Oklahoma Law Review

Volume 66 | Number 4
Symposium: Law Enforcement Access to Third Party Records

2014

Ubiquitous Privacy

Thomas P. Crocker
University of South Carolina School of Law, crocketp@law.sc.edu

UBIQUITOUS PRIVACY

THOMAS P. CROCKER*

Privacy does not name a single value, practice, or principle. It has multiple meanings and appears in different contexts and guises.[1] It depends on background social and political practices and values, varying with time, intensity, salience, and scale, among other conditions.[2] For example, small amounts of information, not salient to important decisions that do not reveal very intense preferences or events in a person's life, and are small in scale within a person's life history, might not be very private, whereas large amounts of information, salient to important personal decisions, revealing deeply important information about a person's identity, could be highly private. The relative weights and measures regarding these factors are a strong, but not determinative, indicator of the degree of privacy to afford information. Measuring privacy, given the array of potential factors, is therefore both contextual and contingent. We can weigh and measure privacy in different manners.[3]

To take one example from Supreme Court jurisprudence, writing for a majority in *Kyllo v. United States*, Justice Scalia concludes that when police use infrared technology to view the relative heat dispersal of the outer walls

---

* Distinguished Professor of Law, University of South Carolina School of Law. For helpful conversations on these issues, I would like to thank Marc Blitz, Josh Eagle, Andrew Ferguson, Susan Freiwald, David Gray, Stephen Henderson, and Christopher Slobogin. Stephen Henderson deserves special thanks for starting and organizing the conversation. I am grateful for the research assistance of Andrew Webb and Adam Mandell.

1. *See, e.g.*, HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 2-3 (2010); Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1099-1124 (2002) [hereinafter Solove, *Conceptualizing Privacy*] (considering privacy as the right to be left alone, to limit access to the self, to secrecy, to control over personal information, to protect dignity and autonomy, and to develop intimacy); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 484-91 (2006); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1153 (2004); Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L. J. 2087, 2087 (2001) (reviewing JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA (2000)) ("Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all.").

2. *See generally* Whitman, *supra* note 1.

3. But these manners are not unrelated. They have conceptual similarities and overlaps. Nonetheless, there are no necessary or sufficient criteria that all examples of privacy share. *See* LUDWIG WITTGENSTEIN, PHILOSOPHICAL INVESTIGATIONS §§ 66-67 (G.E.M. Anscombe trans., 1958); Solove, *Conceptualizing Privacy*, *supra* note 1, at 1096-99.

of a home, they learn too much about the intimate details of the home.[4] By contrast, Justice Stevens, writing in dissent, argues that such "off the wall" surveillance implicates no constitutional privacy interests.[5] Justice Scalia focuses on the intimate household details that the technology might reveal, such as when "the lady of the house takes her daily sauna and bath,"[6] whereas Justice Stevens focuses on what he construes as the superficial information already exposed to the general public.[7] This disagreement is about where the boundaries are drawn between what information the state might acquire and what information persons are entitled to keep to themselves, even if exposed to others for limited purposes and in specific circumstances. This disagreement depends on judgments about the role information plays within a person's life. Control over informational aspects of personal life is part of what it means to have and develop a person's own identity. What many different approaches to the relative weights and measures of privacy have in common is that privacy is understood to implicate the conditions for realizing personal identity. Privacy is a matter of establishing the boundaries between self and other. These boundaries become especially significant when the other is an official of the state.

By analyzing privacy as a value disconnected from the persons in whom it inheres, it is often easier to tradeoff other, equally abstracted values, such as security. Questions about how to conceptualize, and thus whether to protect, privacy in the information persons share with third parties produce different answers if approached from the perspective of personal identity, rather than from the perspective of law enforcement practice. At the very least, such a perspective will require more attention to the practical implications of police action than will conclusory Supreme Court assertions that a holding considering only the interests of police provides "ample protection for the privacy rights that the [Fourth] Amendment protects."[8] Because the conditions in which persons develop and sustain their identities are diverse and polymorphic, so too will be the occasions and practices in which privacy is a value. As a consequence, legal conclusions about privacy both arise out of, and give shape to, social practices.

As a conceptual matter, before determining the degree of protection to afford privacy, a decision maker may first have to classify the effects of law enforcement's access to particular kinds of information. By first deciding

4. Kyllo v. United States, 533 U.S. 27, 38-40 (2001).
5. *Id.* at 41 (Stevens, J., dissenting).
6. *Id.* at 38.
7. *Id.* at 43-44 (Stevens, J., dissenting).
8. Kentucky v. King, 131 S. Ct. 1849, 1862 (2011).

the level of privacy that particular kinds of information warrant, a decision maker can then determine how much procedure to impose on law enforcement officials seeking access. Categorizing internet search histories or a person's public movements, for example, as private to a high or minimal degree will guide further decisions about how much constraint to place on law enforcement's ability to access such information. One such example, provided by the 2013 ABA Standards for Law Enforcement Access to Third Party Records (LEATPR Standards), is to offer a sliding scale ranging from highly private information to moderate, minimal, or non-private information.[9] Focusing on the nature of the information and its use, the ABA Standards ask the following: whether sharing is necessary to meaningful participation in modern society, whether information is personal and intimate, whether information is ordinarily accessible to parties other than those with whom a person has shared, and whether existing law establishes baseline rules about access to shared information.[10] Questions about which information is private and what level of protection is appropriate require interpretive decisions open to debate and disagreement. But the need to make a decision is unavoidable.

To forego adopting an explicit framework to determine the procedures by which law enforcement may gain access to third party records is to make a decision about law enforcement access. Default rules and practices will otherwise govern and guide policing practice. Moreover, in deciding on privacy, classifications will influence social and political practices, which in turn will inform how classificatory schema are implemented. The current legal approach, in the absence of comprehensive guidance, provides fragmentary regulation, leaving many kinds of data uncovered.[11] As a result, individuals often have the burden of maintaining their own privacy by withholding information or foregoing transactions that are otherwise conditions of everyday life. In this way, privacy receives protection through a form of withholding or nondisclosure—a retreat to the self-contained

9. The Standards choose a four-category classification, sliding from highly private information to moderately, minimally, or non-private information. *See* ABA STANDARDS FOR CRIMINAL JUSTICE: LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS 25-4.1 (2013) [hereinafter LEATPR STANDARDS]. Individual standards will be referred to using the format 'Standard x-x.'

10. STANDARD 25-4.1(a)-(d).

11. *See, e.g.*, 12 U.S.C. § 3402 (2012) (financial records); 42 U.S.C. § 290dd-2 (2012) (health records). *See generally* Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485 (2013) (analyzing the interaction between statutory protections and the Fourth Amendment).

aspects of personal identity. But is nondisclosure really the privacy of personal identity?

We give the name "privacy" to an overlapping set of practices and concerns that shape the conditions in which we realize our personal identities. These practices are social. They are shared with others in all the familiar as well as more distant relations persons maintain as conditions of a complete life. In this way, persons share information with others widely and to varying degrees. But they also maintain a claim of privacy regarding much of this information and many of these associations, despite the limited disclosures they make. In this way, privacy is not about being alone, but about the conditions under which persons relate to others.

Because law is not neutral regarding the shape these practices and relations among persons and their information take, this article focuses on three overlapping considerations. Part I addresses the question of how to weigh and measure the relative degree of privacy maintained in particular kinds of information. A default position is to think that information held more closely to the chest is the paradigm of privacy, while what is more loosely guarded is public and fair game. Such a view is consistent with the surveillance practices of repressive regimes and cautions reconsideration of how decision makers weigh and measure more shallow forms of personal information. Part II considers how the ubiquity of third party information entails a similar ubiquity of privacy. If, as a condition for leading a complete life, persons share information for limited purposes in diverse contexts, then privacy's location in legal and conceptual space depends on choices decision makers must make. Treating third party information as highly or minimally private does not follow deductively from the nature of the information itself, separated from the practices in which it functions. In choosing whether and how to protect diverse instantiations of privacy, it is important to consider the constitutional meanings and related values of association and speech. Part III explores the constitutional and conceptual aspects of privacy, concluding that law enforcement access to third party records should be constrained by a higher showing of relevance and need the more such access impacts core values of association, expression, and personal identity. The mere fact of widespread social sharing does not entail a conclusion that cyberspaces are no different than public streetscapes.

I. Privacy's Weights and Measures

Václav Havel, former Czech Republic President and playwright, described how in pre-1989 Czechoslovakia in the face of pervasive surveillance, "[i]ndependent thinking and creation retreated to the trenches

of deep privacy."[12] By referring to the trenches of "deep privacy," Havel suggested that there is a quality of privacy to which the individual under surveillance, chilled from creative and associational activities, might retreat.[13] The question is whether "in a world of ubiquitous third party information,"[14] as the LEATPR Standards identify the present state of affairs, deep privacy provides a safe retreat. A common view, adopted by courts and scholars, is that privacy is defined by what is withheld from others—what is kept secret is often something deeply private.[15] What is revealed to others is something made public and therefore to be contrasted with what is private.[16] Thus, on the view adopted in Supreme Court opinions, deep privacy is a primary form of constitutionally protected privacy. For, as the Court has made clear, a person assumes the risk that in sharing information with a third party, law enforcement may thereby become the unexpected recipients.[17] Havel's understanding of "deep privacy" as a retreat from ordinary forms of expressive human interaction within a polity, however, suggests that such a form of privacy is inadequate to protect human freedom.[18] Reliance on deep privacy to protect independent thinking from the potential for pervasive government interference and intrusion on citizens' liberties through constant

12. VÁCLAV HAVEL, DISTURBING THE PEACE 120 (Paul Wilson trans., 1991).

13. *Id.*

14. STANDARD 25-3.1 commentary.

15. *See, e.g.*, Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 393 (1978) ("[O]ne aspect of privacy is the withholding or concealment of information."); William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1025 (1995) ("[O]ne fairly well-defined and fairly narrow interest, the interest in secrecy, seems predominant.").

16. *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 213-14 (1986) (commenting on the public nature of contraband in a fenced yard, the Court noted that "[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed").

17. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 744 (1979) ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed."); United States v. Miller, 425 U.S. 435, 443 (1976) ("[A person] takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.").

18. Havel suggests that the political state triggering a retreat into "deep privacy" was "an attack by the totalitarian system on life itself, on the very essence of human freedom and integrity." HAVEL, *supra* note 12, at 128.

surveillance is a deficient mode of privacy protection. The problem with this retreat is that deep privacy is not associational, interactive, open, or interpersonal. It does not rely on the reciprocal interaction of self-disclosure essential to realizing personal identity.[19] Since it is not part of any shared discourse, what is retained as deep privacy may not even count as information. Deep privacy supports neither the associational activities necessary to developing one's distinct personal identity, nor the interactions thought necessary for engaged citizenship.[20]

Deep privacy reveals who a person may be when left alone with her thoughts, but personal knowledge and identity also require a form of what can be called "shallow privacy" to give experience and understanding to a person's deep privacy. Shallow privacy can include information that could be classified as both highly private and minimally private, or even non-private, because shallow privacy is less about the nature of the information than it is about the relation of information to a person's core identity. Medical records about a person's severe contusion suffered while snowboarding may be classified as highly private, but may also be relatively shallow in what they reveal about a person's core self-identity. Third parties discovering that a person suffered a snowboarding injury may not learn anything a person would not readily reveal herself. Minimally private categories of information, say a person's present or historical movements on city streets, might nonetheless be highly private. A person

19. It is beyond the scope of this essay to enter into philosophical debate about the necessary conditions for the possibility of personal identity and development. On the degree to which questions of justice, for example, depend on individuals understood in relative isolation or in community, one can see the debate between JOHN RAWLS, A THEORY OF JUSTICE (1971) and MICHAEL J. SANDEL, LIBERALISM AND THE LIMITS OF JUSTICE (1982). But, perhaps this much can be asserted here: a central feature of privacy is the fact of a person's relations to others. The boundaries of that relation are, in turn, essential to forming and sustaining a person's identity within society. *See also infra* note 24 and accompanying text.

20. *See* CASS R. SUNSTEIN, DEMOCRACY AND THE PROBLEM OF FREE SPEECH 244 (1995) ("[W]e might hope that a well-functioning system of free expression will ultimately encourage a degree of public virtue and produce high levels of participation and genuine deliberation."); ALAN F. WESTIN, PRIVACY AND FREEDOM 39 (1967) (suggesting that privacy "is basically an instrument for achieving individual goals of self-realization"); *see also* Bruce Ackerman, *Reviving Democratic Citizenship*, 41 POL. & SOC'Y 309, 310 (2013) (outlining a participatory and deliberative "citizenship agenda"); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 455 (1980); ("Privacy . . . encourages the moral autonomy of the citizen, a central requirement of a democracy."); Martin H. Redish, *The Value of Free Speech*, 130 U. PA. L. REV. 591, 603-04 (1982) (promoting the democratic value of individual self-realization).

attending a job interview about which a current employer is unaware might hold this information to be highly private—not data for public knowledge. Such information may be central to a person's present identity—revealing ambitions and dissatisfactions not apparent to other third party sources, though perhaps known to intimates. In this way, information about a person's more shallow forms of privacy can tell us something about the deeper recesses of his ambitions and desires.

The contingent and contextual depth of specific information and the weight a person might attach to it, makes regulating based on classifications more difficult. It may be that no classificatory framework will completely fit actual practices and will thus both over- and underprotect information. Overprotection occurs when policies grant a high degree of protection to information persons may not think very private, while underprotection occurs when those same policies fail to protect other information a person might hold dear. From the perspective of privacy, any classificatory scheme is likely to be incomplete, given the complexity and contingency of private information. Law enforcement will agree with this claim of imperfect fit, though for different reasons. From the perspective of law enforcement, the worry is not whether information vital to the realization of personal identity is revealed, but whether information thought necessary to effective crime investigation and prevention will be more difficult to obtain.[21] Thus, pressures on classifications exist from both sides. Individuals objecting to law enforcement snooping and police seeking technologically enhanced access to information may both find reason to pressure decision makers.

Because the relationship between shallow and deep privacy is important to the development and maintenance of personal identity, imperfections in the weights and measures of privacy can have effects on other constitutional values. For example, constructive access to third party records allows law enforcement officials to interfere with the relation between shallow and deep privacy in a way that can be iniquitous to self-realization, a value often praised and protected under the First Amendment.[22] By subjecting people to "too permeating police

21. *See, e.g.*, STANDARD 25-4.2 (giving legislatures the option of reducing protections on certain types of information if "the limitation imposed [by the Standards] would render law enforcement unable to solve or prevent an unacceptable amount of otherwise solvable or preventable crime").

22. *See, e.g.*, United States v. White, 401 U.S. 745, 763 (1971) (Douglas, J., dissenting) ("The individual must keep some facts concerning his thoughts within a small zone of people. At the same time he must be free to pour out his woes or inspirations or dreams to

surveillance"[23] of their shallow privacy, the interactions that make realization of deep privacy possible may be suppressed or even foreclosed, rendering vulnerable the processes of deep identity formation and maintenance. Persons must have interactions of shallow privacy in order to form the core of deep privacy.[24] Knowing that one's social media interactions may be subject to indiscriminate police surveillance may alter a person's decisions about what to share.[25] At the moment a person self-censors because of a risk that a zealous police officer might misconstrue what she says or view what is intended only for friends, then a permeating surveillance has chilled First Amendment protected activity.[26] In this way, regulation of police access to third party records implicates constitutional values of both privacy and association. And, in each case, protecting privacy requires classifying information with attention to how it is used and how it relates to other practices.

To be fair, there are many reasons a person might choose to edit and alter what she says to different audiences. We all self-censor. We present ourselves in varying ways in light of differential social circumstances and our roles within them.[27] Advocates for greater law-enforcement access to

---

others. . . . This is the essence of the idea of privacy implicit in the First and . . . Fourth [Amendments]."); *see also* Redish, *supra* note 20, at 604.

23. United States v. Di Re, 332 U.S. 581, 595 (1948).

24. Interactions with and attachments to others play roles in forming a self, as philosophers have argued. *See, e.g.*, ALASDAIR MACINTYRE, AFTER VIRTUE 221 (2d ed. 1984) ("For the story of my life is always embedded in the story of those communities from which I derive my identity."); CHARLES TAYLOR, *Atomism*, *in* PHILOSOPHY AND THE HUMAN SCIENCES: PHILOSOPHICAL PAPERS 2, at 187, 209 (1985) ("[O]ur identity is always partly defined in conversation with others or through the common understanding which underlies the practices of our society."); BERNARD WILLIAMS, MORAL LUCK: PHILOSOPHICAL PAPERS 1973-1980, at 14 (1981) (arguing that the conception of morality "depends on the idea of one person's having a character, in the sense of having projects and categorical desires with which that person is identified"); *see also*, Erving Goffman, *The Nature of Deference and Demeanor*, 58 AM. ANTHROPOLOGIST 473, 493 (1956) ("[T]he individual must rely on others to complete the picture of him of which he himself is allowed to paint only certain parts.").

25. *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 108 (2008) ("Surveillance can lead to self-censorship and inhibition."); Julie E. Cohen, *Examined Lies: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423-28 (2000); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3; Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013).

26. *See* Keyishian v. Bd. of Regents of Univ. of State of N.Y., 385 U.S. 589, 604 (1967) ("[T]he danger of that chilling effect upon the exercise of virtual First Amendment rights must be guarded against . . . ."); Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the "Chilling Effect"*, 58 B.U. L. REV. 685 (1978).

27. *See* ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE 17-76 (1959).

third party information might argue that adding one more factor to our existing reasons for selective self-disclosure may be of minimal consequence. Indeed, when talking about criminal activity, a person always assumes a risk of speaking to a confidential informant.[28] We all assume the risk that when we share information with others they will in turn share our information with law enforcement.[29] But, there is a difference between the self-censorship that is inseparable from social interaction and the state's subtle alteration of the forms of those same interactions.

By intruding upon the forms of shallow privacy, state officials can thereby subtly alter the conditions under which forms of deep privacy are shaped. When people know that pervasive surveillance is possible, they may alter their behavior to conform to perceived norms and expectations that otherwise would not apply.[30] In a world of widespread surveillance, persons do not need confirmation that they are currently being watched to alter their behavior, which in turn can be internalized to change their beliefs. Justice Douglas first sounded this note in dissents from the Court's third party and confidential informant doctrines, arguing that "[m]onitoring, if prevalent, certainly kills free discourse and spontaneous utterances."[31] Without free discourse, individuals will not have the liberty necessary for realizing personal identity and engaging in self-government.[32] Because government monitoring of both deep and shallow privacy interactions can lead to subtle alterations of both social forms and norms, it is important to examine how information sharing works within social practices. And for

---

28. *See* United States v. White, 401 U.S. 745, 750 (1971).

29. *See* Hoffa v. United States, 385 U.S. 293, 303 (1966) ("'The risk of being overheard by an eavesdropper or betrayed by an informer or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society. It is the kind of risk we necessarily assume whenever we speak.'" (quoting Lopez v. United States, 373 U.S. 427, 465 (1963) (Brennan, J., dissenting))).

30. Jeremy Bentham first introduced the idea of the panopticon in the eighteenth century. *See* JEREMY BENTHAM, THE PANOPTICON WRITINGS 29-95 (Miran Bozoic ed., Verso 1995) (1787). Michel Foucault explores the panoptic effect as a general way that society disciplines individual behavior. *See* MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 207-08 (Alan Sheridan trans., 1977). Most recently, Justice Scalia objected in dissent to the idea of creating a "genetic panopticon." Maryland v. King, 133 S. Ct. 1958, 1989 (2013) (Scalia, J., dissenting). The majority held that collecting DNA samples from those arrested for serious offenses is reasonable under the Fourth Amendment. *Id.* at 1980.

31. *White*, 401 U.S. at 762 (Douglas, J., dissenting).

32. Justice Douglas also warned that "when the most confidential and intimate conversations are always open to eager, prying ears . . . privacy, and with it liberty, will be gone." Osborn v. United States, 385 U.S. 323, 354 (1966) (Douglas, J., dissenting); *see also* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999).

this analysis, recitations of what risks persons assume in sharing information with others do not reveal much about why we must assume these risks or what the effects of law enforcement access will be on social practices. Moreover, claims about assumed risk are circular because we all assume the risks courts or legislatures sanction and impose through the privacy rules they create.[33]

Perhaps from a social welfare perspective, subtle alternations in the patterns of sharing are nonetheless optimal given the social value that might accrue from law enforcement's ready access to large amounts of minimally private information. So long as the intrusions are proportional to law enforcement needs, why be concerned about pervasive surveillance of data already publicly observable by others? Such a question is premised on understanding privacy as undisclosed or secret, smuggling into the discussion a fixed, and narrow, conception of privacy to be measured against the social welfare goals of crime prevention and investigation. But, as should be clear, privacy is more than the content of undisclosed deep privacy. What is in question here is whether intrusions on forms of shallow privacy have harmful effects of a similar magnitude as harms to deeper forms of privacy, from the perspective of personal identity. Both the quantity and quality of information accessible, absent regulation for relatively shallow forms of privacy, have costs that are more difficult to measure, but in the aggregate no less real.

In constitutional discourse, gesturing is sometimes sufficient. In First Amendment jurisprudence, a background principle is that more speech is better,[34] that debate about matters of public importance "should be uninhibited, robust, and wide-open,"[35] that "no official, high or petty, can prescribe what shall be orthodox,"[36] and that "freedom to think as you will and to speak as you think"[37] are indispensable to self-governance. These

33. *See, e.g.*, *White*, 401 U.S. at 786 (Harlan, J., dissenting) ("Our expectations, and the risks we assume, are in large part reflections of laws that translate into rules the customs and values of the past and present.").

34. *See* Cohen v. California, 403 U.S. 15, 25 (1971) ("That the air may at times seem filled with verbal cacophony is, in this sense not a sign of weakness but of strength."); Whitney v. California, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring) ("[T]he remedy to be applied is more speech, not enforced silence."), *overruled in part by* Brandenburg v. Ohio, 395 U.S. 444 (1969).

35. N.Y. Times Co. v. Sullivan, 376 U.S. 254, 270 (1964).

36. W. Va. State Bd. of Educ. v. Barnette, 319 U.S. 624, 642 (1943) ("If there is any fixed star in our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion . . . .").

37. *Whitney*, 274 U.S. at 375 (Brandeis, J., concurring).

gestures become the bedrock meanings of free speech, not subject to further welfarist balancing. By contrast, there is a comparably less than robust background principle that more privacy is always better; for in the hidden recesses of social life lies the potential for disorder that sometimes erupts into visible social decay of the kind that "broken windows" policing seeks to forestall.[38] Thus, articulations of privacy often imbed a form of balancing that already takes into account the security or policing needs of the state.[39]

But if more privacy is not always better, it does not follow that present understandings of policing practices should uncritically shape everyday political and social life. To focus legal analysis on enabling suspicionless access to third party records risks ignoring other values that zealous pursuit of order and security impact. As Charles Reich observed in the midst of the Warren Court's project of constitutionalizing criminal procedure, "The good society must have its hiding places—its protected crannies for the soul."[40] Under the First Amendment, one of the reasons for protecting speech against official interference is that persons must remain free to form their own opinions and perspectives in pursuit not only of their own identities, but also of collective self-determination.[41] Under the Fourth Amendment, one of the central values of privacy is that persons must retain the liberty to form their own personal identities through acts of both sharing and withholding information and spaces.[42] As Justice Brandeis argued,

38. *See generally* James Q. Wilson & George L. Kelling, *Broken Windows*, ATLANTIC MONTHLY, Mar. 1982, at 29-30. Under the broken windows theory, police focus on low-level crime and social disorder, aiming both to forestall the development of more serious crime and to reinforce social norms of law-abidingness and social order. *Id*.

39. *See* Thomas P. Crocker, *The Political Fourth Amendment*, 88 WASH. U. L. REV. 303 (2010) [hereinafter Crocker, *Political Fourth Amendment*].

40. Charles Reich, *Police Questioning of Law Abiding Citizens*, 75 YALE L. J. 1161, 1172 (1966).

41. *See, e.g.*, Owen M. Fiss, *Free Speech and Social Structure*, 71 IOWA L. REV. 1405, 1415-16 (1986).

42. *See, e.g.*, Minnesota v. Olson, 495 U.S. 91, 98 (1990) (protecting privacy of overnight guest in the host's home); Berger v. New York, 388 U.S. 41, 53 (1967) (protecting private conversations because "'[t]he basic purpose of [the Fourth] Amendment . . . is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials'" (quoting Camara v. Mun. Ct. of City & Cnty. of S.F., 387 U.S. 523, 528 (1967))); Katz v. United States, 389 U.S. 347 (1967); *see also* Thomas P. Crocker, *From Privacy to Liberty: The Fourth Amendment After* Lawrence, 57 UCLA L. REV. 1 (2009) [hereinafter Crocker, *From Privacy to Liberty*].

"The makers of our Constitution . . . sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations."[43]

The "self" of First Amendment self-determination is the person whose privacy the Fourth Amendment protects. This Fourth Amendment value sets a constitutional background against which legislatures and executive officials can form more refined policies and classificatory frameworks for regulating police access to third party records. To bring these values to the foreground makes it possible to better measure what might be lost to practices that further entrench the ability for police to access social media records with minimal or no showing of individualized suspicion.

What the distinction between deep and shallow privacy reveals is that the depths and measures of privacy are contingent and contextual. Privacy descriptions are also defeasible. As a result, decision makers armed with classificatory frameworks, looking to judge third party records as highly or minimally private, should be attuned to descriptions of how privacy works within social practices. Remembering who is to receive privacy protections and why are as important as classifying what information counts as private. And what counts as private depends on consideration of how information functions in practice, not merely on whether, or how, it is shared.

II. Privacy's Locations

Whether we designate information or relations to third parties as implicating "deep" or "shallow" privacy, privacy is everywhere. Thus, because privacy is so all-pervasive, it is difficult to provide analytic order to needed legal protections. We all share enormous amounts of information with others as conditions of everyday life. Such sharing is always within contextual boundaries. A transaction with a bank is a type of information sharing not meant to be a matter further shared. An opinion expressed on a social media platform is information often intended only for a particular circle friends, not for general dissemination. One's preferences for products are shared with merchants, one's buying habits are observable to credit providers, one's energy use is observed by utility providers, and one's health care information is shared with physicians and insurers—to name just a few of the ways data is shared and collected with the third parties with whom we transact. In addition, we regularly share the numbers we dial and the email addresses to which we send messages. We also share our

43. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting), *overruled in part by Katz*, 389 U.S. 347.

continuous location to various phone and internet providers, as well as to application services for mobile and cloud computing.

Given the prevalence of all this data, there are now additional businesses that collect and collate our information for other interested parties wanting to know more about who we are and what our habits might be—a ubiquitous surveillance of personal reputations to determine whether to extend credit, market goods, or offer a lease, among other uses.[44] With all of this sharing, it is easy to conclude that we readily and regularly give away our privacy. Nonetheless, sharing is contextual and contingent. Sharing can be enabled or burdened by law. Persons share limited information with others for specific purposes. The fact that such information might be used otherwise does not undermine the reasons for understanding an exchange as contextually private. Indeed, such contextual understandings often inform whether we view subsequent uses of personal information as legitimate or harmful.

Privacy's ubiquity complements its polysemy—it takes many different meanings and implicates many different roles and aspects of our lives.[45] As the LEATPR Standards note more than once, "[W]e now live in a world of ubiquitous third party information"[46] that seems to match the ubiquity of our interactions—be they commercial or personal—in multiple settings with a diverse array of others. The mere existence of pervasive third party information does not settle the question of personal privacy. Social norms can shape legal understandings and practices. In turn, legal practices can shape social meaning.[47] In this dynamic, the Supreme Court's Fourth Amendment jurisprudence provides constitutional meaning to privacy that

---

44. *See, e.g.*, Alice E. Marwick, *How Your Data Are Being Deeply Mined*, N.Y. REV. OF BOOKS, Jan. 9, 2014, http://www.nybooks.com/articles/archives/2014/jan/09/how-your-data-are-being-deeply-mined/; Charles Duhigg, *Psst, You in Aisle 5*, N.Y. TIMES, Feb. 19, 2012, at MM30, *available at* http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html. *See generally* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET (2008); Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595 (2004); Lior Jacob Strahilevitz, *Reputation Nation: Law in an Era of Ubiquitous Personal Information*, 102 NW. U. L. REV. 1667 (2008).

45. *See generally* Ronald J. Krotozynski, Jr., *The Polysemy of Privacy*, 88 IND. L.J. 881 (2013); Post, *supra* note 1; Solove, *Conceptualizing Privacy*, *supra* note 1, at 1099-1124.

46. LEATPR STANDARDS, *supra* note 9, at 2; STANDARD 25-3.1 commentary.

47. *See generally* ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES (1991) (discussing a move away from legal means dispute resolution in favor of informal means); Lawrence Lessig, *The Regulation of Social Meaning*, 62 U. CHI. L. REV. 943 (1995).

influences the possibilities for the legislative reforms that the LEATPR Standards contemplate.

One significant conceptual barrier to creating a Fourth Amendment framework for addressing the dual ubiquities of privacy and third party information is the Supreme Court's decision to narrow the scope of privacy to mean little more than secrecy through its construction of the third party doctrine.[48] Thus, the first hurdle to addressing the relation of these dual ubiquities is to do more, and go further than the Supreme Court to protect privacy in self-disclosure.[49] In this way, legislative initiatives can lead the way in a project Justice Sotomayor argued may be necessary. In *United States v. Jones*, Justice Sotomayor suggested that the Court may need to reconsider its adherence to the third party doctrine because "this approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[50] In important ways, the creative refashioning that must continually recur to match judicial doctrines crafted during an age of the rotary telephone to social practices in the digital age is no different than the work of reconsidering the third party doctrine to give renewed meaning to the values of liberty and privacy the Fourth Amendment protects.

In disclosing limited information to others in specific contexts and for particular purposes, individuals maintain a large measure of privacy. Yet if Fourth Amendment doctrine treats secrecy as a prerequisite for privacy, then it remains conceptually unmoored from important conceptions of privacy as well as from widespread social practices. Privacy implicates practices of sharing more than withholding, for the liberty of engaging in everyday life is a liberty to associate with others governed by social norms established through social interaction. To understand privacy as more than secrecy will make it possible for courts to analyze the divisible ways

48. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 117 (1984) ("It is well settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information."); Hoffa v. United States, 385 U.S. 293, 302 (1966).

49. The Standards propose shifting the focus, claiming that "privacy is not secrecy." STANDARD 25-4.1(a) commentary.

50. 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring); *see also*, Aya Gruber, *Garbage Pails and Puppy Dog Tails: Is That What* Katz *Is Made Of?*, 41 U.C. DAVIS L. REV. 781, 805-816 (2008); Stephen E. Henderson, *After* United States v. Jones*, After the Fourth Amendment Third-Party Doctrine*, 14 N.C. J. L. & TECH. 431, 454-57 (2013); Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L. J. 1309, 1330-36 (2012).

privacy matters to everyday life. As Havel suggests, deep privacy is not a desirable retreat from the world of pervasive surveillance.[51] Deep privacy may be a necessary condition for the development of personal identity, but it is far from sufficient.

Another significant conceptual hurdle to understanding the relationship between privacy and third party records is the constant tendency to retreat to a version of deep privacy as the paradigm against which we measure the intrusiveness of law enforcement access. So long as some form of deep privacy captures our imagination as what must really be protected, we risk losing sight of the need to protect the forms of shallow privacy, taken individually or in the aggregate, that comprise the ubiquity of everyday privacy.

The ubiquity of shallow privacy, therefore, has both a quantitative and qualitative aspect. The quantity of information we share across a range of platforms and practices means that unfettered police access to third party records opens the possibility of altering social practices that technology otherwise makes available. As Danielle Citron and David Gray have argued, focusing on the quantitative aspect of privacy protection enables courts and policy makers to consider how indiscriminate surveillance affects constitutionally protected liberties in the aggregate.[52] The quality of information, by contrast, is not simply a matter of whether it is undisclosed or intimate—whether access to information invades reasonable expectations of privacy—but what roles it plays in enabling the realization of personal identity. Focusing on the quality of the information accessed, and the social practices that depend on particular forms of sharing, enables courts and policy makers to be sensitive to the actual nature of the information beyond whether it is undisclosed.

Because the Supreme Court provides meaning to core constitutional values, and because values can follow the development of social practices and movements, legislatures can play an important role in pointing the way

---

51. HAVEL, *supra* note 12, at 120.

52. As they argue,

> The threshold Fourth Amendment question should be whether a technology has the capacity to facilitate broad and indiscriminate surveillance that intrudes upon reasonable expectations of quantitative privacy by raising the specter of a surveillance state if deployment and use of that technology is left to the unfettered discretion of law enforcement officers or other government agents.

David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 71-72 (2013).

towards broader privacy protections and understandings.[53] As it stands, the Supreme Court's current understanding of Fourth Amendment privacy is a barrier to conceptualizing privacy as enabling personal identity. Legislative standards for protecting privacy can lead the way. The LEATPR Standards provide one model for doing so. But legislating such a framework becomes possible only if decision makers adopt the attitudes and perspectives entailed from recognition of privacy's location in polymorphic and shared social life.

If policy makers are to obtain any organized limits and control over policing practices that access third party records, then some form of contingent and contextual judgments must be made to determine when and what can be accessed under which standards. The problem of contingency leads to classificatory pressures. Privacy advocates would like to see more information placed into the highest protected classifications, while law enforcement pushes in the opposite direction.[54] Because third party information must be classified, normative considerations are inseparable from factual claims. Deciding that information is highly private provides the justification for limiting police access. By evaluating the nature of third party information, prior commitments to understanding the scope and meaning of privacy will determine outcomes. Thus, if forms of privacy—in quality and quantity—are viewed as shallow within a framework that prioritizes deep privacy, then different normative outcomes will follow from a framework sensitive to privacy's ubiquity in everyday life.

Law enforcement exerts two kinds of pressure on constitutional protections for privacy: practically oriented downward pressure and necessity based outward pressure. Practical considerations concerned with preserving police practices exert downward pressure on the kinds of

---

53. *See, e.g.*, Roper v. Simmons, 543 U.S. 551, 564-69 (2005) (noting shifting conceptions of cruel and unusual punishment in the states); Lawrence v. Texas, 539 U.S. 558, 573 (2003) (noting changing understandings of sexual orientation). On social movements and changing constitutional understandings, see generally Jack M. Balkin & Reva Siegel, *Principles, Practices, and Social Movements*, 154 U. PA. L. REV. 927 (2006); Reva Siegel, *Dead or Alive: Originalism as Popular Constitutionalism in* Heller, 122 HARV. L. REV. 191 (2008); Reva Siegel, *Constitutional Culture, Social Movement Conflict and Constitutional Change: The Case of the De Facto ERA*, 94 CAL. L. REV. 1323 (2006).

54. *Compare* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 79-117 (2007) (arguing for more regulation of public surveillance), *with* Florida v. Jardines, 133 S. Ct. 1409, 1413-14 (2013) (involving law enforcement attempts to expand the use of dog sniffs to the home).

practices that constitute searches for Fourth Amendment purposes.[55] Necessity and exceptional circumstances exert pressure on courts to create exemptions to the application of otherwise governing doctrinal rules.[56]

Downward pressures place more information in the least protected categories. The first question of Fourth Amendment law is whether a form of police investigative-looking constitutes a search.[57] In order to avoid more constraining constitutional rules, the Court has concluded that a number of practices that would constitute searching in everyday parlance, do not rise to the level of a constitutional search. For example, looking through a person's trash left by the street in accordance with municipal regulations is not a search,[58] nor is hovering over a person's residential property from a height of 400 feet in a helicopter to look through the roof of a greenhouse.[59] Examining a person's "open fields" is not constitutional searching,[60] nor is gathering information from third parties such as banks or telephone providers with whom a person has "voluntarily" conveyed personal information.[61] At least as a general matter, Physically tracking a person's movements on public roadways does not constitute a search, even with technological assistance.[62] After the Supreme Court in *United States v. Jones* held that placing a tracking device on a person's vehicle constitutes

55. *See, e.g.*, United States v. Place, 462 U.S. 696, 707 (1983) ("A 'canine sniff' by a well-trained narcotics detection dog . . . is much less intrusive than a typical search."); *see also* Christopher Slobogin, *Why Crime Severity Analysis Is Not Reasonable*, 97 IOWA L. REV. BULL. 1, 4-6 (2012) (considering the prospect that altering the standard for searches based on severity of the crime will lead to lower standards for more serious crimes).

56. *See* Florence v. Bd. of Chosen Freeholders, 132 S. Ct. 1510, 1522 (2012) (holding that because of "the essential interest in readily administrable rules," the Fourth Amendment does not limit imposition of strip searches on those arrested for minor crimes); *see also* Kentucky v. King, 131 S. Ct. 1849, 1857 (2011) (police-created exigency); California v. Acevedo, 500 U.S. 565 (1991) (automobile exception); New Jersey v. T.L.O., 469 U.S. 325, 340-43 (1985) (special needs exception). The Court rejected a "murder scene exception" in Mincey v. Arizona, 437 U.S. 385 (1978).

57. *See, e.g.*, United States v. Dunn, 480 U.S. 294, 301 (1987) (distinguishing looking in open fields from observing areas within curtilage in deciding whether a search has occurred).

58. California v. Greenwood, 486 U.S. 35, 37 (1988).

59. Florida v. Riley, 488 U.S. 445, 452 (1989).

60. *See* Oliver v. United States, 466 U.S. 170, 179 (1984) ("[O]pen fields do not provide the setting for those intimate activities that the Amendment is intended to shelter from government interference or surveillance. There is no societal interest in protecting the privacy of those activities, such as the cultivation of crops, that occur in open fields.").

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

62. *See* United States v. Knotts, 460 U.S. 276, 281-82 (1983).

an unconstitutional physical trespass,[63] a key unresolved constitutional question is whether specific forms of tracking, such as using a cell phone's GPS location data or short-term electronic monitoring of a person's movements, would constitute a Fourth Amendment search.[64] When the Court views restrictions on policing practices as too burdensome, the first analytic step is to conclude that an investigatory technique is not a search.[65]

Outward pressure employs exigencies as ways to exit otherwise applicable constitutional rules. If special circumstances or emergency situations arise, then exceptions sometimes authorize police to act free from normal legal constraints. When responding to violence unfolding in a home, police may enter without a warrant, arrest persons, and conduct searches incident to those arrests, despite the background rule stating otherwise.[66] And when special needs have been asserted, such as enforcing immigration laws near an international border[67]; ensuring compliance with licensing, registration, and sobriety requirements when driving a vehicle[68]; or enforcing compliance with anti-drug use policies for student athletes,[69] the Court has altered default rules to allow officials an exemption. Such outward pressure comes from prioritizing the necessity of particular circumstances over the ex ante governance of rules. In this dynamic, constitutional principles serve as pre-commitments against which the flexibility of necessity stands opposed.[70] But the circumstantial contingency of necessity provides flexibility at the risk of undermining constitutional norms. The Court has held that strict enforcement of a rule requiring police to obtain a warrant before entering a home to conduct a search would be unreasonable when police have reason to fear evidence might be destroyed.[71] On this view, well-established exceptions must be carefully safeguarded against the encroaching influence of constitutional rules.[72]

---

63. 132 S. Ct. 945, 950-51 (2012).

64. *See In re* Application of United States for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (holding no Fourth Amendment search when police acquire historical cell site data of a person's movements).

65. *See, e.g.*, *id.*

66. *See* Brigham City, Utah v. Stuart, 547 U.S. 398, 403 (2006) (stating that home entry without a warrant is reasonable to render emergency aid).

67. *See* United States v. Martinez-Fuerte, 428 U.S. 543, 545 (1976).

68. *See* Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990).

69. *See* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 664-65 (1995).

70. *See, e.g.*, JON ELSTER, ULYSSES UNBOUND: STUDIES IN RATIONALITY, PRECOMMITMENT, AND CONSTRAINTS 174 (2000).

71. Kentucky v. King, 131 S. Ct. 1849, 1857 (2011) ("[A] rule that precludes the police from making a warrantless entry to prevent the destruction of evidence whenever their

Both forms of pressure would be brought to bear on any legislative classificatory scheme designed to regulate police access to third party records. Such pressure leads to descriptive defeasibility. Law enforcement will argue that most third party records, perhaps apart from medical records, are either not private or are minimally private, access to which warrants little or no oversight. In this dynamic, policing priorities create focused reasons to allow more access in the name of security.[73] In this way, downward pressure would exist in deciding how to classify information. And classificatory decisions in turn rely on background conceptions of privacy's importance as compared to the claimed need and perceived intrusion of policing practices.

Descriptive defeasibility is also evident in placing exigent circumstance exceptions at the heart of a rule's conceptualization. Commitments to constitutional constraints are only as strong as the availability of claims of necessity. By seeking to ensure freedom from constraint in particular circumstances, policy makers reveal that their constitutional commitments extend no further than the easy cases, when the inconvenience of protecting privacy does not pinch too much. This constitutional hesitation is evident in the recently adopted LEATPR Standards, which give ample regard to the possibility of exigent circumstances.[74] But so long as legal rules and principles constrain what would otherwise be unfettered, episodic, and circumstantial responses to perceived investigatory needs, they function as self-binding guides on behalf of values and principles that might otherwise go unrealized.[75]

In two nods to the uncertainty and complexity of police investigative needs, the Standards grant purposive override to any of their prescriptions for claims based on exigency and on the social cost of inhibiting the ability to solve an "unacceptable amount of otherwise solvable or preventable crime."[76] If constraints on police access to third party records pinch too much, then, according to the LEATPR Standards, the practical exigencies

---

conduct causes the exigency would unreasonably shrink the reach of this well-established exception to the warrant requirement.").

72. *See* Thomas P. Crocker, *Order, Technology, and the Constitutional Meanings of Criminal Procedure*, 103 J. CRIM. L. & CRIMINOLOGY 685, 716-19 (2013) [hereinafter Crocker, *Constitutional Meanings*].

73. Of course, security is something the Fourth Amendment seeks to provide by granting a right "to be secure," though from a different risk—that of the state itself. *See* Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 104 (2008).

74. *See* STANDARD 25-5.4.

75. *See* ELSTER, *supra* note 70, at 115-18.

76. STANDARD 25-4.2(b).

should override privacy protections. Of course, social costs abound—both in limiting and in freeing police discretion. How this determination of social cost is made depends on prior decisions about which factors are relevant. Imagine an alternative formulation of the social cost, one that does not permit an investigatory exit from constitutional rules: if access to records thought reflective of minimally private information ("shallow privacy") would unduly risk inhibiting First Amendment activities or risk undermining other protected liberties, then legislatures should increase the level of justification required for access. Because the social cost to privacy is at least as great as the cost of losing investigatory advantage, whether we choose to imbed an exigency exception or a privacy boost depends on prior judgments about purposes and priorities.

In thinking about whether, or to what extent, courts or legislatures should be sensitive to social costs, it is important to consider how interests are checked by institutional design within constitutional structure. In the conflict between privacy and security, which institution will check claims of necessity? Under the Fourth Amendment, the Supreme Court often takes note of the interests of law enforcement in having bright line rules that are easily administered and not unduly burdensome.[77] These interests are represented by law enforcement agencies backed by legislative empowerment. Yet this same Court must also check law enforcement by interposing constitutional constraints on investigation procedures.[78]

Similarly, the legislature represents the people's desire to criminalize various behaviors, charging the executive to implement and enforce legislative will. At the same time, a legislature also has the institutional power to check illegitimate policing practices. Citizens do not want law enforcement to exercise illegitimate means when maintaining order and security or investigating crime.[79] Constitutional structure is thus divided on the question of privacy. The governing institutions whose function is to check investigatory zeal are the same institutions often inclined to authorize it. Because privacy is a value shared by all, no particular group represents

77. *See, e.g.*, Atwater v. City of Lago Vista, 532 U.S. 318, 347 (2001) ("Courts attempting to strike a reasonable Fourth Amendment balance thus credit the government's side with an essential interest in readily administrable rules.").

78. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 40 (2001).

79. *See, e.g.*, Stephen J. Schulhofer et al., *American Policing at a Crossroads: Unsustainable Policies and the Procedural Justice Alternative*, 101 J. CRIM. L. & CRIMINOLOGY 335, 349-56 (2011); Tom R. Tyler et al., *Legitimacy and Deterrence Effects in Counterterrorism Policing: A Study of Muslim Americans*, 44 LAW & SOC'Y REV. 365, 369-71 (2010).

an insular minority against whom legislation warrants particular judicial scrutiny.[80] As a result, the pressures represented by an added layer of "social cost" balancing also serve to make less visible the diffuse harms privacy invasions impose, since the "social cost" to be measured is a further calculation of what is lost through investigatory constraints.[81]

Successful implementation of any regulatory regime restricting law enforcement access depends upon the background privacy conceptions at hand. In some way, this structure is the companion to Milton Friedman's claim about emergency: "Only a crisis—actual or perceived—produces real change. When that crisis occurs, the actions that are taken depend on the ideas that are lying around."[82] When police practices become visible as problematic, the reforms undertaken will depend on what conceptions of privacy and liberty we have at hand. It may also be the case that only a crisis produced by excessive police practices will produce real change. It can be all too easy to think that if one has nothing to hide, then one need not worry about pervasive surveillance[83]—a claim that itself depends on the invisibility of many surveillance techniques, especially those that gain access to third party records.

Privacy's ubiquity is paradoxically related to its visibility.[84] The more new forms of sharing with others in everyday life become visible, the more privacy becomes vulnerable under the third party doctrine. At the same time, the more visible police presence is in everyday life, the more salient the intrusions on liberty and privacy become. A police officer on every street corner or officers who follow persons wherever they go would make visible the existence of a permeating police presence.[85] By contrast, a police

---

80. *See* United States v. Carolene Prods. Co., 304 U.S. 144, 152 n.4 (1938). Of course, something similar could be said about equal protection or free speech—courts play a dual role of institutional check and institutional authorization. But when it comes to privacy's ubiquity, the very conception of the value imbeds a tradeoff (privacy and security) in a way that free speech does not, for example.

81. As the Standards note, "[B]ecause whereas law enforcement need for a type of information will often rightly be evident and compelling, the effects of inadequately regulating such access can be just as compelling, if often more diffuse and long-term." STANDARD 25-4.2(a) commentary.

82. MILTON FRIEDMAN, CAPITALISM AND FREEDOM xiv (2002).

83. *See* Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 748-53 (2007).

84. *See* Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181, 191-92 (2008).

85. Attitudes about surveillance take into account the quantity of surveillance, not simply the visibility of being seen in public. *See* SLOBOGIN, *supra* note 54, at 183-85; Jeremy A. Blumenthal et al., *The Multiple Dimensions of Privacy: Testing Lay "Expectations of*

officer tracking a person through third party records, including real-time cell site location data, does so unseen by the target. Yet, in other contexts, a political society in which police officers are a ubiquitous presence is one the Supreme Court has identified as a "police state."[86] In this way, privacy protections depend on surveillance visibility. If officers were to follow large numbers of people everywhere they went during a day, watching and recording their movements, noting their associates, and listening to their conversations, Americans would declare the existence of a police state and demand political change. Such a judgment would in part reflect the visibility of such policing practices and the discernible effects such a permeating presence would have on social and political life. Though, to be clear, nothing about such practices would violate present Supreme Court understandings of Fourth Amendment constraints that place no restrictions on public observations by law enforcement.[87]

Is privacy located in the deep recesses of personal life or the more interactive world of social sharing? Does it depend on the priorities of policing or the prevalence of interpersonal social practices? Where we locate privacy in both conceptual analysis and social practice impacts the legal conclusions we reach. In this way, privacy has a geography that law shapes even as it charts.

III. Privacy's Constraints: Constitutional and Conceptual

Constitutional restrictions apply when police interact with individuals, seeking to ascertain whether perceived suspicious behavior indicates criminal conduct. Although widespread use of "stop and frisk" techniques has generated controversy,[88] police are free to conduct temporary seizures

---

Privacy," 11 U. PA. J. CONST. L. 331 (2009); Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society"*, 42 DUKE L.J. 727 (1993).

86. Johnson v. United States, 333 U.S. 10, 17 (1948) (speaking of "the most fundamental distinctions between our form of government, where officers are under the law, and the police-state where they are the law"); *see also* Harris v. United States, 331 U.S. 145, 171 (1947) (Frankfurter, J., dissenting) (speaking of the Fourth Amendment, Justice Frankfurter noted "its important bearing in maintaining a free society and avoiding the dangers of a police state").

87. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 449-52 (1989); Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986); United States v. Knotts, 460 U.S. 276, 281-82 (1983).

88. *See* Floyd v. City of N.Y., 959 F. Supp. 2d 668 (S.D.N.Y. 2013); Benjamin Weiser & Joseph Goldstein, *Mayor Says City Will Settle Suits on Frisk Tactics*, N.Y. TIMES, Jan. 31, 2014, at A1, *available at* http://www.nytimes.com/2014/01/31/nyregion/de-blasio-stop-and-

and limited searches as part of their practice of maintaining street order.[89] Police need not wait until criminal actions are complete, but may intervene proactively to prevent criminal conduct.[90] When combined with order-maintenance policing practices inspired by a "broken windows" perspective, the goal becomes to reduce low-level criminal behaviors such as loitering, littering, and vagrancy in order to signal social intolerance for criminal conduct. By adopting a zero-tolerance policy, police reinforce community norms of law abidingness that in turn are thought to reduce the prevalence of criminal conduct.[91] No restrictions exist on the frequency or distribution of such techniques so long as each encounter individually complies with constitutional standards.[92] Absent constitutional barriers, order-maintenance policing becomes a low-cost and pervasive approach to law enforcement practice.[93] When conducting street patrols, police presence

---

frisk.html; Al Baker, *City Minorities More Likely to Be Frisked: Increase in Police Stops Fuels Intense Debate*, N.Y. TIMES, May 13, 2010, at A1, *available at* http://www.nytimes.com/2010/05/13/nyregion/13frisk.html?pagewanted=all; *see also* Shannon Parker, *Independent Oversight Needed to Curb NYPD Stop and Frisk Abuse, Experts Say*, BRENNAN CTR. FOR JUST. (May 30, 2013), http://www.brennancenter.org/blog/independent-oversight-needed-curb-nypd-stop-and-frisk-abuse-experts-say; *Stop-and-Frisk Campaign: About the Issues*, N.Y. CIVIL LIBERTIES UNION, http://www.nyclu.org/issues/racial-justice/stop-and-frisk-practices (last visited Jan. 28, 2014).

89. Terry v. Ohio, 392 U.S. 1, 29-30 (1968).

90. *Id.* at 24. As the Supreme Court reasoned in *Terry*, "[W]e cannot blind ourselves to the need for law enforcement officers to protect themselves and other prospective victims of violence in situations where they may lack probable cause for an arrest." *Id.*; *see also* Stephen A. Saltzburg, Terry v. Ohio*, A Practically Perfect Doctrine*, 72 ST. JOHN'S L. REV. 911, 952 (1998) ("The common sense of *Terry* is that law enforcement officers should not be required to wait to act until a crime is complete, whereby society suffers a criminal injury . . . .").

91. *See* Dan M. Kahan, *Social Influence, Social Meaning, and Deterrence*, 83 VA. L. REV. 349, 369 (1997) ("Visible disorder is a self-reinforcing cue about the community's attitude toward crime."); Tracey L. Meares & Dan M. Kahan, *Law and (Norms of) Order in the Inner City*, 32 LAW & SOC'Y REV. 805, 806 (1998) ("By shaping preferences for crime, accentuating the perceived status of lawbreaking, and enfeebling the institutions that normally hold criminal propensities in check, disorderly norms create crime."). *But see* BERNARD E. HARCOURT, ILLUSION OF ORDER: THE FALSE PROMISE OF BROKEN WINDOWS POLICING 7 (2001) ("After reviewing the available social-scientific data . . . I find that there is no good evidence to support the broken windows theory.").

92. *See, e.g.*, Illinois v. Wardlow, 528 U.S. 119, 123 (2000); Whren v. United States, 517 U.S. 806, 811-13 (1996). *But see* City of Chi. v. Morales, 527 U.S. 41, 63-64 (1999) (holding frequently used ordinance against loitering was unconstitutionally vague).

93. *See* Crocker, *Constitutional Meanings*, *supra* note 72, at 735-39; Debra Livingston, *Police Discretion and the Quality of Life in Public Places: Courts, Communities, and the New Policing*, 97 COLUM. L. REV. 551, 653-59 (1997).

is visible to citizens whose communities either cooperate in maintaining social order or engage the political process to institute changes in practice. But the consequences of police presence through digital media, or through suspicious activity monitoring, is less visible and therefore more difficult for citizens to check through political processes.

The digital "stop and frisk" becomes possible if police are allowed to patrol social media as they do the streets and sidewalks.[94] Like the tension that exists between a free public sphere and stop and frisks, the digital stop and frisk risks altering the experience of the public sphere for many persons.[95] First Amendment jurisprudence has long recognized that a robust public sphere is a necessary condition for successful democratic self-determination.[96] When they see something suspicious, law enforcement officers might inquire further, following a person across different platforms containing third party information. The difference is that in a standard stop and frisk the amount of information available to police is comparatively limited—typically a person's identity and whatever can be quickly ascertained through consensual conversation.[97] Even here, the information accessible through police questioning is limited by an individual's right to decline to answer.[98]

But in a digital "stop and frisk," police have a vast amount of additional information at hand that also has the qualitative aspect of providing more detailed information about a person's identity. Personal beliefs, habits, associations, and activities can be easily compiled to form a third person

94. *See Terry*, 392 U.S. at 29-30; *see also*, Ian Urbina, *Social Media, a Trove of Clues and Confessions*, N.Y. TIMES, Feb. 16, 2014, at SR5, *available at* http://www.nytimes.com/2014/02/16/sunday-review/social-media-a-trove-of-clues-and-confessions.html?_r=0.

95. Such "transactional surveillance" or "digital dossiers" have the capacity to alter social participation and experience. *See* SLOBOGIN, *supra* note 54, at 168-203 ("transaction surveillance"); DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 165-209 (2004) ("digital dossiers").

96. *See, e.g.*, Int'l Soc'y for Krishna Consciousness, Inc. v. Lee, 505 U.S. 672, 696 (1992) (Kennedy, J., concurring in judgment) ("Public places are of necessity the locus for discussion of public issues . . . . At the heart of our jurisprudence lies the principle that in a free nation citizens must have the right to gather and speak with other persons in public places."); Red Lion Broad. Co. v. FCC, 395 U.S. 367, 390 (1969) ("It is the purpose of the First Amendment to preserve an uninhibited marketplace of ideas in which truth will ultimately prevail . . . .").

97. *See* Hiibel v. Sixth Jud. Dist. Ct. of Nev., Humboldt Cnty., 542 U.S. 177, 185-89 (2004).

98. *See, e.g.*, Illinois v. Wardlow, 528 U.S. 119, 125 (2000); Florida v. Royer, 460 U.S. 491, 497-98 (1983) ("The person approached, however, need not answer any question put to him; indeed, he may decline to listen to the questions at all and may go on his way.").

narrative about a person's identity. Through an extended digital "stop and frisk," police can ascertain a person's religious, political, and sexual orientations, in addition to one's reading, traveling, and shopping proclivities.[99] The digital "stop and frisk" also can be of greater temporal duration. The amount of time police may detain a person on the street is limited to the scope of the reasonable suspicion that justifies the temporary seizure in the first instance.[100] But there are no comparable temporal limits of police inquiry into the digital person.

This one example illustrates how difficult it is to import questions and issues from everyday policing into the electronic context. When an officer confronts an individual on the street, the stop is relevant to a suspicion articulable at the outset of the encounter.[101] It is an encounter with a definite end, identifiable by citizen and police alike. But the digital stop and frisk has neither this symmetry nor the limits imposed by reasonableness and relevance. Thus, police monitoring of social media is not at all like police monitoring of city streets. Nor is access to digital records, as a general matter, on par with access to specific data such as phone records for a specific time period.[102] In this way, a key precedent, *Smith v. Maryland*,[103] often cited to justify broad authority to examine third party records for which individuals have no expectation of privacy,[104] does not readily apply.[105] Neither the quality nor the quantity of data available to many searches of social media or other forms of third party records is sufficiently analogous to the pen register data found to reside outside Fourth Amendment protections in *Smith*.[106] The amount of added content available, in addition to the persons to whom that content is made available, is a far

99. *See, e.g.*, Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 389 (2008).

100. *See, e.g.*, Arizona v. Johnson, 555 U.S. 323, 333 (2009) (concluding a lawful seizure occurs "so long as those inquiries do not measurably extend the duration of the stop"); United States v. Sharpe, 470 U.S. 675, 686 (1985) (examining "whether the police diligently pursued a means of investigation that was likely to confirm or dispel their suspicions quickly").

101. *See* Terry v. Ohio, 392 U.S. 1, 21 (1968).

102. Though even here, the amount of information a police officer might acquire in a street stop and frisk will likely be much smaller than the constitutionally ungoverned check of a person's financial records.

103. 442 U.S. 735 (1979).

104. *Id.* at 743-44.

105. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 31 (D.D.C. 2013). *But see* ACLU v. Clapper, 959 F. Supp. 2d 724, 750-52 (S.D.N.Y. 2013).

106. 442 U.S. at 742-43.

more powerful view of a person's identity, history, and current projects than either phone records or brief street conversations in isolation.[107]

Personal history is both about who we are as persons as well as who others construe us to be. It is in the nature of personal identity that there is no single answer to the question of who one is. Although questions of personal identity invite nettlesome philosophical issues, one important aspect is often thought to be maintaining the continuity of a person's experiences and relations to others.[108] We are, in important respects, our histories. But histories can be ambiguous, the full meaning of which is open to future articulation as experiences lead to further narrative refinements about who a person is through the actions and beliefs that sustain the person through time. The further back in a personal history one goes, the more attenuated some of the information might become, and the less accurate a third party's construction of the person's identity, motives, and dispositions might become. Police access to historical data requires interpretation, and the further removed from context the information is, the more misleading the data can be. Moreover, the more incomplete the data, the more interpretive freedom the police have to construe the meaning of prior events.[109] But investigative police work is not always about prosecutions. It is often about social order, involving discretion, and backed by general statutes about public order that can be employed almost at will.[110]

---

107. As Judge Richard Leon concludes in analyzing surveillance activity of the National Security Agency, "I am convinced that the surveillance program now before me is so different from a simple pen register that *Smith* is of little value in assessing whether the Bulk Telephony Metadata Program constitutes a Fourth Amendment search." *Klayman*, 957 F. Supp. 2d at 32. `

108. *See, e.g.*, MACINTYRE, *supra* note 24, at 190; DEREK PARFIT, REASONS AND PERSONS 281-306 (1984); BERNARD WILLIAMS, PROBLEMS OF THE SELF 46-63 (1973). *See generally* PERSONAL IDENTITY (John Perry ed., 1975).

109. A similar danger from pervasive surveillance is that ordinary behavior may amplify state power, "adding information to databases that makes inferences more powerful and effective. Our behavior may tell things about us that we may not even know about ourselves." Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 13 (2008).

110. *See generally* Robert C. Ellickson, *Controlling Chronic Misconduct in City Spaces: Of Panhandlers, Skid Rows, and Public-Space Zoning*, 105 YALE L. J. 1165 (1996); Meares & Kahan, *supra* note 91; *see also* Tracey M. Meares, *The Good Cop: Knowing the Difference Between Lawful or Effective Policing and Rightful Policing—And Why It Matters*, 54 WM. & MARY L. REV. 1865, 1870 (2013) ("Broad discretion allows police to shape, redescribe, and recategorize situations and contexts in ways that defy strictly defined codes, so that attempts to specify strict rule compliance seem somewhat misfitting.").

Police investigation of the First Amendment protected activities of Occupy Wall Street activists in New York City during 2011 illustrates well the significance of this link between unregulated access to greater quantities and quality of electronic data.[111] Using access to social media, which under current Supreme Court jurisprudence is non-protected information,[112] New York City police (and police in other cities) tracked and followed Occupy Wall Street activists.[113] Ascertaining their planned protest-related activities, New York police intervened, preemptively in many cases, to disrupt organizing activities and to prevent the exercise of freedom of association and public speech.[114] They intervened with arrests not for serious crime, but for "obstructing governmental administration," as the *New York Times* reported.[115] The digital stop and frisk was *not* for the purposes of investigating a conspiracy to obstruct "governmental administration," nor could it be based on a particular suspicion that a particular individual was engaged in criminal activity. Rather, the purpose was to monitor the political activities of a particular group.[116] The decision to exercise legal authority to intervene and prevent political activity came later—and at the discretion of the police officer now on the street backed by a profile of the person's identity gleaned through third party records. It is not difficult to imagine a similar scenario in which officers monitor a planned political gathering to which many individuals will travel by car. To forestall the

111. *See, e.g.*, Michael S. Schmidt & Colin Moynihan, *F.B.I. Counterterrorism Agents Monitored Occupy Movement, Records Show*, N.Y. TIMES, Dec. 25, 2012, at A18, *available at* http://www.nytimes.com/2012/12/25/nyregion/occupy-movement-was-investigated-by-fbi-counterterrorism-agents-records-show.html; *see also* Bernard E. Harcourt, *Occupy Wall Street's 'Political Disobedience'*, N.Y. TIMES (Oct. 13, 2011), *available at* http://opinionator.blogs.nytimes.com/2011/10/13/occupy-wall-streets-political-disobedience/; Mattathias Schwartz, *Pre-Occupied: The Origins and Future of Occupy Wall St.*, NEW YORKER (Nov. 28, 2011), http://www.newyorker.com/reporting/2011/11/28/111128fa_fact_schwartz?currentPage=all.

112. Smith v. Maryland, 442 U.S. 735, 744 (1979). Such information would likely fall under the category of minimally protected or unprotected data according to the Standards. *See* LEATPR STANDARDS, *supra* note 9, at 13-14.

113. Colin Moynihan, *Wall Street Protesters Complain of Police Surveillance*, N.Y. TIMES, Mar. 12, 2012, at A17, *available at* http://www.nytimes.com/2012/03/12/nyregion/occupy-wall-street-protesters-complain-of-police-monitoring.html?_r=0.

114. *Id.*

115. *Id.*

116. Similar activities led to legislative reform of government power to conduct domestic surveillance. The FBI engaged in a Counter Intelligence Program (COINTELPRO) beginning in the 1950s in which it conducted covert surveillance of anti-war and civil rights groups, among others, leading to an eventual Senate investigation lead by Senator Church. *See* S. REP. 94-755, at 1-2 (1976).

success of the planned activities, police have at their discretion the ability to pull over any car at practically any time for violation of some traffic rule (e.g., deviating in a lane) and where authorized, to make an arrest for minor misdemeanor offenses.[117] In other contexts, the Supreme Court has limited the discretion of police by striking down vague public order statutes as violating due process and the First Amendment.[118]

In the Occupy Wall Street intervention, the relevance of the third party records access was unrelated to the eventual justifications for arresting individuals. If we focus only upon the synchronic and episodic moment of the traffic stop and the subsequent arrest, then the only question is whether the police had legal justification—in this case probable cause—for their actions. The fact that the stop was a pretense on behalf of other purposes is a fact that is invisible under the Court's current Fourth Amendment jurisprudence.[119] The surrounding context—how the police came to be in a position to make a seizure or conduct a search—does not affect, according to the Court, the legitimacy of the search or seizure.[120] In this way, prior investigatory techniques or actions are disconnected from subsequent police actions. Targeting political groups for surveillance of constitutionally protected activity for discretionary misdemeanor-based interventions has not affected the legality of those interventions under the Fourth Amendment—even if they are pretextual and designed to suppress activities police have no direct authority to suppress. If the police surveillance can be shown to disrupt or deter the exercise of free speech, it might constitute a cognizable First Amendment injury.[121] But short of that, according to the

117. *See* Atwater v. City of Lago Vista, 532 U.S. 318, 327 (2001). Use of pretense, and outright misconduct, are part of the story of how Occupy organizers were treated. *See, e.g.*, Jason Cherkis & Zach Carter, *FBI Surveillance of Occupy Wall Street Detailed*, HUFFINGTON POST, Jan. 5, 2013, http://www.huffingtonpost.com/2013/01/05/fbi-occupy-wall-street_n_2410783.html; Matthew Rothschild, *Spying on Occupy Activists*, PROGRESSIVE, June 2013, http://progressive.org/spying-on-ccupy-activists.

118. *See, e.g.*, Papachristou v. City of Jacksonville, 405 U.S. 156, 168-69 (1972); Shuttlesworth v. City of Birmingham, Ala., 394 U.S. 147, 153 (1969).

119. *See* Whren v. United States, 517 U.S. 806, 810 (1996); *Atwater*, 532 U.S. at 354.

120. *See, e.g.*, Kentucky v. King, 131 S. Ct. 1849, 1857-61 (2011) (rejecting analysis of police created exigent circumstances); Scott v. Harris, 550 U.S. 372, 383-85 (2007) (rejecting consideration of whether police should cease pursuit of motorist in determining the reasonableness of deadly force); *Atwater*, 532 U.S. at 354 ("If an officer has probable cause to believe that an individual has committed even a very minor criminal offense in his presence, he may, without violating the Fourth Amendment, arrest the offender.").

121. *See* United States v. U.S. Dist. Ct. for E. Dist. of Mich., 407 U.S. 297, 320 (1972) ("Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech."). The

Court, we "assume the risk" that our acts of sharing render us vulnerable to police who may access what we have shared.[122] In this respect, police are said to be no different than any other member of the public who can observe our public movements and receive information third parties choose to reveal.[123]

Who is being targeted, what kinds of activities are being targeted, and how much the access police seek relates to constitutionally protected liberties versus how much relates to criminal activity are among the questions relevant to preventing law enforcement from using minor offenses as a pretext for suppressing political activity. When the justification for searching third party records is based on a lower standard of reasonable suspicion, there is a greater risk that the grounds for the investigation may be disconnected from the eventual exercise of discretionary authority to enforce traffic stops, "obstructing governmental administration," and the like. This risk is related to both the quality and quantity of information available that can be used against individuals based on government officials' judgments about the value and desirability of the underlying free speech, or otherwise protected, activities. Of course, inadvertence when conducting a justified search does not undermine the ability for police to seize evidence for use in a related criminal arrest.[124] The search for drugs backed by a warrant that uncovers an illegally possessed handgun is not an invalid search merely because the evidence found was not purposefully sought.

Supreme Court indicated, while not holding, that the First Amendment could be violated by government presence at public meetings. Laird v. Tatum, 408 U.S. 1, 11 (1972) (suggesting that "constitutional violations may arise from the deterrent, or 'chilling,' effect of governmental regulations that fall short of a direct prohibition against the exercise of First Amendment rights"). Lower courts have followed this approach. *See, e.g.*, Alliance to End Repression v. City of Chi., 627 F. Supp. 1044, 1055-56 (N.D. Ill. 1985); Handschu v. Special Servs. Div., 349 F. Supp. 766, 770-71 (S.D.N.Y. 1972).

122. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 117 (1984) ("It is well settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities."); *see also* Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 CALIF. L. REV. 1593, 1648-50 (1987); Crocker, *From Privacy to Liberty*, *supra* note 42, at 48-56.

123. *See* California v. Greenwood, 486 U.S. 35, 41 (1988) ("[P]olice cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public."); United States v. Knotts, 460 U.S. 276, 281-82 (1983).

124. *See* Horton v. California, 496 U.S. 128, 137 (1990); Arizona v. Hicks, 480 U.S. 321, 326 (1987).

But the issue of the scope and quality of third party records searches is different. First, pressure exists to treat cyberspace like streetscapes,[125] allowing police to rove at will through social networks with lowered standards of justification for targeting individuals for further inquiry. Social media sharing is a form of shallow privacy that enables the development of beliefs and opinions necessary for personal identity. Second, the quality and quantity of information law enforcement can acquire increases the risks that law enforcement will use access to social media records to harass and suppress disfavored groups and activities—risks associated in American history with the general warrants the Fourth Amendment proscribes.[126] Third, because law enforcement may occupy social media, the use and trust individuals place in their communications changes, creating a risk of chilling free expression and associational liberties that the Constitution otherwise protects.[127] In light of these risks, placing the standard for access even to so-called "minimally private" information lower than probable cause too easily allows the digital stop and frisk to undermine protected liberties.

Context matters to the liberties that privacy sustains. At present, synchronic analysis of police conduct does not recognize how action that seems reasonable under a narrow context can be unreasonable in light of additional contextual facts.[128] In assessing Fourth Amendment reasonableness, the Supreme Court focuses only upon the moment when a

125. *See supra* notes 73-75 and accompanying text.

126. In a related case involving searches of computer databases for specific files, the Ninth Circuit noted that the "pressing need of law enforcement for broad authorization to examine electronic records . . . creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176 (9th Cir. 2010). *See generally*, Boyd v. United States, 116 U.S. 616, 625-26 (1886) (explaining historical foundations for the Fourth Amendment as a response to "grievous abuses," "[p]rominent and principal among these was the practice of issuing general warrants.").

127. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (discussing how the mode of observation in and of itself can have a deleterious effect on the relationship between society and government).

128. *See* David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J. L. & TECH. 381, 399 (2013); Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1, 24-25 (2012). *But see* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012) (undercutting the mosaic theory approach to regulating police searches).

search or seizure occurs, purporting to ignore broader contextual factors.[129] But, judgments about reasonable expectations of privacy, or judgments about the reasonableness of police action in particular circumstances, require context. The only question is how broadly to construe the context.[130] By taking a synchronic approach, the Court chooses to look narrowly at context. Categorizing standards of law enforcement access based on the social practices in which information is embedded is already a contextual approach, albeit one focused on the practices of personal sharing or withholding.[131] What is needed is consideration of the context of the uses to which law enforcement might put information gained through broad access to third party records.

Whether information is deep or shallow, police access should require probable cause when the search of third party records gives information about activities and associations that can be used to target individuals for discretionary intervention unrelated to the justification for access to the information. The First Amendment models such restrictions when it forbids state officials from compelled disclosure of membership lists when there is a risk of chilling the exercise of associational freedoms.[132] Such requests for disclosure would reveal the same kinds of information available from third party records, to which public officials may have unregulated access. It cannot be the case that the value the Court attaches to the "collective effort

---

129. *See* Kerr, *supra* note 128, at 320-43; *see also supra* note 120 and accompanying text.

130. *See, e.g.*, Gray & Citron, *supra* note 128, at 427-28 (recognizing the contingency of doctrinal decisions regarding timeframes under mosaic theory); Slobogin, *supra* note 128 , at 16-17 (suggesting that courts aggregate the time of investigation to determine whether a search has occurred).

131. What makes an expectation of privacy reasonable under the Court's Fourth Amendment jurisprudence depends on the context. *See* California v. Greenwood, 486 U.S. 35, 40 (1988) (relying on "common knowledge" and regular practice to ascertain whether "society is prepared to accept" an expectation of privacy as reasonable).

132. As the Court declared,

> [C]ompelled disclosure of petitioner's Alabama membership is likely to affect adversely the ability of petitioner and its members to pursue their collective effort to foster beliefs which they admittedly have the right to advocate, in that it may induce members to withdraw from the Association and dissuade others from joining it because of fear of exposure of their beliefs shown through their associations and of the consequences of this exposure.

NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 463 (1958); *see also* Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741 (2008).

to foster beliefs"[133] through associations depends on the method by which public officials acquire the information. Under the First Amendment, what matters is the possession and use of such information by government officials. In this way, the standard for access does not vary based on the nature of the crime; rather, the standard considers the contextual uses to which law enforcement might put the information.[134]

Law enforcement that seeks to solve a particular crime by examining a suspect's social media records is different than law enforcement surveillance of social media as if it were a busy street corner, which in turn is different than monitoring the activities of a particular social and political group because of a believed heightened risk that they may engage in disorderly behavior in pursuit of their political goals. When probable cause exists to think that examination of third party records will produce evidence of a crime, then there is a lowered concern about inappropriate targeting of groups and individuals for surveillance and harassment. But when there need only be suspicion that the groups or individuals might disrupt public order in some minor way in pursuit of their associational freedoms, then there is a far greater risk of inappropriate targeting on the basis of political views, as the Occupy episode illustrates.[135] This risk exists no matter whether the records reveal deep or shallow forms of privacy. Indeed, the risk seems greatest regarding shallow forms of privacy, for these are the contexts of sharing that are necessary for political association, the very contexts that a stultifying police state undermines, as Václav Havel's commentary illustrates.[136]

The standard for access to third party records thus varies based on the protected liberties impacted by the nature of the use and its relevance to legitimate justifications for law enforcement access. Targeting individuals for enforcement of traffic laws or public order should not require access to

133. *Alabama ex rel. Patterson*, 357 U.S. at 463.

134. By considering how the use of information impacts the privacy of persons, this approach harmonizes with the quantitative privacy approach, which, in determining whether police access constitutes a Fourth Amendment search, asks "[w]hether those technologies have the capacity to facilitate the sorts of broad programs of indiscriminate surveillance that raise constitutional concerns about a surveillance state." Gray & Citron, *supra* note 52, at 126.

135. As Professor Simitis argues, "Neither freedom of speech nor freedom of association nor freedom of assembly can be fully exercised as long as it remains uncertain whether, under what circumstances, and for what purposes, personal information is collected and processed." Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 734 (1987).

136. HAVEL, *supra* note 12, at 120.

third party records of internet usage, social media content, or even cell-cite information. And targeting individuals for their political activities already violates their First Amendment rights.[137] Lowered standards, such as relevance to an investigation, do not afford the protections against roving, barely fettered surveillance of groups and individuals—including their transactions, associations, and liberties—that risks altering and harming the ubiquity of privacy. While awaiting Supreme Court recognition that unconstrained access to third party records renders persons insecure in their political liberty, legislatures have independent authority to protect privacy's ubiquity as a constitutional value. In this way, the ABA Standards could be understood to invite new constitutional understandings through legislative means in advance of judicial pronouncements. Constitutional meanings need not await judicial determinations in order to put them into legal practice.

Limiting access to the ubiquity of electronic records of persons' social and political interactions with others increases the risk of potential disorderly conduct or other minor, and politically motivated, civil disobedient behavior going undetected. It may even increase the risk of missing the mosaic of information that might identify a potential violent offender in advance of his crime. Law enforcement combined with counter-terrorism efforts synthesize information through regional fusion centers in part on a theory that somewhere in the vast amount of transactional data about individuals is the clue to the next major terrorist attack.[138] But this is the price a free political society should be willing to pay in order to guarantee that the processes of deliberative self-determination will be

137. *See, e.g.*, Texas v. Johnson, 491 U.S. 397, 414 (1989) ("If there is a bedrock principle underlying the First Amendment, it is that the government may not prohibit the expression of an idea simply because society finds the idea itself offensive or disagreeable.").

138. *See* Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1443 (2011); David E. Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628, 650 (2005). Technological capacity enables this "mosaic approach" and official risk-aversion of another attack motivates it, as President Obama explained: "[T]he combination of increased digital information and powerful supercomputers offers intelligence agencies the possibility of sifting through massive amounts of bulk data to identify patterns or pursue leads that may thwart impending threats." President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence. However, "the men and women at the NSA know that if another 9/11 or massive cyber-attack occurs, they will be asked, by Congress and the media, why they failed to connect the dots." *Id.*

"uninhibited, robust, and wide-open."[139] Placing the burden otherwise creates an unjustified risk of suppressing political speech that in turn diminishes the legitimacy and efficacy of democratic self-governance.[140] In this way, legislative standards can lead constitutional doctrine to develop a broader, diachronic justificatory framework for analyzing police searches.

Political speech and association begins with the ubiquity of privacy. Our private thoughts, which Justice Brandeis called the "freedom to think as you will,"[141] are intertwined with our public speech through which we engage in critical thinking and opinion formation.[142] Therefore, when the state interferes with the processes of belief formation, it undermines the integrity of First Amendment protected activities.

In this way, the boundaries of Fourth Amendment jurisprudence shape the efficacy of First Amendment activities.[143] This relation has been recognized by members of the Court, both past and present. Justice Sotomayor takes up the claim Justice Douglas repeated to no avail in a prior era, noting in *United States v. Jones* that "[a]wareness that the Government may be watching chills associational and expressive freedoms."[144] Moreover, pervasive surveillance may "alter the relationship between citizen and government in a way that is inimical to democratic society."[145]

---

139. New York Times Co. v. Sullivan, 376 U.S. 254, 270 (1964).

140. Such a doctrinal approach would be in tension with law enforcement tendencies to view political movements and activities with criminal suspicion. An earlier era of law enforcement abuses were examined by the Church Committee and led to some legal reform. *See* S. REP. 94-755 (1976). The tendencies, however, appear to be unreformed, as evidenced by investigations of the Occupy Wall Street protesters. *See* Moynihan, *supra* note 113, at A17.

141. Whitney v. California, 274 U.S. 357, 375 (1927) (Brandeis, J., concurring), *overruled in part by* Brandenburg v. Ohio, 395 U.S. 444 (1969).

142. *See generally* Seana Valentine Shiffrin, *A Thinker-Based Approach to Freedom of Speech*, 27 CONST. COMMENT. 283 (2011).

143. The Fourth Amendment protects a broader conception of political liberty modeled on the liberty protected by due process in cases such as *Lawrence v. Texas*, 539 U.S. 558 (2003). In so doing, the Fourth Amendment can protect the interactions of persons in the public sphere. *See* Crocker, *Political Fourth Amendment*, *supra* note 39, at 307. The First and Fourth Amendments can be mutually informing in the other direction as well. *See, e.g.*, Marc Jonathan Blitz, Stanley *in Cyberspace: Why the Privacy Protection of the First Amendment Should Be More Like That of the Fourth*, 62 HASTINGS L. J. 357 (2010).

144. 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring); *see also* United States v. White, 401 U.S. 745, 762 (1971) (Douglas, J., dissenting); Osborn v. United States, 385 U.S. 323, 343 (1966) (Douglas, J., dissenting) (warning of "a society in which government may intrude into the secret regions of man's life at will").

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

As the Supreme Court colorfully put the point in *West Virginia State Board of Education v. Barnette*, "If there is any fixed star in our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion or force citizens to confess by word or act their faith therein."[146] But maintaining order in the public sphere through monitoring of third party records, if unchecked, fails to align the security and liberty protected by the Fourth Amendment with the freedom to speak protected by the First.[147] Political action is coordinated action. Under free speech principles, individuals must remain free to discuss the matters of critical importance as well as the frivolous, for social interactions and practices should determine prevailing viewpoints, not the local police officer or other "petty" official.[148] Dissent is only possible if privacy is protected—both deep and shallow in Havel's terms.[149]

In occupying social media by standing in the place of the third parties with whom we all share information as conditions of everyday life, local government administrators through their police can impose their own conception of proper social and political order. In order to forestall the use of traffic stops or arrests for "obstructing governmental administration" to impede free speech activities, courts and legislatures need to include contextual factors when considering the justification for police action. In doing so, they should raise the standard for access to third party records to a standard of probable cause when the targeted activities include core political speech—regardless of whether the content of the information

146. 319 U.S. 624, 642 (1943).

147. *See* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 143-45 (2007); *see also*, Danielle Keats Citron, *Fulfilling Government 2.0's Promise with Robust Privacy Protections*, 78 GEO. WASH. L. REV. 822, 829-39 (2010).

148. *See* Cohen v. California, 403 U.S. 15, 24-25 (1971) ("[T]he immediate consequence of this freedom may often appear to be only verbal tumult, discord, and even offensive utterance. These are, however, within established limits, in truth necessary side effects of the broader enduring values which the process of open debate permits us to achieve."); *see also* Owen M. Fiss, *Free Speech and Social Structure*, 71 IOWA L. REV. 1405, 1410 (1986); Alexander Meiklejohn, *The First Amendment Is an Absolute*, 1961 SUP. CT. REV. 245, 262.

149. *See* STEVEN H. SHIFFRIN, DISSENT, INJUSTICE, AND THE MEANINGS OF AMERICA 10 (1999) ("The First Amendment has a special regard for those who swim against the current, for those who would shake us to our foundations, for those who reject prevailing authority."); Thomas P. Crocker, *Displacing Dissent: The Role of "Place" in First Amendment Jurisprudence*, 75 FORDHAM L. REV. 2587, 2587 (2007); *see also*, Heather K. Gerken, *Dissenting by Deciding*, 57 STAN. L. REV. 1745 (2005).

gained from electronic records is classified as private to a high or low degree.

The First Amendment exemplifies this type of heightened scrutiny when the activities the state impacts are core political activities.[150] If government action burdens the expression of ideas because of its content, then it must meet the rigid standard of strict scrutiny.[151] Even general regulations that have non-content based, incidental burdens on free expression, such as regulations involving time, place, and manner restrictions, receive heightened scrutiny.[152]

Thus, the question is not simply whether the police are seeking evidence of a crime—no matter how minor or serious—but whether in seeking to investigate a crime by accessing third party records the police have a high risk of engaging in suppression of political speech.[153] By requiring a heightened showing of probable cause to believe a specific crime is being committed for which searching particular third party records is relevant, the police are foreclosed from using reasonable suspicion as a generalized warrant to examine claimed suspicious activity.[154] Patrolling streetscapes is

---

150. The Standards do a good job emphasizing the implications of records access for freedoms like speech and association, recognizing that "privacy is a critical component of many fundamental rights." STANDARD 25-3.3 commentary; *see also* Meyer v. Grant, 486 U.S. 414, 421 (1988) ("The First Amendment 'was fashioned to assure unfettered interchange of ideas for the bringing about of political and social changes desired by the people.'" (quoting Roth v. United States, 354 U.S. 476, 484 (1957))).

151. *See, e.g.*, Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Bd., 502 U.S. 105, 115 (1991); Police Dep't of Chi. v. Mosley, 408 U.S. 92, 95 (1972).

152. *See, e.g.*, Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989); Clark v. Cmty. for Creative Non-Violence, 468 U.S. 288, 293 (1984).

153. The issue here is not changing the level of justification needed to conduct searches based on the severity of the crime. Rather, the issue is raising the level of scrutiny when the more specific, constitutionally protected activities of speech and association are implicated by police access to "less private" social media and third party records. *Compare* Jeffrey Bellin, *Crime-Severity Distinctions and the Fourth Amendment: Reassessing Reasonableness in a Changing World*, 97 IOWA L. REV. 1 (2011) (arguing courts should consider the severity of a crime in determining if a search is reasonable), *with* Slobogin, *supra* note 55 (opining that severity analysis would backfire, resulting in less protection than the present).

154. A principal purpose of the Fourth Amendment is prohibiting general warrants, which British officers used against American colonialists. *See* Boyd v. United States, 116 U.S. 616, 630 (1886), *rejected by* Warden, Md. Penitentiary v. Hayden, 387 U.S. 294 (1967); *see also* NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 68-69 (1937); Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 562-70 (1999); William

not the same as patrolling cyberspaces. The digital stop and frisk is not the same as a sidewalk stop and frisk.

A necessary condition for the possibility of self-governance is the liberty to form a self through interactions with others. When police have access to those forms of sharing, unfettered from purposes carefully constrained by legitimate needs, there is a risk to both self and society.[155] Personal identity is often not about a self in isolation, for important aspects of our personal identities are formed through our associations. Thus, the intertwining of personal identity with others—our shared narratives—are vulnerable to pervasive surveillance. Whether policy makers use the classifications of high or low, deep or shallow, a conception of privacy protected from unconstrained police access is important to understanding why and how to construct such constraints.

Privacy's ubiquity therefore has two important aspects. One is the proliferation of shared information that reflects and enables the development of personal identity. The other is the multiple ways that acts of sharing are part of forming a political self, capable of exercising critical thought and fulfilled through forms of collective action in concert with others. In neither case is privacy a condition of nondisclosure, and in both cases privacy is a function of constitutional limitations on the domains in which government may intrude. In this way, expectations of privacy are not merely subjective or even social. They are political. Both aspects fall under the protection of the First Amendment. And each aspect has a strong basis for protection under the Fourth Amendment.

When a legislature considers the LEATPR recommendations, it does so against the background of the most salient constitutional and conceptual constraints on privacy. State constitutionalism can have a role to play in contributing to the legal protections afforded privacy. But it can do so only by recognizing how privacy is connected to other core constitutional values implicated by law enforcement access to third party records.

The temptation is to say that we have all already given up the game. That with all the social sharing in which many people engage, the time is already past to provide new protections for privacy. Moreover, despite the differences between cyberspaces and streetscapes, many people may be inclined to say that if a person reveals information to others, the police should not be disabled more than any other member of the public from

---

J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 396-411 (1995).

155. *See* Richards, *supra* note 25, at 1935.

gaining access to that information. These are contestable value judgments that depend on contestable conceptions of privacy—conceptions this article seeks to analyze through recognition of privacy's ubiquity in everyday life. Motivation to adopt new frameworks for protecting privacy as modeled by the LEATPR Standards requires adopting attitudes and perspectives informed by such recognition.

IV. Conclusion

By creating a framework for protecting against unregulated law enforcement access to third party records, policy makers can begin to make privacy more than the occasional value to which courts gesture when claiming to balance liberty against the security needs of police.[156] Because privacy as a form of sharing is a practice as ubiquitous as the third parties with whom we all share, how law conceptualizes privacy and its relation to third party records shapes the practices of privacy. Moreover, the role of third party records within the comprehensive pursuit of individual liberty, as Justice Brandeis eloquently described, is "that freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth; that without free speech and assembly discussion would be futile."[157] How we conceptualize privacy is also related to the law's frame of reference. Do legal doctrines seek to facilitate the needs of police or the protections of privacy? Only by prioritizing the latter can legal decision makers create effective constraints on law enforcement access to the growing body of third party records.[158] When social costs reemerge in the midst of thinking about how to protect a domain of privacy free from unconstrained law enforcement access, they do so at the behest of police, not personal privacy. Protecting privacy, by contrast, requires having at the forefront a model of privacy as an important aspect to a system of constitutionally protected liberties. In this way, how courts and legislatures

156. When purporting to balance liberties and security, "no one but a fool thinks that the threat from the state is zero." Jeremy Waldron, *Security and Liberty: The Image of Balance*, 11 J. POL. PHIL. 191, 208 (2003).

157. Whitney v. California, 274 U.S. 357, 375 (1927) (Brandeis, J., concurring), *overruled in part by* Brandenburg v. Ohio, 395 U.S. 444 (1969); *see also* Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) ("The makers of our Constitution . . . sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone -- the most comprehensive of rights, and the right most valued by civilized men."), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

158. *See* Crocker, *Political Fourth Amendment*, *supra* note 39, at 303.

understand the meanings and relations of Fourth and First Amendment rights shapes future application of those rights.[159] Courts and legislatures need the guidance that articulations of constitutional values provide. In the case of civil liberties, constitutional values are norms for the practice and protection of privacy's ubiquity.

Whether legislatures or courts take the lead, by making visible the core privacy values at stake, decisions about how to weigh and measure tradeoffs with order and security require consideration of the consequences for social practice and personal identity. When it comes to privacy's relation to association, speech, and everyday sharing, these values are easily overlooked because of their ubiquity. What is everywhere is difficult to see, for it lacks a discernible site on which to focus. The home has served this purpose for the Fourth Amendment, becoming the paradigm of space protected from the insecurity of unreasonable searches.[160] The ever-present privacy of our sharing as a condition of everyday life renders us vulnerable only to the degree that we fail to match the institutional pressures of policing with commitments to the constitutional values of liberty and privacy—in speech, association, and in the formation of our personal identities in pursuit of self-government.

159. *See* Crocker, *Constitutional Meanings*, *supra* note 72, at 688.

160. As the Court explains, "At the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion." Silverman v. United States, 365 U.S. 505, 511 (1961); *see also* Kyllo v. United States, 533 U.S. 27, 40 (2001); United States v. Karo, 468 U.S. 705, 716 (1984); Stephanie M. Stern, *The Inviolate Home: Housing Exceptionalism in the Fourth Amendment*, 95 CORNELL L. REV. 905, 912-13 (2010).