (2001)).

arbitrary, or that dividing the world into public and private 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.[236] Because the protection provided by the private sphere 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.[237] Those decisions will help determine both the value of the sphere of its privacy and its costs.

B. *Privacy and Civility*

Robert 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."[238] 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[239]—and one reason the Court has been right to ignore that principle when it protects, for example, the privacy of a telephone call.[240] 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."[241]

The relational nature of privacy also suggests that infringements on 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.[242] That leaves the effects of privacy violations on the violators—both individuals and the organizations for which they work—out of the picture. And 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.[243]

---

[236] *See, e.g.*, SUK, *supra* note 23, at 4-8, 125-27.
[237] *See* Georgia v. Randoph, 547 U.S. 103 (2006) (answering no, absent an imminent danger of domestic violence or other extenuating circumstances).
[238] Post, *supra* note 113, at 2092; *see also* Post, *supra* note 213, at 1008-09.
[239] *See, e.g.,* United States v. Smith, 442 U.S. 735, 743-44 (1979); United States v. Miller, 425 U.S. 435 (1976).
[240] *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 should be reconsidered).
[241] EUR. CONV. HUM. RTS., art. 8, § 1.
[242] *See, e.g.*, INNESS, *supra* note 35 , at [*].
[243] *See supra* text accompanying notes 165-185.

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 awkwardness"; the "depersonalization" and "dehumanization" that transformed these students into "perpetrators of abuse" was a gradual process.[244] 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." 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.[245] 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],"[246] 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."[247] On the second day of the experiment, when some of the prisoners tore numbers from the front 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."[248] 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 of a mechanism of debasement and status reinforcement.

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."[249] The traumatizing effects of strip searches on inmates—the sense of humiliation, helplessness, and degradation that the practice can cause—is well documented.[250] 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. It is not surprising that the torture of prisoners at Abu Ghraib was accompanied by rampant and intentionally degrading strip searches and by prisoners forced to remain naked while they were interrogated. Nor should it be surprising that military investigators concluded that at least in some cases the "tone and environment"

---

[244] PHILIP ZIMBARDO, THE LUCIFER EFFECT: UNDERSTANDING HOW GOOD PEOPLE TURN EVIL 53-54, 56, 73 (2007).
[245] *Id.* at 40.
[246] *Id.*
[247] *Id.* at 55.
[248] *Id.* at 60.
[249] DOBASH, DOBASH & GUTTERIDGE, *supra* note 208, at 205 (1986).
[250] *See, e.g.*, Ha, *supra* note 208, 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).

surrounding these practices were "the causative factor that set the stage" for worse abuses.[251]

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.[252] 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. 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.

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 Justice Blackmun that this sphere is defined partly by places (especially the home and the body) and partly by activities (especially those that relating to intimacy and self-definition).[253] We can say that privacy is not so much a thing or quantity that someone has, but rather that it resides in the respect shown by others—including officers of the government—for an individual's sphere of personal sovereignty. Violations of that respect matter 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

---

[251] Maj. Gen. George R. Fay, *AR 15-6 Investigation of the Abu Ghraib Detention Facility and 205th Military Intelligence Brigade*, *in* LT. GEN. ANTHONY R. JONES AND MAJ. GEN. GEORGE R. FAY, INVESTIGATION OF INTELLIGENCE ACTIVITIES AT ABU GHRAIB 6, 57 (2004); *see also* AIDAN DELGADO, THE SUTRAS OF ABU GHRAIB 153-54 (2007).

[252] It is noteworthy, though, that Sartre builds his discussion of shame around the example of a person discovered in the act of spying through a keyhole. JEAN-PAUL SARTRE, BEING AND NOTHINGNESS 347-49 (1943) (Hazel E. Barnes trans., 1956).

[253] Bowers v. Hardwick, 478 U.S. 186, 203-07 (1986) (Blackmun, J., dissenting).

habits and ways of thinking for governmental officers and governmental 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 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 should 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, 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 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 "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 with large issues in criminal justice, and not just criminal justice for the rich. Those issues include the harms of mass incarceration and the fairness and effectiveness of street policing. 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.[254] 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.[255] And the brutalization associated with invasions of privacy connect 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 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 centered around respecting zones of personal refuge helps to avoid the problems of circularity the Supreme Court has encountered in linking Fourth Amendment protection to "reasonable expectations of privacy." An infringement does not become "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."[256] 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 a zone 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."[257] The special treatment of the home and

---

[254] [*]
[255] [*]
[256] Post, *supra* note 113, at 2094.
[257] *E.g.*, Florida v. Jardines, 133 S. Ct. 1409, [*](2013) (quoting Silverthorne v. United States, 365 U.S. 505, 511 (1961).

the reduced level of protection elsewhere have often been criticized as old fashioned, formalistic, and class-biased,[258] 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,[259] but because the home is the paradigmatic place of "retreat." Invasions 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 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 great 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 instrumentally—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*,[260] for example, the Supreme Court confronted the following question: if one resident 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."[261] 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."[262] 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.[263] 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

---

[258] [*]

[259] *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*").

[260] 547 U.S. 103 (2006).

[261] *Id.* at 122-23.

[262] *Id.* at 111, 113.

[263] *Id.* at 127 (Roberts, C.J., dissenting). On the rhetorical uses of social conventions in *Randolph*, see SUK, *supra* 23, at [*].

that information or those papers *or places* with the government."[264] 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, it whether making cohabitants assume this particular risk raised an undue threat to 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. 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 is not especially violative if the guards do not touch him?[265] Has a thirteen-year-old girl undergone a "strip search" if she is allowed is to keep her undergarments on and merely pull them away from her body?[266] 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.

That means that courts have been right to treat strip searches as particularly serious and particularly worrisome infringements of privacy. It also means there 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 searchers and their employers to depersonalize and dehumanize the individuals in their charge.

3. *Investigatory stops and frisks*. Conceiving privacy as protecting a sphere of personal sovereignty—non-absolute but nonetheless vital—suggests that investigatory

[264] 547 U.S. at 128 (Roberts, C.J., dissenting).
[265] *See supra* note 202 and accompanying text.
[266] *See supra* note 198 and accompanying text.

stops and frisks should be understand 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.[267]) Thinking about stops and frisks in this way may help us to remember what the Supreme Court itself stressed when it approved the stop-and-frisk tactic but only based on specific, articulable suspicion: that the tactic is not a "petty indignity" but "a serious intrusion upon the sanctity of the person."[268] 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.

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.[269] 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 were the spies he unknowingly made 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, at least in the United States.[270] 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.

---

[267] *See supra* note 202 and accompanying text.

[268] *Terry v. Ohio*, 392 U.S. 1, 17 (1968).

[269] For a thoughtful discussion, see NATAPOFF, *supra* note 171 , at 116-19; *see also supra* note 170 and accompanying text. Natapoff points out that these may be particularly acute in poor, inner-city communities "because social networks are more disorganized and people's lives and spaces are less private." NATAPOFF, *supra* note 171 , at 117.

[270] *See, e.g.*, NATAPOFF, *supra* note 171, 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).

5. *Electronic surveillance.* The prevailing, information-centered conception of privacy is widely thought to particularly well-suited for addressing the geometrically proliferating ways in which our movements, transactions, and conversations are subject to electronic monitoring; that perception is one of the reasons that 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 separate out the data flows that are 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 that raises the question of what should count as "personal." As I have suggested earlier, that amounts to another way 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 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"[271] as those that "society is prepared to recognize as reasonable."[272] 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.[273] 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."[274]

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

---

[271] Katz v. United States, 389 U.S. 347, 363 (1967) (Harlan, J., concurring).
[272] Oliver v. United States, 466 U.S. 170, 191 (1984).
[273] *See, e.g.,* INNESS, *supra* note 35, at [*].
[274] *Katz*, 389 U.S. at 352 (opinion of the Court).

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,[275] 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 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. Technologies of social interchange today are more varied, and sorting out which venues are "vital" to 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 have suggested earlier—have the potential to turn being passively recorded (on the internet or on the sidewalk) into being actively watched.[276]

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.

---

[275] *See* Ohm, *supra* note 90.

[276] *See supra* note 187 and accompanying text.