View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by University of Oklahoma College of Law

Oklahoma Law Review

Volume 66 | Number 4

Symposium: Law Enforcement Access to Third Party Records

2014

Third Party Records Protection on the Model of Heightened Scrutiny

Marc J. Blitz

Oklahoma City University, mblitz@okcu.edu

Follow this and additional works at: https://digitalcommons.law.ou.edu/olr

 Part of the Computer Law Commons, Fourth Amendment Commons, and the Internet Law Commons

Recommended Citation

Marc J. Blitz, *Third Party Records Protection on the Model of Heightened Scrutiny*, 66 OKLA. L. REV. 747 (2014).

This Introduction is brought to you for free and open access by University of Oklahoma College of Law Digital Commons. It has been accepted for inclusion in Oklahoma Law Review by an authorized editor of University of Oklahoma College of Law Digital Commons. For more information, please contact darinfox@ou.edu.

THIRD PARTY RECORDS PROTECTION ON THE MODEL OF HEIGHTENED SCRUTINY

MARC JONATHAN BLITZ*

Introduction

In his famous dissenting opinion in *Olmstead v. United States*, Justice Brandeis warned that as technology advanced, liberty would face new dangers never imagined by the Framers.[1] When the first Congress enacted the Fourth Amendment, for example, the chief bulwark against government spying lay in the sanctity of the home—and the Constitution's ban on entering it without a warrant.[2] By stopping officials from arbitrary "breaking and entry," the Fourth Amendment stopped them from gaining "possession of [a person's] papers and other articles incident to his private life."[3] But technology, wrote Brandeis, would likely provide government spies with another route into an individual's inner thoughts and intimate activities. "Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."[4]

Brandeis was, of course, correct. Secret papers are no longer confined to the interior of wooden or metal drawers. They now often take the form of electronic files that can be easily copied, transmitted, stored, or searched en masse.[5] And government officials who want a digital copy are not always

---

* Professor, Oklahoma City University School of Law; J.D. University of Chicago (2001); Ph.D. (Political Science) University of Chicago (2001), B.A. Harvard University (1989). Thanks to Professor Stephen Henderson for organizing this Symposium and to him, Professor Joseph Thai, and to my fellow Symposium participants—Thomas Crocker, Andrew Ferguson, Susan Freiwald, David Gray, Christopher Slobogin—for thought-provoking discussion about records privacy questions. I am also grateful to Ivaylo Lupov for valuable research assistance and the *Oklahoma Law Review* editors for valuable help in revising this article.

1. Olmstead v. United States, 277 U.S. 438, 472 (Brandeis, J., dissenting), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

2. U.S. CONST. amend. IV.

3. *Olmstead*, 277 U.S. at 473 (Brandeis, J., dissenting).

4. *Id.* at 474.

5. *See* ABA STANDARDS FOR CRIMINAL JUSTICE: LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS 2 (2013) [hereinafter LEATPR Standards] ("[W]ith the maturation of digital storage and search technologies, and virtually costless distributions, we now live in a world of ubiquitous third party information"); CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 3 (2007) (finding that

Published by University of Oklahoma College of Law Digital Commons, 2014

forced to obtain one from an individual's computer. They can often get the same information from the many third party entities with whom modern Americans constantly share such information: the companies that provide our cell phone service, Internet service, credit cards, or insurance policies.

Even where an individual does not consciously create a record of her preferences and minute-to-minute choices, an Internet or other technology company will often create such a record for her.[6] Electronic book companies, for example, keep detailed records of which books an individual reads, the pages she reads, passages she highlights in each book, and notes she records in the margin.[7] Music and Internet video companies can likewise generate detailed records of what television shows, movies, or other media content are watched or listened to on a particular computer—and for how long and how often.[8] In short, as Stephen Henderson writes, "[W]e now live in a world of ubiquitous third party information,"[9] embracing everything from our conversations with friends, to our encounters with books and other reading materials, to our commercial transactions.[10]

The challenge that this state of affairs creates for courts and lawmakers is even more difficult than Brandeis imagined. When Brandeis insisted the courts stand ready to protect the "secret drawers" in a person's home, he could insist that such legal protection be strong and unyielding. As English

---

records of transactions with hospitals, banks, stores, schools, and other institutions, usually found only in file cabinets until the 1980s, are now much more readily obtained with the advent of computers and the Internet). Individual Standards will be referred to using the format 'STANDARD x-x.'

6. *See* Sara M. Watson, *The Latest Smartphones Could Turn Us All into Activity Hackers*, WIRED (Oct. 10, 2013), http://www.wired.com/opinion/2013/10/the-trojan-horse-of-the-latest-iphone-with-the-m7-coprocessor-we-all-become-qs-activity-trackers/ (explaining how Apple SmartPhones might create records of activity the user is unaware that he or she is creating).

7. *See* NICOLE A. OZER & JENNIFER A. LYNCH, PROTECTING READER PRIVACY IN DIGITAL BOOKS 3 (2010).

8. *See* Andrew Leonard, *How Netflix Is Turning Viewers into Puppets*, SALON (Feb. 1, 2013), http://www.salon.com/2013/02/01/how_netflix_is_turning_viewers_into_puppets/ ("Net-flix doesn't know merely what we're watching, but when, where and with what kind of device we're watching. It keeps a record of every time we pause the action—or rewind, or fast-forward—and how many of us abandon a show entirely after watching for a few minutes."); *see also* Bill Brennar, *Spotify Is a Danger to Privacy Lovers and I Don't Care*, CSO ONLINE (Oct. 6, 2011), http://blogs.csoonline.com/1736/spotify_is_a_danger_to_privacy_lovers_and_i_dont_care.

9. Stephen E. Henderson, *After* United States v. Jones, *After the Fourth Amendment Third Party Doctrine*, 14 N.C. J. L. & TECH. 431, 435-36 (2013).

10. *Id.*

https://digitalcommons.law.ou.edu/olr/vol66/iss4/4

lawyers have insisted since before the founding of the American republic, a man's house is "his castle"[11] and a realm that must, in most cases, remain immune to government entry except where officials have a warrant supported by probable cause.[12] Such a legal barrier against official investigation cannot, however, plausibly encircle every one of the numerous records that modern individuals generate in their interactions with phone companies, financial entities, and other organizations.

Many such records form a critical part of law enforcement investigation[13]—often before police can obtain the probable cause they need to conduct more intrusive searches, such as the search of a home or a wiretap. Police may be tipped off to the possibility of criminal activity, for example, by an unusual pattern of travel movements or financial transactions.[14] If such information were as strongly walled off from police examination as the details of in-home activity, law enforcement investigations might rarely get off the ground. Fourth Amendment privacy protection accorded to the home tends to be invariable—treating "all details" as "intimate details."[15] By contrast, this probably cannot be true of the privacy protection that lawmakers give to diverse records of individual activity. Such records protection has to vary, based upon the types of records involved or on other circumstances that affect individuals' expectations about the records' privacy or their likely importance in law enforcement investigations.

Moreover, such a nuanced scheme for records privacy cannot be found in contemporary Fourth Amendment law. While the Court has squarely addressed the challenge of adapting the Fourth Amendment to

---

11. *See* Moore v. Madigan, 702 F.3d 933, 945 (7th Cir. 2012) (Williams, J., dissenting) (noting that the seventeenth century English jurist Lord Edward Coke explained that "a man's home was his castle"); Comer v. Warden, Ohio State Penitentiary, No. 2:13-CV-0003, 2013 WL 1721126, at *3 (S.D. Ohio Apr. 22, 2013) (noting that "[t]he maxim that a man's home is 'his castle' has deep roots in English law . . . [and] has long been a cherished part of American law").

12. *See* U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon probable cause . . . ."); Brigham City, Utah v. Stuart, 547 U.S. 398, 403 (2006) ("It is a 'basic principle of Fourth Amendment law that searches and seizures inside a home without a warrant are presumptively unreasonable.'" (quoting Groh v. Ramirez, 540 U.S. 551, 559 (2004))).

13. *See* STANDARD 25-3.2 commentary ("'[R]ecords searches'—in which law enforcement obtains evidence of crime via records maintained by institutional third parties—are surely one of the most important investigatory activities.").

14. *Id.*

15. Kyllo v. United States, 533 U.S. 27, 37 (2001) (emphasis omitted).

Published by University of Oklahoma College of Law Digital Commons, 2014

technological invasions of the home,[16] it has not taken the same approach to the challenge of protecting "secret papers" generated and stored outside the home. Rather, under its "third party doctrine," the Court has found that when we share records with third parties, we "assume the risk" those records might then be passed onto government officials (whether voluntarily or in response to a subpoena).[17] In short, under the third party doctrine, government is not barred by the Fourth Amendment from obtaining information we have put within its reach by sharing it with business entities (such as banks or phone companies).

Of course, legislators are free to fill the gap that the Court left in this aspect of its Fourth Amendment law—they *can* take up the challenge of protecting the records that the Court's Fourth Amendment law has left unprotected. If and when they do, they will find an invaluable template in the American Bar Association's new Standards for Law Enforcement Access to Third Party Records (LEATPR Standards). The centerpiece of these standards is a tiered system of privacy protection that directly addresses the complexity just discussed, whereby different records must be given distinctive levels of protection. In short, the LEATPR Standards advise that lawmakers should strive to categorize each set of records according to their "degree of privacy,"[18] classifying them as "highly private," "moderately private," "minimally private," or "not private."[19] Once a set of records receives a category designation, a corresponding level of protection then follows. Only records in the highest tier of privacy receive a level of protection akin to that which the Fourth Amendment establishes for wiretaps or searches of the home: namely, the requirement that police receive a court order based upon probable cause.[20] Access to moderately private records, by contrast, should require a court order based only upon reasonable suspicion (or in some cases, an even lower threshold of suspicion).[21] Minimally private records should be accessible to police

16. *See* Berger v. New York, 388 U.S. 41, 64 (1967) (Douglas, J., concurring) (noting that the majority opinion in *Berger* "overrules *sub silentio Olmstead v. United States,* and its offspring, and brings wiretapping and other electronic eavesdropping fully within the purview of the Fourth Amendment" (internal citations omitted)); *Kyllo*, 533 U.S. at 37.

17. *See* Smith v. Maryland, 442 U.S. 735, 744 (1976) (noting that telephone subscribers realize that the phone company has technology and reasons to record their calls); *see also* United States v. Miller, 425 U.S. 435, 443 (1976) (holding that a bank depositor could not expect that his financial records would retain their privacy once he shared them with a bank).

18. *See* LEATPR STANDARDS, *supra* note 5, at 10.

19. *Id.*; *see also* STANDARD 25-4.1; STANDARD 25-4.2 (emphasis omitted).

20. STANDARD 25-5.3.

21. *Id.*

https://digitalcommons.law.ou.edu/olr/vol66/iss4/4

without the approval of the courts at all, as long as a prosecutor or other agency official has some basis for believing the records have relevance to the law enforcement effort for which they are sought.[22] And records that are not private should be available at any time to police pursuing a "legitimate law enforcement purpose."[23]

This system has a number of advantages as a template for legislatures and agencies. By designing a system whereby law enforcement's path of least resistance leads them to initially non-private or minimally private records, the Standards help encourage law enforcement practices in which officials refrain (where possible) from too hastily intruding into records about the more intimate areas of life. They also provide guidance on how lawmakers should assign types of records to different tiers—about what factors might help them tell if a record should be classified as "highly" or "moderately" private and receive its attendant protections, or remain accessible to police even without a court order.

Here, however, the Standards meet the challenge of providing nuance, and do so too successfully. As the Standards themselves note, apart from a few paradigmatic cases of private information, such as medical records, "there are few bright lines in privacy."[24] Information that might seem "highly private" to one person, might seem "minimally private" to another—and while the Standards' factors provide a way to begin addressing the classification challenge in an orderly fashion, the same individuals who disagree in their intuitions about privacy are likely to differ in how they apply the factors, and with what results.

This article therefore proposes a rethinking of the Standards' set of factors. It proposes modeling it on another familiar framework which, like the Standards, aims at "striking" a "delicate balance" between government power and individual freedom[25]—between the need for government to regulate and the need for individuals to continue to have insulated spaces, in the midst of such regulation, in which they are largely free to organize their own lives in their own way. More specifically, the model that strikes this balance in constitutional law consists of requiring the government to meet tiers of scrutiny—"strict scrutiny" where the individual liberty interest is strongest, "minimal scrutiny" (or "rational basis") where it is weakest and the government therefore most free to regulate, and "intermediate scrutiny" for the territory in between where the need for liberty and the need for

22. *Id.*
23. *Id.*
24. STANDARD 25-4.1 commentary.
25. United States v. Stevens, 533 F.3d 218, 247 (3d Cir. 2008) (Cowen, J., dissenting).

Published by University of Oklahoma College of Law Digital Commons, 2014

regulation are of comparable strength (or the balance is, at least initially, largely unclear).[26]

In some respects, the Standards' own system of tiers closely resembles the courts' system of tiers for protecting liberties in constitutional law. However, there are important differences, and my central thesis in this article is that, while the Standards cannot and should not simply adopt the constitutional scrutiny unchanged, or simply substitute it for their own (justifiable) category choices, they can benefit by borrowing from the scrutiny-based system in certain ways.

One respect in which heightened scrutiny provides a model is that courts do not, as a general matter, use a complex multifactor test to divide the realm of strict scrutiny from that of intermediate and minimal scrutiny.[27] The dividing lines, while in some cases certainly contestable, are clearer than that. They cannot be identical to the lines that divide up our informational lives, but they can provide a model.[28] We might, for example, begin in privacy law as courts do in cases applying judicial scrutiny to laws limiting individual liberties, by most strongly insulating the realms of life over which the government has the least business exercising control—the realms where we form or exchange our opinions and where we engage in intimate activities. Traditions and norms of privacy may then move these initial lines—giving the government greater power to monitor realms of communication, and perhaps lesser power, in some cases, to regulate the financial or physical realm where government normally has a greater role to play in assuring safety and market fairness. But the starting point, at least, is clearer than a set of factors that different audiences will interpret in very different ways.

There is also a second benefit to treating heightened scrutiny as a model: not only would it help legislators, courts, and agencies to better apply the Standards' tiers of privacy, it would also help lawmakers to refine—and make more practicable—the corresponding tiers of protection. The Standards currently take account of this law enforcement interest chiefly by making it clear that officials *are able to* gain access to records of any kind, as long as they meet whatever standard of suspicion corresponds to the records' privacy: probable cause for highly private records, reasonable

26. *See generally* 1 WILLIAM J. RICH, MODERN CONSTITUTIONAL LAW § 11:3 (3d ed. 2013).

27. *See infra* notes 130-133 and accompanying text.

28. *See infra* Part II.

https://digitalcommons.law.ou.edu/olr/vol66/iss4/4

suspicion for moderately protected records, relevance for minimally private records, and no burden at all for records that are not private.[29]

These four tiers of protection, taken alone, however, do not take adequate account of the possibility that law enforcement may sometimes need to obtain even highly or moderately private information more easily than the Standards permit. So the Standards also suggest, at various points, that the hurdles facing law enforcement may be lowered even further. They may be lowered, for example, to meet an emergency,[30] or, more generally, in any situation where the burden imposed by their multi-tier privacy protection system "would render law enforcement unable to solve or prevent an unacceptable amount of otherwise solvable or preventable crime."[31]

But such a provision offers little guidance. It simply emphasizes that there may be times when legislators will be reasonable in setting aside the guidance given in the Standards' multi-tier protection system. While it is probably impossible to completely specify ahead of time exactly when and where law enforcement will face challenges that require faster and more data analysis than the Standards allow, it is better to try to identify and more carefully define those circumstances, instead of simply including a general escape hatch that may well grow into an exception that swallows the Standards' earlier rules.

Again, the model of heightened scrutiny suggests a valuable corrective. Under strict scrutiny in First Amendment cases, for example, even where government has a sufficiently compelling need to limit speech, it must still adopt a "narrowly tailored" means of imposing such a limit.[32] Applied to the realm of records protection, such a model would require not only that law enforcement show that they have a genuine need for quick access to certain records, but that they will satisfy this need in a way that avoids unnecessary damage to individuals' privacy interests.

Part I elaborates on the value of the four-tier privacy categorization scheme in the LEATPR. While some are likely to criticize these Standards as being insufficiently nuanced, this Part argues that simplification in this case is probably valuable and unavoidable. Part II next draws on First Amendment law and other areas where the court uses heightened scrutiny

29. STANDARD 25-5.3.

30. STANDARD 25-5.4.

31. STANDARD 25-4.2.

32. *See, e.g.*, Ariz. Free Enter. Club's Freedom PAC v. Bennett, 131 S. Ct. 2806, 2817 (2011) (noting that laws burdening political speech must not only meet a compelling interest but also must be "narrowly tailored" to achieve that interest).

Published by University of Oklahoma College of Law Digital Commons, 2014

to rethink the Standards' four-factor analysis for assigning types of records to tiers of privacy. Part III then turns from the Standards' tiers of privacy to its tiers of protection. This part examines how this system of protection might be refined by incorporating elements of the scrutiny-based classification scheme one finds in First Amendment case law, and its similarity with the minimization requirements (or factors) one finds respectively in wiretapping and special needs jurisprudence.

I. Tiers of Privacy and the Need for Simplification

Any attempt to divide our activities into four tiers of privacy will inevitably simplify a complex world. Individuals' intuitions about degrees of privacy will often be more nuanced, allowing them, for example, to find some "moderately private" records more sensitive (and potentially embarrassing) than other "moderately private" records. Moreover, different individuals will sometimes have starkly different judgments about what kinds of activities are private. This is clear in the fact that while some people are outraged when computer applications broadcast their music or reading choices to the world, others are happy to let Facebook tell their friends (and perhaps others) about every song they listen to and every newspaper article they read.[33]

The simplification inherent in the Standards' tiers of privacy is thus likely to be targeted by some critics of the Standards. But I want to begin this article's analysis by explaining why, on the whole, such simplification is not only justified but also probably necessary.

First, law is filled with categorization schemes that necessarily sacrifice some of life's complexity in order to provide judges with administrable rules and make it more likely that the rules will be applied predictably and consistently. Consider, for example, two areas of constitutional law where courts have opted to adopt a three- or two-tier scheme instead of trying to place a person's liberty or equality interests along a precise point on a flowing continuum. I have already mentioned one of these above: the tradition of subjecting government measures that implicate certain First or Fourteenth Amendment rights to strict, intermediate, or minimal scrutiny. For example, in Equal Protection contexts, the Court subjects government classifications based on race or ethnicity to strict scrutiny,[34] classifications

33. *See* Danah Boyd & Eszter Hargittai, *Facebook Privacy Settings: Who Cares?*, FIRST MONDAY (Aug. 2, 2010), http://firstmonday.org/article/view/3086/2589.

34. *See, e.g.*, Grutter v. Bollinger, 539 U.S. 306, 308 (2003) ("All government racial classifications must be analyzed by a reviewing court under strict scrutiny."); Regents of

https://digitalcommons.law.ou.edu/olr/vol66/iss4/4

based on gender or illegitimacy to intermediate scrutiny,[35] and other classifications to minimal scrutiny.[36] Strict scrutiny is the most demanding, permitting government regulation of a subject only where it can show its restriction is "necessary" and "narrowly tailored to serve a compelling government interest."[37] Intermediate scrutiny is somewhat more permissive, allowing regulation even if the government's interest is "important" or "significant" rather than a "compelling" interest of the highest order, and also allowing a less than perfect fit between the government's goal and the means it uses to achieve it.[38] It requires only a "substantial" relationship between the two.[39] Finally, minimal scrutiny—or "rational basis"—is the most permissible of the three and leaves the government with plenty of leeway to regulate, allowing it to do so whenever it has any "legitimate governmental objective," even a minor one, and uses means "rationally related" to that objective, even if the government regulates far more then necessary.[40]

In adhering to this three-tier scheme, the Court has rejected occasional calls for a more nuanced approach—among them Justice Stevens' claim

---

Univ. of Cal. v. Bakke, 438 U.S. 265, 291 (1978) ("Racial and ethnic distinctions of any sort are inherently suspect and thus call for the most exacting judicial examination.").

35. *See* Craig v. Boren, 429 U.S. 190, 197 (1976) ("[C]lassifications by gender must serve important governmental objectives and must be substantially related to achievement of those objectives."); *see also* J. Harvie Wilkinson III, *The Dual Lives of Rights: The Rhetoric and Practice of Rights in America*, 98 CALIF. L. REV. 277, 296 n.119 (2010) (collecting cases).

36. *See, e.g.*, Phila. Police & Fire Ass'n for Handicapped Children, Inc. v. City of Phila., 874 F.2d 156, 163 (3d Cir. 1989) (stating that the "general rule" in Equal Protection Clause analysis is that—except for a few types of government classifications, such as those based on race or gender—classifications receive only "minimal scrutiny").

37. *See* Fisher v. Univ. of Texas at Austin, 133 S. Ct. 2411, 2422 (2013) (Thomas, J., concurring) ("Under strict scrutiny, all racial classifications are categorically prohibited unless they are 'necessary to further a compelling governmental interest' and 'narrowly tailored to that end.'" (quoting Johnson v. California, 543 U.S. 499, 514 (2005))); *Bakke*, 438 U.S. at 299 (stating that, where government is permitted to impose a burden on the individual under strict scrutiny, the burden must be "precisely tailored to serve a compelling governmental interest").

38. *See Craig*, 429 U.S. at 197 ("[C]lassifications by gender must serve important governmental objectives and must be substantially related to achievement of those objectives."); Wilkinson, *supra* note 35, at 296 n.119 (noting that use of such classifications involves application of "intermediate scrutiny").

39. *Craig*, 429 U.S. at 197.

40. *See, e.g.*, Dunagin v. City of Oxford, Miss., 718 F.2d 738, 753 (5th Cir. 1983) (holding that under "minimal scrutiny. . . . the classification challenged need only be rationally related to a legitimate state interest").

Published by University of Oklahoma College of Law Digital Commons, 2014

that the Court should acknowledge that its Equal Protection cases "reflect a continuum of judgmental responses to differing classifications which have been explained in opinions by terms ranging from 'strict scrutiny' at one extreme to 'rational basis' at the other,"[41] and Justice Marshall's call for a sliding scale approach which likewise varies according to the "constitutional and societal importance of the interest adversely affected and the recognized invidiousness of the basis upon which the particular classification is drawn."[42]

In the First Amendment context, the Court has likewise opted for categories instead of continua in public forum doctrine, the strand of free speech law that bars government from silencing speakers indirectly by driving them out of streets, parks, or other public space.[43] To be sure, the courts cannot simply prevent government from regulating public space. Such regulation is necessary to control traffic, protect the environment, and accomplish numerous other tasks. So the Court has, under "public forum" doctrine, divided public space into "public forums," (e.g., streets and parks) where government's interests in regulation must often be trumped by speakers' interests in free and robust communication,[44] and "non-public forums,"(e.g., airports) where other public interests, like the need for safe and efficient air travel, trump speakers' freedom.[45]

Like the three tiers of scrutiny, the simple categorization in forum analysis has been challenged.[46] Indeed, before settling into the modern

41. City of Cleburne, Tex. v. Cleburne Living Ctr., 473 U.S. 432, 451 (1985) (Stevens, J., concurring).

42. San Antonio Indep. Sch. Dist. v. Rodriguez, 411 U.S. 1, 99 (1973) (Marshall, J., dissenting).

43. *See, e.g.*, Sullivan v. City of Augusta, 511 F.3d 16, 46 (1st Cir. 2007) (Lipez, J., dissenting) (noting that "access to public spaces to speak on matters of public concern has long been a concomitant privilege of the right of expression" and this right has included the right of speakers to use "streets and other public places").

44. *See* Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 45-46 (1983) (describing the different types of forums).

45. Lee v. Int'l Soc'y for Krishna Consciousness, Inc., 505 U.S. 672, 679 (1992) (describing the different categories of forums and concluding that airport terminals "are nonpublic fora"); Cornelius v. NAACP Legal Def. & Educ. Fund, 473 U.S. 788, 802 (1985) (describing the features of different types of forums and finding a fundraiser for federal employees to be non-public).

46. *See, e.g.*, ROBERT C. POST, CONSTITUTIONAL DOMAINS: DEMOCRACY, COMMUNITY, MANAGEMENT 199 (1995) (stating that public forum doctrine prevents "sensitive First Amendment analysis"); Daniel A. Farber & John E. Nowak, *The Misleading Nature of Public Forum Analysis: Content and Context in First Amendment Adjudication*, 70 VA. L. REV. 1219 (1984).

https://digitalcommons.law.ou.edu/olr/vol66/iss4/4

public forum approach, the Court hinted it might approach such issues by simply performing a particularized contextual analysis of each public space in which the government regulated speech: in each case, it would look at "[t]he nature of a place" and "the pattern of its normal activities" and ask whether the speech restricted by the government was "incompatible with the normal activity of a particular place."[47] Instead of this highly contextualized inquiry, however, the Court opted to simplify matters. It categorized public space into two major types—and accorded different levels of protection to each type. In public forums, speakers' interests in use of public space received extraordinary protection. By contrast, in non-public forums, speech interests were subordinated to other public needs.

As I have pointed out elsewhere,[48] one finds a similar simplification in the way that current Fourth Amendment law treats the home as opposed to public space. The home receives extraordinary protection. Police need a warrant based on probable cause to enter and observe—and this is true even when the in-home activity they observe is not particularly private. As the Supreme Court stated in *Kyllo*, an officer needs to meet this high standard even when he "barely cracks open the front door and sees nothing but the nonintimate rug on the vestibule floor."[49] By contrast, police are free to observe intimate behavior when it takes place in a public setting. Police might watch, for example, as somebody enters a psychologist's or psychiatrist's office, presumably to inquire about setting up or attending a medical appointment.[50]

So, perhaps, the same kind of approach makes sense in the context of public records. After all, we certainly have some powerful intuitions that certain records are more private than others. As the Standards Commentary notes, for example, most people would agree that health records are more sensitive and merit more protection than utility records.[51] Moreover, just as public forum doctrine deals with competing public interests—in robust speech, on the one hand, and in other uses of public space, on the other—a four-level classification of records' privacy might be seen as dividing the

47. Grayned v. City of Rockford, 408 U.S. 104, 116 (1972).

48. *See* Marc Jonathan Blitz, *The Fourth Amendment Future of Public Surveillance Remote Recording and Other Searches in Public Space*, 63 AM. U. L. REV. 21, 41-43 (2013).

49. Kyllo v. United States, 533 U.S. 27, 37 (2001).

50. *See* Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World That Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1357-58 (2004) (noting that "[a] person usually cannot enter a psychiatrist's office, marriage counseling center, or infertility clinic except from a public street").

51. STANDARD 25-4.1 commentary.

Published by University of Oklahoma College of Law Digital Commons, 2014

realm of information into different "territories," in some of which individuals' interest in free and unmonitored exploration is paramount, and in others where law enforcement interests in vigorously finding, and following, leads is given more weight.

Moreover, while this article later raises some concerns about the Standards' proposed factors for assigning categories to each type of records,[52] certain elements of the proposed factors would move records laws in the right direction. More specifically, some of these factors help assure that this division of records into "territories" with different levels of privacy is not simply an arbitrary one. For example, the Standards are certainly right that privacy becomes more critical when it provides crucial support for an individual's ability to engage in "freedom of speech and association."[53] Where the integrity of certain records is essential to free and spontaneous discussion or intellectual exploration, then there is a case to be made that these are records where protection of privacy becomes more crucial. This is an argument I have made in an earlier work on the privacy of library or Internet activity.[54]

It has also received significant discussion in the work of Professor Julie Cohen and Professor Neil Richards. As Cohen writes, "[C]ompelled disclosure of information about intellectual consumption threaten[s] rights of personal integrity and self-definition in subtle but powerful ways . . . [because] fine-grained observation subtly shapes behavior, expression, and ultimately identity."[55] Richards writes,

> [W]hen the government is listening to our phone calls or businesses are tracking and analyzing what we read, these activities menace our processes of cognition and our freedoms of thought and speech. If we are interested in a free and robust *public* debate we must safeguard its wellspring of *private* intellectual activity.[56]

In the twentieth century, such intellectual privacy was largely achieved in a manner akin to public forum doctrine: by giving individuals an institutional space—namely, the public library—where strong privacy

52. *See infra* Part III.

53. STANDARD 25-4.1(a).

54. *See* Marc Jonathan Blitz, *Constitutional Safeguards for Silent Experiments in Living: Libraries, the Right to Read, and a First Amendment Theory for an Unaccompanied Right to Receive Information*, 74 UMKC L. REV. 799 (2006).

55. Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 577 (2003).

56. Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 391 (2008).

https://digitalcommons.law.ou.edu/olr/vol66/iss4/4

norms allowed them to access all manner of reading materials free from external observation.[57] As BJ Ard writes, the rise of the Internet and digital reading have undermined this institutional actor-based privacy regime.[58] Intellectual privacy in the modern age, he argues, thus requires privacy protection that applies not just to particular actors (like libraries) but to reading records with particular content.[59] In other words, intellectual privacy now requires the type of third party protection that the Standards advocate. In fact, the emphasis that the Standards' first factor places on free speech and association in some respects carves up the world of private information enclaves in a way that is parallel—in both form and purpose—to the way that public forum doctrine carves up shared public spaces. Public forums such as parks and streets are set aside for robust debate and communication of private ideas. They are places where certain other public interests (such as interests in noise and pollution control) must therefore take a "back seat" to speech interests. In the law of records protection, certain channels of informational activity are likewise crucial for another part of the speech process—namely the private reflection upon, and forging of, new ideas—and so these too are realms where certain interests, such as the interest in crime investigations, must be limited enough to leave space for intellectual freedom.

The other factors offered by the Standards likewise provide sensible guidelines for marking off certain informational realms as zones of heightened privacy. Health records, for example, are not by and large records of our intellectual activity: a record indicating that a medical visit revealed a heart condition, for example, does not divulge confidential thoughts or communications. But there are other reasons for treating such records as "highly private" because while their release might not chill intellectual exploration or private conversation, it might well do another kind of harm. In the words of the factors used by the Standards, it might cause "embarrassment" or "stigma" if released to others in the person's

57. *See* Blitz, *supra* note 54, at 805-07. The protection that the First Amendment provides for the privacy of one's home has also provided space for intellectual freedom. As the Supreme Court wrote in *Stanley v. Georgia*, under the First Amendment the "State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch." 394 U.S. 557, 565 (1969).

58. BJ Ard, *Confidentiality and the Problem of Third Parties: Protecting Reader Privacy in the Age of Intermediaries*, 16 YALE J.L. & TECH. 1, 30-45 (2013).

59. *Id.* at 46.

Published by University of Oklahoma College of Law Digital Commons, 2014

community—and may also have other negative consequences (such as loss of a job).[60]

To be sure, legislators who simplify the world by artificially dividing it into three or four categories should take careful account of what they sacrifice in doing so. In the case of personal records, one might well find numerous counterexamples to any classification that a legislature proposes. As the Standards note, the "content of communications" in phone conversations and e-mails is almost certainly a paradigmatic example of "highly private" information.[61] But anyone can probably remember numerous phone conversations and e-mail exchanges that lacked any sensitive details—whether it is small talk with a relative or colleague revealing nothing of interest about a person's life, or a call to a coffee shop or Department Store to confirm the hours it will open. One can likewise identify certain minimally private records within the generally private realm of personal health information. People are generally less guarded about a thumb injury than about a serious illness. Moreover, not only do certain communications and health records present counterexamples, but certain individuals do as well. While some people may be horrified at the thought of alerting strangers to a cancer diagnosis, others may blog about it on a public website.[62]

None of these examples, however, seriously undermines the Standards' classification scheme. In the first place, there is no plausible way for a legal protection scheme to capture every nuance in individuals' expectations about privacy protection. Moreover, this kind of simplification is often necessary to give people some control over what they choose to keep private. People are free, for example, to fill their protected communication space with non-private conversation, and often do. But high levels of protection at least preserve their option to use it for confidential communications. In this respect, the records classification scheme resembles First Amendment public forum jurisprudence. Public forum doctrine allows individuals to use parks or streets for numerous activities far more mundane than political debates or religious proselytizing (such as organizing and playing a game of Frisbee) but always leaves them with the possibility of having some space from which they can preach to the

60. STANDARD 25-4.1(b).

61. STANDARD 25-4.1(a) commentary.

62. *See* Eliza Barclay, *Why More Patients Should Blog About Illness and Death*, NPR (Mar. 28. 2013), http://www.npr.org/blogs/health/2013/03/26/175383540/why-more-patients-should-blog-about-illness-and-death (noting that "while many illness blogs are read only by friends and family, some patients go more public with their stories").

https://digitalcommons.law.ou.edu/olr/vol66/iss4/4

world about their political or religious beliefs or about other topics on which they wish to communicate with the public.[63]

If the Standards have a problem, then, it is not that they divide up the realm of our personal information in a way that entails some simplification, but rather in how such a necessary simplification is carried out and what happens *after* such a division of our informational space is made, when specific protection mechanisms are put in place for each tier. I will elaborate upon each of these issues in turn.

II. Rethinking the Factors for Setting Privacy Levels

As teachers at all levels realize, it is often less challenging to come up with a general grading system (e.g., assigning students an "A","B", "C", "D", or "F") than it is to figure out which essay deserves which grade. The same is true here. While some may push for more complexity and nuance in records' classification, and perhaps for giving courts a freer hand to assign records a particular privacy "value," the Standards can and do make a strong case for a tier-based system of records classification that runs from "not private" at the bottom of the list to "highly private" at the top. As the Standards Commentary recognizes, however, "while people typically agree on the extremes . . . there are few bright lines in privacy, and there will be reasoned disagreement in many cases."[64]

To help lawmakers and others tackle this disagreement—and perhaps, their own uncertainty—in an orderly fashion, the Standards propose the factors discussed above, drawing heavily upon the past privacy law cases, legislative judgments, and scholarly contributions. It is helpful, at this juncture, to state them fully in the Standards' own language. Under Standard 4.1, when deciding whether

> information maintained by third parties . . . [is] highly private, moderately private, minimally private, or not private, a legislature, court, or administrative agency should consider present and developing technology and the extent to which:
>
> (a) the initial transfer of such information to an institutional third party is reasonably necessary to participate meaningfully in

63. *Cf.* Christian Legal Soc'y Chapter of the Univ. of Cal., Hastings Coll. of the Law v. Martinez, 130 S. Ct. 2971, 2989 n.17 (2010) (finding law school's nondiscrimination policy for student organizations, including both religious and Frisbee clubs, followed applicable limited public forum precedents).

64. STANDARD 25-4.1 commentary.

Published by University of Oklahoma College of Law Digital Commons, 2014

> society or in commerce, or is socially beneficial, including to freedom of speech and association;
>
> (b) such information is personal, including the extent to which it is intimate and likely to cause embarrassment or stigma if disclosed, and whether outside of the initial transfer to an institutional third party it is typically disclosed only within one's close social network, if at all;
>
> (c) such information is accessible to and accessed by non-government persons outside the institutional third party; and
>
> (d) existing law, including the law of privilege, restricts or allows access to and dissemination of such information or of comparable information.[65]

These factors capture a number of important insights and intuitions about the values that underlie protection of third party information. But like many other factor-based tests, they risk leaving lawmakers, courts, and agencies with too little guidance to generate administrable and consistent legal frameworks. Different lawmakers may well give different weight to different factors. Indeed, the first two factors above seem to add to this complexity and unpredictability because each of them is more accurately understood as a package of factors than a discrete and focused concern. Factor (a) asks lawmakers to determine (1) whether the information at issue is the kind that individuals are compelled to share in order to participate in modern life, (2) whether, even if individuals are free to avoid such sharing, its dissemination would undermine some social benefit, and (3) whether such benefits are not merely social benefits, but the safeguarding of First Amendment freedoms that, unlike other social benefits, the Constitution places beyond democratic majorities' capacity to trade for other benefits.[66] For some transfers of information, such as telephone conversations, the answer to all three of these questions might be "yes."[67] But it is also true that, of the activities required for meaningful participation in life, some are more beneficial than others, and not all of them might play a significant role in speech or other First Amendment activity.

---

65. STANDARD 25-4.1(a) to -4.1(d).

66. STANDARD 25-4.1(a).

67. STANDARD 25-4.1(a) commentary (noting that telephone conversations, as well as e-mail and other electronic communications, further "the freedoms of expression and association" and are "necessary to participate meaningfully in society and in commerce").

https://digitalcommons.law.ou.edu/olr/vol66/iss4/4

Factor (b) likewise asks both (1) whether the information is intimate information of a sort that will cause emotional shame if released, or (2) whether it should be considered "personal" simply because individuals' existing practice tends to show that people tend to treat it as such, and avoid sharing it, whether because they fear its release will cause shame and stigma, or for some completely different reason.[68]

The upshot of these factors' complexity is that the order and predictability that the Standards promise with one hand, they at least begin to retract with the other: They offer an overarching four-tier system for classifying records' privacy level but then make the tier designation for each record depend on a highly contextual factor-based analysis, the result of which is likely to vary depending on who is applying it. While no legal framework can avoid some unpredictability in its application, one of the major reasons that certain judges prefer systems of legal categories rather than fine-grained contextual judgments is that such systems are more likely to resist reasoning that is arbitrary, idiosyncratic, or result-oriented. Consider again First Amendment public forum doctrine: One of the reasons the Court has adhered to it despite calls for nuance is to keep constitutional rules from being too easily bent or redefined to accommodate discomfort with their implications. As Justice Kennedy said in a 1996 case, a more rule-like approach to the law forces justices to adhere to a rule provided "in advance" regarding a law's constitutional validity "rather than letting the height of the bar be determined by the apparent exigencies of the day."[69] Such a system also provides "notice and fair warning to those who must predict how the courts will respond to attempts to suppress their speech."[70] As Justice Souter agreed in the same case, "Reviewing speech regulations under fairly strict categorical rules keeps the starch in the standards for those moments when the daily politics cries loudest for limiting what may be said."[71] This doesn't mean that such strict categorical rules are always optimal. Perhaps they are less essential in legislation, which can always be amended, than in constitutional precedent, which legislators cannot override and judges are hesitant to overrule.

But if there is a way to help guarantee that the Standards' four-tier system can provide the order and predictability it promises, then it is worth

68. STANDARD 25-4.1(b).

69. Denver Area Educ. Telecomm. Consortium, Inc. v. FCC, 518 U.S. 727, 785 (1996) (Kennedy, J., concurring in part and dissenting in part).

70. *Id.*

71. *Id.* at 774 (Souter, J., concurring).

Published by University of Oklahoma College of Law Digital Commons, 2014

seeking. Here then is one attempt at simplifying the factors and at leaving them less of a Rorschach test than they otherwise might be.

The factors seem to be principally focused on counseling legislators to undertake two major efforts. One is to analyze and understand the gravity of the harms that flow from certain privacy violations. While the Standards do not provide a definitive assessment of which harms are the gravest, they give most sustained attention to the harms that threaten constitutional interests, such as free speech or the autonomy at the core of substantive due process. As factor (a) notes, government surveillance—and the risk of subsequent dissemination—of certain private communications may well discourage individuals from participating in modern society and commerce, and may even undercut the intellectual exploration, debate, and association that the First Amendment is meant to safeguard.[72] And as factor (b) notes, where information concerns intimate activity or is otherwise personal, its release can cause "embarrassment or stigma."[73] Standard 25-3.3 gives further emphasis to this concern, noting that the release of a recording can "chill freedoms of speech, association, and commerce; and deter individuals from seeking medical, emotional, physical or other assistance for themselves or others."[74]

Rather than simply counseling legislators to reflect generally upon the social costs (or foregone benefits) that may flow from a lessening of privacy and to weigh them as they see fit, a slightly amended framework might provide more guidance. It might ask that lawmakers adopt a presumption that, where the activity reflected in the information involves a sphere of activity protected by First Amendment or due process protections, such records should be classified as "highly private" or "moderately private," and that such a presumption should be set aside only when there are certain powerful reasons that cut the other way. A presumption in favor of privacy might be overridden, for example, by strong traditions or norms that treat such information as "non" or "minimally private," or concrete evidence that such a classification—and the burdens it imposes on police—would have grievous effects on their ability to fight crime.

Apart from concerns about privacy harms, the Standards' factor-based analysis also dwells (in at least three of the four factors) on a second concern: that legislators should strive to align their classifications with individuals' intuitions and society's norms about when and where privacy is

72. STANDARD 25-4.1(a).
73. STANDARD 25-4.1(b).
74. STANDARD 25-3.3.

https://digitalcommons.law.ou.edu/olr/vol66/iss4/4

most necessary. As the Standards Commentary emphasizes, a drafter of new records law is "not writing on a clean slate."[75] Rather, there are already social expectations, norms, and rules about privacy, and it makes sense to craft legal privacy protections that reflect these background understandings and previous privacy rules. This imperative is already built into the "*Katz*" test that courts use to determine what constitutes a search under the Fourth Amendment—wherein they classify as a search (and thus, subject to constitutional limits) any governmental investigatory technique that intrudes upon an "expectation of privacy . . . that society is prepared to recognize as reasonable."[76] Legislators should consider, says factor (b), whether people seem to treat information as "personal" in that they "typically disclos[e] [it] only within [their] close social network[s]."[77] They should also consider, under factor (c), whether information about a person is the kind that people already understand is frequently available to others.[78] And they should understand, as factor (d) makes clear, that evidence of existing privacy expectations is found not only in social norms and practices, but also in existing law, such as the law of privilege.[79] The Standards Commentary also points lawmakers to other evidence about intuitions, norms, and practices, such as the survey responses that Christopher Slobogin and Joel Schumacher obtained from Americans regarding how they would rank the intrusiveness of different kinds of government investigatory techniques.[80]

Of course, apart from examining existing norms, social practices, and laws, lawmakers also have to decide what to do with such an analysis: in many cases, the evidence is likely to be inconclusive. Different evidence will point in different directions. And in the case of new computer technologies, individuals may not yet have developed strong intuitions or social norms about its privacy.

One possibility is for lawmakers to adopt a default position that, in the absence of a clear answer, tilts the scales towards a higher or lower privacy level. There is at least one strong reason to tilt the scales in favor of lower

75. STANDARD 25-4.1(d) commentary.

76. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

77. STANDARD 25-4.1(b).

78. STANDARD 25-4.1(c).

79. STANDARD 25-4.1(d).

80. STANDARD 25-4.1(b) commentary (citing 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)).

Published by University of Oklahoma College of Law Digital Commons, 2014

privacy protection: a presumption the other way might leave law enforcement with little room for investigating third party information. This result seems plausible given that, in the discussion of the factors focused largely on possible harms (factors (a) and (b)), the Standards tentatively find that most of their examples are likely to count as highly or moderately private, at least insofar as that particular factor is concerned.[81] The content of individuals' phone and Internet communications is, of course, central to speech and central to meaningful participation in modern society. So, applying the first factor, the Standards find such content to be "more private."[82] They reach the same conclusion for "information relating to communication[]," "medical records," "utility consumption," "[f]inancial [a]ccount and [t]ransaction [r]ecords," IP address information and URLs, and (more tentatively), "Geographic Vicinity" records.[83]

The results are more mixed when the Standards' discussion moves to the second factor and looks at whether particular categories of records are "personal." They emphasize that "some information is more personal than other information."[84] And among their examples, utility records and IP address information appear to drop to the lower privacy tiers.[85] But here as well, most of their examples (e.g., communications content and metadata, financial transaction records, URL address information, and geographic vicinity information) can plausibly be categorized as personal and often seem to be regarded as such by survey respondents and others.[86] Some of these categories of records would likely be excluded from the highest rungs of the privacy classification under my own revised proposal. That proposal accords a presumption of high privacy only to information, the release of which would threaten autonomy interests related to free speech, intellectual exploration, medical treatment, intimate activity, or some other activity in the zones that our constitutional systems mark off as a realm of individual autonomy, therefore insulated against government control. Financial records may receive some privacy protection, for example, but it is less likely that their release would compromise core speech interests.

In any event, if a consideration of privacy harms tends to err on the side of placing third party records off-limits to police investigation—until they obtain a court order based on probable cause or reasonable suspicion—it

81. *See* STANDARD 25-4.1(a) commentary; STANDARD 25-4.1(b) commentary.
82. STANDARD 25-4.1(a) commentary.
83. *Id.*
84. STANDARD 25-4.1(b) commentary.
85. *Id.*
86. *See id.*

https://digitalcommons.law.ou.edu/olr/vol66/iss4/4

may not make sense for inconclusive analyses of social norms and intuition to err in the same direction. As the Standards note, "[R]ecords searches . . . are surely one of the most important investigatory activities, and have been for many years."[87] Phone and Internet records, bank records, and purchase records can often be essential to giving police a lead to find criminals who would otherwise evade justice, and "records access has the additional benefit of not risking a physical confrontation with the target."[88] Moreover, police need to have *some place* to begin an investigation.[89] In order to satisfy the probable cause or reasonable suspicion standard, there needs to be some information they can collect for that purpose beforehand.

Perhaps, then, where the privacy of third party information is *not* central to our exercise of speech or other First Amendment rights, and *not* central to the personal autonomy we exercise over our bodies and in our bedrooms, lawmakers should not rush to assume classify it has "highly private" where social norms and practice point only ambiguously or weakly in that direction.

To be sure, there are countervailing considerations. As Justice Brandeis wrote in *Olmstead* many years ago, even when an investigation is "in aid of law enforcement. . . . [our] experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent."[90] Such a consideration may favor erring on the side of keeping records private—and perhaps on the side of assuming that information should retain a higher level of privacy unless and until powerful evidence is produced showing that it should be "minimally private" or "not private." But given police's long-standing reliance on records investigations, and the importance such investigations have for law enforcement's success, legislators should be hesitant to apply—to *all* types of records—a presumption of high privacy. After all, when Brandeis wrote the above-quoted language, he was not focused on all methods of police investigation, but rather about wiretapping, searches of "secret papers," and other invasions of what he considered core Fourth Amendment liberties.[91]

A system that disables police—across all types and methods of surveillance—even when such core interests are not at stake, is unlikely to

87. STANDARD 25-3.2 commentary.

88. *Id.*

89. *See* Marc Jonathan Blitz, *The Fourth Amendment Future of Public Surveillance Remote Recording and Other Searches in Public Space*, 63 Am. U. L. REV. 21, 37 (2013).

90. Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

91. *Id.*

Published by University of Oklahoma College of Law Digital Commons, 2014

strike a "delicate" and correct balance between law enforcement interests and privacy.[92]

To summarize: I propose that the factor analysis might be simplified and that legislators should at least begin by considering (1) privacy harms and (2) existing social practices and laws. As they do so, they may adopt a presumption in favor of treating records related to core First Amendment or autonomy interests as "highly private" and another presumption that other records will be minimally private (and thus, accessible without a court order) unless there is strong evidence that individuals regard and treat information as moderately or highly private.

This proposal is certain to draw some objections—one of which is that it overlooks certain important elements of the Standards' proposed factors and too quickly subsumes others into the broad categories of "privacy harms" or "law, social norms, practices revealing privacy level," when there are good reasons to consider them independently.

Consider one aspect of the factors I did not discuss above: Apart from asking whether a records investigation would cause certain types of harms (e.g., constitutionally significant autonomy interests), the Standards' first factor also appears to have another important purpose. It aims to right one of the wrongs that scholarly commentators—and Supreme Court dissenters—have long found in the Court's doctrine. As explained earlier,[93] under this doctrine an individual has no constitutionally protected privacy interest against police investigation of information that she knowingly shared with third parties. More specifically, the Standards' first factor discourages lawmakers from adopting the mistaken assumption—often found in the third party cases[94]—that individuals can protect their privacy by simply keeping the information to themselves. As Stephen Henderson notes, when the Supreme Court insisted that depositors knowingly share information with their banks, the Court failed to take into account that "the

92. To be sure, computer technology may, in the future, provide us with an alternative way of marking the boundary between highly protected information (available only with probable cause or reasonable suspicion) and information that police can access more quickly and easily. Rather than distinguishing between more and less private *types* of records, legislators might instead require those who keep digital records to distinguish between the more and less sensitive *component of* each record. It is possible, for example, for many categories of records police will be able to satisfy probable cause or reasonable suspicion with de-identified data, and thus be permitted to connect it to particular individuals only after satisfying such a threshold. The Standards include a discussion of such a system. *See* STANDARD 25-5.6.

93. *See supra* notes 16-17 an accompanying text.

94. *E.g.*, United States v. Miller, 425 U.S. 435 (1976).

https://digitalcommons.law.ou.edu/olr/vol66/iss4/4

'choice' to convey information to a bank is not voluntary in any meaningful sense."[95] Indeed, individuals are required to constantly share information about their activities, including very sensitive information, if they want to participate in modern society. This was true in the 1970s, when an individual could not call another person unless they made contact through, and shared the number they were calling with, a telephone company's central office. It is even more true in an age where individuals cannot use a computer without conveying incredibly sensitive information to Internet service providers and cannot carry a cell phone without exposing their physical movements, and phone and Internet activities, to outside observation.[96] The first factor makes clear that the price of life in modern society should not be a complete sacrifice of privacy. It urges lawmakers to consider whether "the initial transfer of such information to an institutional third party is reasonably necessary to participate meaningfully in society or in commerce."[97]

This is certainly an important point, but it is not one that *always* has importance in determining a record's privacy. Some of the information we use to function in modern life is quite private. This is true, for example, of the e-mail content and web surfing choices that we share with Internet service providers.[98] The limited (and unavoidable) sharing that makes such e-mail and web surfing possible should not, as the Standards rightly point out, make it any less private.

However, this is not true of all information we are forced to share as we move through modern society. We often have no choice but to share information about our home address in order to own that property and receive mail and other services there. This does not mean our home address is moderately or highly private, and should consequently be unavailable to law enforcement in the absence of reasonable suspicion or probable cause. Thus, the fact that we must share information as a condition of life in modern society shouldn't weigh against a finding of high privacy, but neither should it weigh in favor of it. Rather, it is most important as a

95. Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 987 (2007) (citing Burrows v. Super. Ct. of San Bernardino Cnty., 529 P.2d 590, 596 (Cal. 1974)).

96. Bob Sullivan, *Byte Me: How Our Gadgets Track Our Every Move*, NBCNEWS.COM (Feb. 5, 2014), http://www.nbcnews.com/tech/security/byte-me-how-our-gadgets-track-our-every-move-n18621.

97. STANDARD 25-4.1(a).

98. *See* Lincoln Spector, *Is Your ISP Spying on You?*, PCWORLD (Sept. 3, 2012), http://www.pcworld.com/article/261752/is_your_isp_spying_on_you_.html.

Published by University of Oklahoma College of Law Digital Commons, 2014

corrective—in those circumstances where lawmakers might otherwise wrongly assume that by knowingly sharing our information with a third party (or perhaps sharing it widely with numerous third parties), we have sacrificed our private interests in it. The Standards rightly point out that this assumption is a flawed one where our sharing is not truly voluntary, but rather something that everyone must do simply to live a normal life.[99] However, putting emphasis on such a corrective only makes sense in the situation it is intended to correct. Thus, legislators should avoid beginning every factor-based analysis of the privacy levels by considering whether information is of the kind we need to share in order "to participate meaningfully in society or in commerce."[100] It makes more sense to raise this point only when it is needed. For example, if existing privacy laws and social practices seem to indicate that a certain kind of information is widely shared, legislators might then ask the follow-up question of whether such information is shared because individuals consider it non-sensitive, or rather because individuals are compelled to share it whether it is sensitive or not.

Defenders of the Standards' current set of factors might also object to simply treating privilege law (factor (d)) or evidence of sharing with numerous "non-governmental entities" (factor (c)) as nothing more than components of a more general analysis about whether information is currently treated as private. Where information is so sensitive as to be subject to a legal privilege, one might argue, this should trump evidence of social practices that points the other way. For example, even if people often tell friends, family, and acquaintances about what their lawyers said to them, perhaps the information should still be treated as highly private when there is a strong attorney-client privilege available in the law for those who choose not to waive it. Likewise, as the Standards note, where information that is "personal" and otherwise regarded as private is widely disseminated to numerous third parties, lawmakers may legitimately ask why not also allow it to be shared with the police.[101] To be sure, it may make sense to try to structure the way legislators apply each factor by formulating sub-factors that can guide the application of that factor. They could, for example, make a list of the types of evidence they will normally apply to uncover evidence of whether (and to what extent) modern social practices, legal rules, and expectations treat certain types of information as

99. STANDARD 25-4.1(a).
100. STANDARD 25-4.1(a).
101. STANDARD 25-4.1(b).

private. But that doesn't mean that the law of privilege, or evidence of dissemination to third parties, is so critical to this inquiry that it should have a separate status. The law of privilege, for example, is intended to protect sensitive information not against police observation, but against discovery and possible use at trial by litigation opponents.[102]

III. An Alternative to Traditional Protection Categories: Another Way to Frame Law Enforcement Interests

Whereas the Standards provide lawmakers, courts, and agencies with detailed advice on how to classify a particular record's level of privacy (as high, moderate, minimal, or non-private), they provide far less explanation as to why they match each such level with a particular type of protection (demands for probable cause, reasonable suspicion, relevance, or no protection).

This is not surprising. Lawmakers and other legal actors may be unfamiliar with how to draw the line between "highly private" and "moderately private" information, for example, because this is not a line that is familiar in legislation or case law. By contrast, the Standards' categories of protection are familiar ones. The Constitution itself demands that government show probable cause to obtain the warrants required under the Fourth Amendment,[103] and courts have struggled for years to define what probable cause means and demands.[104] Since it decided *Terry v. Ohio* in 1968, the Court has demanded "reasonable suspicion" in cases (such as "stop-and-frisk" investigations or "special needs" cases) where they wish to give police more leeway to investigate certain subjects, but still want them to remain subject to external constitutional restraint.[105]

---

102. *See* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 68 cmt. c (2000).

103. U.S. CONST. amend. IV.

104. Terry v. Ohio, 392 U.S. 1, 37 (1968) (Douglas, J., dissenting) ("The requirement of probable cause has roots that are deep in our history." (quoting Henry v. United States, 361 U.S. 98, 100 (1959))); United States v. Brinegar, 338 U.S 160, 175 (1949) (stating that probable cause requires "less than evidence which would justify . . . conviction" but "more than bare suspicion"); Carroll v. United States, 267 U.S. 132, 161 (1924) (defining probable cause as "reasonable ground for belief of guilt" (citing McCarthy v. De Armit, 99 Pa. 63 (1881))); United States v. Locke, 11 U.S. (7 Cranch) 339, 348 (1813) ("It imports a seizure made under circumstances which warrant suspicion.").

105. *Terry*, 392 U.S. at 30 (holding that to make an investigatory stop, an officer does not need probable cause and may instead make such a stop when he "observes unusual conduct which leads him reasonably to conclude in light of his experience that criminal activity may be afoot").

Published by University of Oklahoma College of Law Digital Commons, 2014

Christopher Slobogin provides a fuller account of these standards in the "four-tier" system of protection that he presents in his book, *Privacy at Risk*—a system that advocates use of categories of protection quite similar to those that the Standards set forth for records.[106] As Slobogin observes, "The probable cause and reasonable suspicion standards are well established and fairly well defined," with probable cause often being equated with "a more-likely-than-not (51 percent) finding, or perhaps a level of certainty somewhat below that" and reasonable suspicion "associated with approximately a 30 percent level of certainty."[107] Relevance, by contrast is "commonly associated with subpoenas" rather than court orders, and, as Slobogin explains, generally is used to describe evidence that has "any tendency to make a fact in issue more probable than not."[108]

These "categories of protection" allow legislators to use an "off the shelf" solution for records protection rather than trying to begin from scratch with a system that courts may then take years to refine and that government officials may struggle to understand.

These categories also play a crucial role in the balance that the Standards aim to strike between law enforcement needs and individual privacy interests. These categories of protection essentially measure the government-interest side of that balance. The higher a record's level of privacy, the stronger the government's interest must be to obtain it. This interest is measured by the government's ability to meet probable cause, reasonable suspicion, or whatever level of certainty is required—and, for the two highest tiers of privacy, officials are also faced with the hurdle of convincing a court, and not just an internal agency official, that the requisite level of certainty is met.

However, while legislators should certainly take advantage of these ready-made categories of protection, they should not be confined to them; there are circumstances in which the law enforcement interests at stake may not be fully captured by a "level of suspicion" standard. For example, there may well be circumstances where the government's interest in seeing a record is not the kind of interest that will *meet* probable cause or reasonable suspicion. Rather, in certain circumstances law enforcement may need to be free from such a burden. It may need to examine "highly" or

106. SLOBOGIN, *supra* note 5, at 38.
107. *Id.*
108. *Id.* at 39.

"moderately" private records even when it *cannot* satisfy the probable cause or reasonable suspicion standard.

This kind of circumstance is already a familiar one in Fourth Amendment law's special needs cases. "Special needs" searches are those that occur in a setting where "special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable."[109] In fact, in the special needs context, the Court not only allows officials to conduct a search without a warrant or probable cause—it also allows them to conduct a search without any individualized suspicion of any kind. It allows random drug tests at schools and workplaces,[110] sobriety checks of all drivers at a fixed highway checkpoints,[111] and searches of travelers and their belongings at airports.[112] As the Court has noted, such "even-handed blanket" searches are permissible in special needs searches conducted "outside the criminal context" so long as they are justified by a "balancing [of] the invasion of privacy [entailed by the search] against the government's strong need."[113]

As this statement indicates, the "government's strong need" in this case is one that is not measured by its ability to satisfy probable cause (or some lower threshold of individualized suspicion). Rather, it is an interest that justifies waiving of the normal probable cause or reasonable suspicion requirement.

In some cases, the Court tolerates blanket searches because the State, when conducting them, has stepped out of its role as general enforcer of the laws and into a more limited role in which it is not authorized to jail people or otherwise subject them to criminal penalties. Where such general searches are available to authorities in public schools or workplaces, they are not tools to ferret out and punish crime, but rather tools the State can use only in its special role of ensuring school or workplace safety and

109. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995) (quoting Griffin v. Wisconsin, 483 U.S. 868, 873 (1987)).

110. *Id.* (schools); Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S 602, 619-21 (1989) (workplaces).

111. Mich. Dep't of State Police v. Sitz, 496 U.S. 444 (1990).

112. See United States v. Aukai, 497 F.3d 955, 959-60 (9th Cir. 2007) (finding a search of a traveler at an airport was a reasonable search and noting that administrative searches of this kind have been upheld on the ground that they serve a "special governmental need, beyond the normal need for law enforcement"(quoting Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 665 (1989)).

113. *See Acton*, 515 U.S. at 673 (O'Connor, J., dissenting); *see also* Andresen v. Maryland, 427 U.S. 463, 480 (1976) (noting that the Fourth Amendment forbids "general, exploratory rummaging in a person's belongings").

Published by University of Oklahoma College of Law Digital Commons, 2014

discipline.[114] In this respect, Fourth Amendment law mirrors First Amendment law, which allows school principals and government employers to impose speech limits on students[115] and workers[116] that would run afoul of free speech protection if they were imposed by Congress or state legislatures on citizens more generally. School and workplace officials may likewise conduct searches of a kind that would violate the Fourth Amendment if the state tried to conduct them in other contexts.[117]

But some permissible blanket searches are less clearly outside the criminal context. For example, if we are stopped at a sobriety checkpoint, the search we must undergo is conducted by a uniformed police officer, not a schoolteacher or workplace supervisor. If such a search reveals to the officer that we are in fact drunk while driving on the highway, we not only face immediate limits on our driving privileges, but also potential criminal charges. The same is true at an airport security checkpoint. If a search of our bag turns up evidence of a weapon, such a discovery might well result in an arrest and indictment, not simply a refusal to let us board an airplane.

In these cases, the government need that justifies release from the normal individualized suspicion requirement is not a need that takes place *outside* the law enforcement context (to a school or workplace) but rather a need, which although related to law enforcement, goes beyond "the general interest in crime control."[118] As the Court has noted, such an extraordinary law enforcement need may emerge when police set up roadblocks to "thwart an imminent terrorist attack or to catch a dangerous criminal who is likely to flee by way of a particular route."[119] These examples would likely count as the kind of emergency or exigent circumstance in which, the

---

114. *See, e.g.*, *Von Raab*, 489 U.S. at 666 ("It is clear that the Customs Service's drug testing program is not designed to serve the ordinary needs of law enforcement. Test results may not be used in a criminal prosecution of the employee without the employee's consent.").

115. *See, e.g.*, Hazelwood Sch. Dist. v. Kuhlmeier, 484 U.S. 260, 271-72 (1988) (permitting a principal's censorship of a school newspaper).

116. *See, e.g.*, Connick v. Myers, 461 U.S. 138, 146-49 (1983) (permitting an employer to fire an employee who challenged a transfer and submitted a questionnaire to colleagues about the transfer policy).

117. *E.g.*, New Jersey v. T.L.O., 469 U.S. 325, 341-43 (1985).

118. *See* City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000) (noting that law enforcement may search cars without reasonable suspicion only where their purpose is more particular than "the general interest in crime control"); *see also* Blitz, *supra* note 50, at 1451-52 (noting that suspicionless searches at airports are used not only to prevent terrorism, but to apprehend and punish those attempting it).

119. *Edmond*, 531 U.S. at 44 (forbidding police from using a roadblock program to search for evidence of drug use).

https://digitalcommons.law.ou.edu/olr/vol66/iss4/4

Standards make clear, police may obtain even a highly private record pursuant only to "the request of a law enforcement officer or prosecutor,"[120] without the need to first obtain authorization from a neutral magistrate. But not all such extraordinary law enforcement needs fit easily into the category of emergency or exigency. Routine airport searches, for example, are not performed only in the face of an expected hijacking. They take place every day, even in the absence of any terror alerts. Nonetheless, the cost of police missing such an air travel threat is so high that courts have treated this as an extraordinary security interest that justifies metal detectors and airport searches even absent individualized suspicion.[121]

The Standards also carve out room for such a nonemergency exception to probable cause or other individualized suspicion requirements. Standard 25-4.2(b) waives them in circumstances where these requirements "would render law enforcement unable to solve or prevent an unacceptable amount of otherwise solvable or preventable crime, such that the benefits of respecting privacy are outweighed by this social cost."[122] A modern-day Justice Brandeis might well worry that this is precisely the kind of exception that law enforcement would eagerly broaden to clear away any privacy protecting hurdles in their way. Where court order requirements come to seem frustrating, officials might insist to legislators that they impose high "social cost" and ask for them to be removed. But a more generous reading of this requirement treats it as a parallel of sorts to the Fourth Amendment special needs requirement. Like the special needs cases, it is intended not to sweep away probable cause or other individualized suspicion requirements, but rather to recognize—and permit a response to—the reality that the probable cause and individualized suspicion hurdles that provide invaluable privacy protection in most cases, might erect insuperable barriers to law enforcement activities in others.

Still, the Standards' cost-benefit escape clause is framed in worrisomely broad terms. It is not only in airport searches or other terrorism-related cases that the police may argue that probable cause requirements constitute a hindrance with unacceptable "social costs," but also in many situations where they are addressing the "general interest in crime control" that the Court has so far disqualified from special needs treatment. To some extent, the special needs framework itself presents the same problem: in certain categories of searches, it allows police to escape the individualized

120. STANDARD 25-5.4.
121. United States v. Aukai, 497 F.3d 955, 960-61 (9th Cir. 2007).
122. STANDARD 25-4.2(b).

Published by University of Oklahoma College of Law Digital Commons, 2014

suspicion requirement so long as they can argue that "the invasion of privacy [entailed by the search is outweighed by] the government's strong need [for it]."[123]

This Court's embrace of such cost-benefit analysis in its special needs jurisprudence—and the ABA's embrace of it in Standard 25-4.2(b)—presents a striking contrast to the treatment that the same type of cost-benefit analysis has received in First Amendment cases. In *United States v. Stevens*, for example, the government met firm rejection from the Court when it argued that it should be freed from the normal First Amendment "strict scrutiny" requirements whenever lower protection was merited, given a "balancing of the value of the speech [in question] against its societal costs."[124] The Court responded that such a "free-floating test for First Amendment coverage" was "startling and dangerous" and reminded the government that the First Amendment speech protection "does not extend only to categories of speech that survive an ad hoc balancing of relative social costs and benefits," but rather extends even to speech many consider to be of little value.[125] To use the previously quoted language of Justice Souter, the First Amendment's "strict categorical rules keep[] the starch in the standards for those moments when the daily politics cries loudest for limiting what may be said."[126] By contrast, the outcome of a cost-benefit test would likely be strongly influenced by "daily politics."

To be sure, the Standards are providing a foundation not for constitutional rules, but for democratically enacted legislation, where it is typically more appropriate for decision makers to take account of, and respond to, what "daily politics cries . . . for."[127] Yet the Standards themselves seek to prevent this cost-benefit analysis from simply displacing probable cause and reasonable suspicion requirements. They emphasize that even if societal costs outweigh privacy benefits and necessitate setting aside privacy protections, such a measure should preserve as much privacy as possible: privacy should be compromised only "to the limited extent necessary to correct this imbalance."[128]

---

123. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 673 (1995) (O'Connor, J., dissenting); *see also* Andresen v. Maryland, 427 U.S. 463, 480 (1976) (stating that the Fourth Amendment forbids "general, exploratory rummaging in a person's belongings").

124. 559 U.S. 460, 470 (2010).

125. *Id.*

126. Denver Area Educ. Telecommunications Consort., Inc. v. FCC, 518 U.S. 727, 785 (1996) (Souter, J., concurring).

127. *Id.*

128. STANDARD 25-4.2(b).

There is, however, a better way of striking the right balance in situations where probable cause or other suspicion thresholds fail to take adequate account of law enforcement needs. One finds such an alternative in the scrutiny-based system used in the First Amendment speech cases, the same scrutiny-based system that the justices have generally refused to replace with more "free form" cost-benefit analysis.[129]

It is useful to explore how a framework modeled on the constitutional tiers of scrutiny might serve as an alternative to the balancing system that the Standards currently rely upon—not a full-fledged replacement for the Standards' current model, but one that might be used in limited circumstances where individualized suspicion requirements are inappropriate.

First, it is helpful to review how strict, intermediate, and minimal scrutiny work. In general, each level of scrutiny imposes two types of requirements on government: an ends requirement and a means requirement.[130] The ends requirement demands that the government objective be justified by an interest of a certain strength. Where the government restriction threatens harm to core constitutional interests, for example, and thus triggers strict scrutiny, the government can justify its action only by showing that its interest is "compelling."[131] When intermediate scrutiny is the applicable standard, the government interest must only be "substantial" or "significant."[132] And where the government is subject to "minimal scrutiny," any "legitimate government purpose" is sufficient.[133]

---

129. *See Denver Area Educ. Telecomm. Consortium, Inc.*, 518 U.S. at 785 (Kennedy, J., concurring in part and dissenting in part).

130. *See* 16B AM. JUR. 2D *Constitutional Law* § 857 (2014).

131. *See* United States v. Windsor, 133 S. Ct. 2675, 2717 (2013) (holding that laws subject to strict scrutiny must be "'narrowly tailored' to achieve a 'compelling' government interest" (quoting Parents Involved in Cmty. Schs. v. Seattle Sch. Dist. No. 1, 551 U.S. 701, 720 (2007))).

132. *See* Milavetz, Gallop & Milavetz P.A. v. United States, 559 U.S. 229, 249 (2010) (stating that to withstand intermediate scrutiny, the government must show that its restriction "'directly advanc[es]' a substantial governmental interest" and is "'no more extensive than is necessary to serve that interest'" (quoting Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 566 (1980))); Phelps-Roper v. Koster, 713 F.3d 942, 950 (8th Cir. 2013) (stating that intermediate scrutiny requires, among other things, determining if the government's "regulations are 'narrowly tailored to serve a significant government interest'" (quoting Phelps-Roper v. City of Manchester, Mo., 697 F.3d 678 (8th Cir. 2012))).

133. *See* Schwarz v. Kogan, 132 F.3d 1387, 1390-91 (11th Cir. 1998) (stating that in order to survive rational basis review, or "minimal scrutiny," a "challenged provision need

Published by University of Oklahoma College of Law Digital Commons, 2014

The means requirement goes further in that it demands that even where government has an interest of the appropriate strength, it still must (at least in the case of strict and intermediate scrutiny) take steps to minimize the harm it does to whatever liberty interests are involved.[134]

Consider, for example, how intermediate scrutiny applies to so-called "time, place and manner" restrictions on when, where, and how people can gather for a rally, protest, or otherwise engage in public speech. In these cases, the intermediate level of scrutiny is designed to strike a balance between the First Amendment interests of the protesters in free expressions and the government interests at stake when a protest or parade might disrupt traffic, or prevent others from using public space.[135] Even though government in such cases, is often trying to protect safety interests and not trying to suppress a particular category of speech, it still must be regulating for (1) a sufficiently important reason, and not a minor interest that does not justify the First Amendment sacrifice it demands, and (2) in a way that attempts to minimize that First Amendment sacrifice rather than restricting far more speech than is necessary to fulfill the governments safety, traffic control, or other interests.[136]

These elements of time, place, and manner regulation were all considered by the Court, for example, when it upheld the constitutionality of a Minnesota regulation that required organizations distributing or selling literature at the state fair to do so from an authorized "fixed location[]" at a rented booth.[137] The International Society for Krishna Consciousness (ISKCON), whose members wished to distribute literature in various locations throughout the fair, challenged the regulation.[138] The Court first

---

only be rationally related to a legitimate government purpose" (citing TRM, Inc. v. United States, 52 F.3d 941, 945 (11th Cir. 1995))).

134. 16B AM. JUR. 2D *Constitutional Law* § 857 (2014).

135. *See, e.g.*, Cox v. New Hampshire, 312 U.S. 569, 574 (1941) (noting that constitutional protection of civil liberties is not inconsistent with government's protection of "social need" such as "control of travel on the streets of cities"); Comite de Jornaleros de Redondo Beach v. City of Redondo Beach, 657 F.3d 936, 947-48 (applying the time, place, and matter intermediate scrutiny test to strike down a solicitation that was not narrowly tailored to the "undisputed" government "duty and responsibility to keep their streets open and available for movement" (quoting Cox v. Louisiana, 379 U.S. 536, 554-555 (1965))).

136. *See* Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989) (noting that regulations are constitutional when they "are justified without reference to the content of the regulated speech, . . . are narrowly tailored to serve a significant governmental interest, and . . . leave open ample alternative channels for communication of the information").

137. Heffron v. Int'l Soc'y for Krishna Consciousness, Inc., 452 U.S. 640, 643 (1981).

138. *Id.* at 644.

https://digitalcommons.law.ou.edu/olr/vol66/iss4/4

assured itself that the state fair regulation was not aimed at suppressing the speech of ISKON members or any other speakers. It noted, first, that the rule itself did not discriminate against any speakers, but rather "applie[d] evenhandedly to all who wish to distribute [literature] and sell written materials."[139] Moreover, said the Court, the rules were not only neutral on their face, but also prevented state officials from engaging in the kind of "covert" censorship that might result when "arbitrary discretion [to bar certain speakers but not others] is vested in some governmental authority."[140] Because "[t]he method of allocating space" was a "straightforward first come, first served system," officials could not easily twist it into a tool for suppressing certain speakers, while allowing others to roam the fair.[141] Had the Minnesota state fair rules flunked this test of genuine content-neutrality, they would have been subject not to intermediate scrutiny, but rather to the strict scrutiny that the Court applies to laws that bar speech on the basis of its content.[142]

Even though the Court was convinced of the law's neutrality, its speech limitation still entailed some threat to First Amendment interest—it limited the access that ISKON members had to potential audiences and that interested listeners had to ISKON's speech. So the government did not receive unlimited leeway to impose such restrictions. It first needed to show that it was doing so in furtherance of a significant interest, justifying the First Amendment sacrifice the government was demanding (the ends requirement).[143] The Supreme Court found its interest in crowd control at the state fair met this test.[144] It also needed to show that it was not limiting speech much more severely than necessary to achieve this admittedly important interest, and that it left ample room for ISKON to engage in the speech in question (the means requirement).[145]

We might better explain the logic of the Court's analysis in the line of time, place, and manner cases with the help of a medical analogy. When a surgeon is asked to perform a particularly risky operation to preserve a patient's life or health, she might first seek to assure that whatever incisions she has to make near a vital area will not likely cause damage to an

139. *Id.* at 649.
140. *Id.*
141. *Id.*
142. *See* Burson v. Freeman, 504 U.S. 191, 197-98 (1992).
143. *Heffron*, 452 U.S. at 649.
144. *Id.* at 650.
145. *Id.* at 650-51.

Published by University of Oklahoma College of Law Digital Commons, 2014

essential organ or physiological function.[146] There is after all, little point in performing a brain operation to improve neurological function, if in doing so one causes more harm than improvement, for example, by destroying the hippocampal area necessary for individuals to form memories,[147] or by destroying blood vessels necessary for a person to survive. It is only where such a risk to life or mental integrity is the only hope for survival, or for avoiding some other catastrophic fate, that a doctor might, on such a cost-benefit analysis, decide it is a risk worth taking. By contrast, if the surgery—while not risk-free—raises concerns only about other less essential and central physiological functions, then surgeons whose goal is to safeguard a patient's life and health may carry it out even when the situation is not as desperate. Similarly, where a state's attempt to protect citizens' interest in safety or crime control measures is achieved only by causing harm to a critical constitutional interest—such as individuals freedom to hold and communicate the beliefs of their choice—then courts will allow a state to undertake action that jeopardizes those interests only where the harm it is addressing is so serious that the state can survive "strict scrutiny."

By contrast, where a state's limit on speech is content-neutral, and thus does not oppress speech on the basis of its message or meaning, then the risk to First Amendment values is lower, and the state will have more leeway to impose the limit. However, the risk to First Amendment interest *still* requires that it not do so lightly. Rather, it must still show, under the Court's "intermediate scrutiny" standard, that it is addressing a real and serious problem of the kind that justifies such a sacrifice (the ends requirement), and that it is doing so in a way that is calculated to avoid imposing unnecessary harm (the means requirement).[148]

Where by contrast, a state's actions do not threaten such a critical constitutional interest, the Court applies only minimal scrutiny and gives the government much freer reign. It does not second-guess the government's claim that its regulation is sufficiently important, demanding

146. *See Blood Vessel Anomalies – Bleeding in the Brain*, NEURO-SURGERY.EU, http://www.neuro-surgery.eu/EXEN/site/hs-hersenbloeding.aspx (last visited Mar. 28, 2014) (noting that certain brain malformations are "so large or difficult to access that surgery would be impossible without causing significant damage to normal tissue").

147. *See* Jenni Ogden, *HM: The Man with No Memory: A Neuropsychologist Muses on Brains, Books and Being Happy*, PSYCHOL. TODAY (Jan. 16, 2012), http://www.psychologytoday.com/blog/trouble-in-mind/201201/hm-the-man-no-memory (describing how removal of a patient's hippocampus to treat seizures left him with "dense memory loss").

148. *See* Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989).

only that the government end be a "legitimate" one (the ends requirement).[149] And as long as the government's measure is rationally related to this legitimate end, and not an arbitrary exercise of power, the Court will not second-guess the government's methods (the means requirement).[150]

It is tempting, perhaps, to treat the categories of protection already used by the Standards—probable cause, reasonable suspicion, and relevance—as respectively analogous to strict, intermediate, and minimal scrutiny. But the analogy is actually a weak one. First, probable cause as a general matter erects a far less significant hurdle against government action than does strict scrutiny. As noted earlier, it demands that police have a level of certainty that exceeds (or perhaps nears) 50 percent probability that the evidence they are seeking be associated with a crime.[151] This is a threshold police can often meet; they often succeed, after all, in obtaining a warrant from a neutral magistrate. By contrast, strict scrutiny is, in most cases, almost impossible for the government to satisfy.

Second, when applying the probable cause requirement, courts generally do not question the importance of the particular law enforcement interest that the government is pursuing.[152] All the police need to do is show that they have the requisite level of confidence that the evidence they are seeking is linked to a crime, whatever its severity.[153] To meet strict or intermediate scrutiny, on the other hand, it is not sufficient for the government to convince a court that the problem it is addressing is a real

149. *See* Schwarz v. Kogan, 132 F.3d 1387, 1390-91 (11th Cir. 1998).

150. *Id.*

151. SLOBOGIN, *supra* note 5, at 38.

152. *See* Jeffrey Bellin, *Crime-Severity Distinctions and the Fourth Amendment: Reassessing Reasonableness in a Changing World*, 97 IOWA L. REV. 1, 11 (2011) ("The various overarching verbal formulations that govern Fourth Amendment doctrine similarly ignore the wide variance in the public interest in solving different crimes. To detain (or arrest) a suspect, a police officer must have a reasonable suspicion (or probable cause) that '*criminal activity* is afoot.'" (quoting Illinois v. Wardlow, 528 U.S. 119, 123 (2000)). But see *Andrew E. Taslitz*, *What is Probable Cause, and Why Should We Care?: The Costs, Benefits, and Meaning of Individualized Suspicion*, LAW & CONTEMP. PROBS., Summer 2012, at 145, 153 (noting that a minority of courts consider probable cause to be a "variable standard" depending in part on "the crime's severity").

153. *See* 2 WAYNE R. LAFAVE, SEARCH & SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 3.2(a) (5th ed. 2013) (noting that the Supreme Court refused "to adopt a proposed 'multifactor balancing test' for probable cause which 'would require an officer to weigh . . . the manner and intensity of the interference, the gravity of the crime involved and the circumstances attending the encounter'" (quoting Dunaway v. New York, 442 U.S. 200, 211 n.14 (1979))).

Published by University of Oklahoma College of Law Digital Commons, 2014

one—it must also convince the court that the problem is serious enough to justify the incursions into the liberty that result from (or are at least risked by) a speech restriction.[154]

My proposal here is that, while the Standards' categories of protection should continue to be the norm, legislators might apply a framework akin to scrutiny-based review where the government insists it has a need to be excused from probable cause requirement or whatever the normal category of protection would otherwise be.

More specifically, law enforcement might be excused from such requirements only if it can satisfy (1) an ends requirement that demands, for example, that the law enforcement need is one that raises extraordinary concern and (2) a means requirement, demanding that even when law enforcement is excused from probable cause, reasonable suspicion, or relevance requirements, it must subject itself to other measures that help minimize privacy harms.

As noted above, the ends requirement is at odds with the way the Court has generally decided Fourth Amendment cases. Police need to show probable cause that the area to be searched or things to be seized are connected with a crime—not that the crime is a serious one.[155] However, something akin to a serious crime requirement makes more sense when law enforcement is not attempting to satisfy probable cause (or reasonable suspicion), but rather seeking to justify being excused from such a requirement. This, as already explained, is what is typically required in "special needs" cases, where law enforcement can only engage in suspicionless searches if they show they are addressing a "special need[], beyond the normal need for law enforcement."[156] Moreover, even after officials show that they are addressing a "special need," they then have to show that the government interest justifying their search is strong enough to outweigh the privacy interests it compromises. Emergencies and "exigent circumstances" might represent one set of circumstances that typically meet such an ends requirement. But legislators, courts, and agencies might try to systematically identify others. Rather than simply treating the ends requirement as satisfied by any objective that a free form analysis leads lawmakers to believe outweighs the privacy interests on the other side of

154. *See* Heffron v. Int'l Soc'y for Krishna Consciousness, Inc., 452 U.S. 640, 649 (1981).

155. *See* Texas v. Brown, 460 U.S. 730, 742 (1983) (finding that probable cause requires only "that certain items may be contraband or stolen property or *useful as evidence of a crime*" (emphasis added)).

156. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 655 (1995).

the balance, lawmakers might think more carefully about what specific types of government purposes would justify such an exception to the rules, as courts do when they ask what counts as an interest that is compelling or significant enough to respectively satisfy strict or intermediate scrutiny.

The means requirement is also significant. It allows legislators to place hurdles in government's way that protect privacy even where it is not feasible to place hurdles of the kind one finds in probable cause or reasonable suspicion requirements. More specifically, it might allow them to assure that, even when government demands some sacrifice to our privacy interests, it will cause as little harm as possible to those interests.

One already finds this kind of "minimization" requirement in certain areas of Fourth Amendment law. For example, as Susan Freiwald points out while addressing wiretapping and surreptitious video recording in a private environment, courts have often demanded even more from police in these searches than they do for "one-shot physical searches."[157] Rather, they have imposed a "heightened level of judicial oversight," which demands that police not only have good reasons for using such electronic surveillance, but follow certain procedures when doing so[158]—procedures which, in the words of the Supreme Court in *Berger v. New York*, are designed to "minimize[]" the "danger" by assuring that "no greater invasion of privacy was permitted than was necessary under the circumstances."[159] Under *Berger*, this "minimization" requirement is one of the four requirements the government must meet to survive Fourth Amendment review of an eavesdropping request.[160] And similar minimization demands have become a standard part of electronic surveillance law, and other features of surveillance law, such as the amended version of section 215 of the USA Patriot Act.[161]

It has also found a place in the Court's Fourth Amendment special needs cases. The Court has emphasized the limited nature of the information collected and recorded by the government. In *Skinner v. Railway Labor Executives' Ass'n*, the Court noted that "chemical analysis of urine, like that

157. Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶ 53.

158. *Id.*

159. 388 U.S. 41, 57 (1967).

160. *Id.* at 56-57 (finding minimization to be part of the Fourth Amendment requirement that warrant requests be particularized).

161. *See* USA PATRIOT Act of 2001 § 215, 50 U.S.C. § 1861(g) (2012) (requiring the Attorney General to "adopt specific minimization procedures governing the retention and dissemination by the Federal Bureau of Investigation of any tangible things, or information therein" in foreign intelligence or terrorism investigations governed by the act).

Published by University of Oklahoma College of Law Digital Commons, 2014

of blood, can reveal a host of private medical facts about an employee."[162] The Court then went on to observe that "under the [applicable] regulations," the government was barred from using the urine and breath tests administered to railroad workers "as an occasion for inquiring into private facts unrelated to alcohol or drug use."[163] In *National Treasury Employees Union v. Von Raab*, the Court likewise emphasized that "urine samples may be examined only for the specified drugs" and that "[t]he use of samples to test for any other substances is prohibited."[164] In *Vernonia School District 47J v. Acton*, the Court made a similar point.[165] The information collected by the drug testing system, it stressed, was hardly a treasure trove of personal information about a student's medical condition or past behavior.[166] "[I]t is significant that the tests at issue here look only for drugs, and not for whether the student is, for example, epileptic, pregnant, or diabetic. Moreover, the drugs for which the samples are screened are standard, and do not vary according to the identity of the student."[167]

It has also emphasized the limits on who could access the drug testing information. For example, in *Board of Education of Independent School District No. 92 of Pottawatomie County v. Earls*, the Court emphasized that the drug testing procedures required that "test results be kept in confidential files separate from a student's other educational records and released to school personnel only on a 'need to know' basis."[168] The Court also emphasized (as it had in the other drug testing cases) that the tests "are not turned over to any law enforcement authority," and indeed, in *Earls* itself, could not even lead to "the imposition of discipline or have any academic consequences."[169]

The same kinds of privacy safeguards have likewise received emphasis from some of the courts permitting the collection of DNA—and creation of DNA profiles—from individuals arrested for felonies. Consider, for example, *United States v. Mitchell*, in which the Third Circuit held that it was permissible for the federal government to collect DNA and create computerized DNA profiles from individuals indicted for (but not convicted

162. 489 U.S. 602, 617 (1989).
163. *Id.* at 626.
164. 489 U.S. 656, 673 n.2 (1989).
165. 515 U.S. 646 (1995).
166. *Id.* at 658.
167. *Id.* at 659 (internal citations omitted).
168. 536 U.S. 822, 833 (2002).
169. *Id.*

https://digitalcommons.law.ou.edu/olr/vol66/iss4/4

of) a felony.[170] As courts have done in the special needs cases, the court observed that the nature of information collected was not nearly as revealing as an unfettered chemical or biological testing and analysis regime.[171] The DNA sample itself consisted of only a small fraction of the person's DNA, containing only thirteen "junk DNA" loci, so-called because these parts of the DNA apparently do not provide code that shapes our biology, and thus cannot be used to learn anything about our biological make-ups.[172] The patterns they contained were, like those in a fingerprint, likely unique to the individual who provided the DNA.[173] In this sense, they are no more revealing than a fingerprint: they just provide some sense that the person who left his DNA at a particular location had contact with that place or item.[174]

The Court also emphasized that it was "reassured by the numerous protections in place guarding against" government abuse of even the limited genetic information it had obtained.[175] The federal DNA Act allowed the government to use the sample only for "four limited purposes."[176] It not only criminalized misuse of the DNA sample itself, but also "the analysis generated from the sample."[177] And the administrative rules and procedures applying the Act added a further layer of privacy protections. It permitted only authorized individuals, approved by the FBI, to receive access to the

170. 652 F.3d 387, 406-16 (3d Cir. 2011).

171. *Id.* at 400-01.

172. *Id.* at 400; *see also* Haskell v. Harris, 669 F.3d 1049, 1051 (9th Cir. 2012) ("The laboratory creates a profile only for identification purposes by analyzing thirteen genetic markers known as 'junk DNA,' which are not linked to any known genetic traits."); *see also* Transcript of Oral Argument at 10:21-22, Maryland v. King, 133 S. Ct. 1958 (2013) (No. 12-207), 2013 WL 1842092, at *10 (argument of Katherine Winfree for Maryland) ("It's looking only at 26 numbers that tell us nothing more about that individual."). Some commentators have raised doubts about whether junk DNA is truly lacking in sensitive medical information. *See, e.g.*, Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857, 870 (2006) (noting that "some markers now thought to be meaningless may be (and have been) found to contain predictive medical information as the science progresses"); Alice Park, *Junk DNA—Not So Useless After All*, TIME, Sept. 6, 2012, *available at* http://healthland.time.com/2012/09/06/junk-dna-not-so-useless-after-all/ (describing numerous recent studies showing that "stretches of seeming 'junk' DNA are actually the seat of crucial gene-controlling activity").

173. *Mitchell*, 652 F.3d at 401.

174. *Id.* at 400-01.

175. *Id.* at 407.

176. *Id.* at 408.

177. *Id.* at 407; *see also Haskell*, 669 F.3d at 1052 (noting strict limits on use of DNA information and criminal penalties in California law for violating these limits); Oral Argument, *supra* note 172, at 16:7-8 ("The sample cannot be looked at as a matter of law.").

Published by University of Oklahoma College of Law Digital Commons, 2014

"Combined DNA Index System" [or CODIS] where the computer record of the DNA profile was stored.[178] Thus, to the extent DNA collection under the Act raised graver privacy worries than the more familiar fingerprinting of arrested individuals, such worries were—in the court's view—largely eliminated by statutory and administrative mechanisms which, taken together, prevented the government from learning any more about an individual from DNA data than they could from fingerprints.[179]

This is not to say that such minimization has been demanded. It has rather been an optional component of the free form balancing test for special needs cases mentioned earlier, wherein the courts weigh the government's interest in a search against the privacy harm it causes. Thus, in *Maryland v. King*, the Supreme Court upheld Maryland's procedures for taking DNA from arrestees and found it was constitutional because—like routine fingerprinting of an arrestee—it was an acceptable method of assuring adequate "identification" of the arrestee, and the Court said little about the procedural protections in Maryland's DNA Act.[180] The Court has likewise been willing to let the government dispense—in some special needs cases—with procedural protection it has emphasized in others.[181]

However, legislators might require the procedural protections of the kind the Court has refused to require in the special needs cases. The Standards already provide some hints as to how lawmakers might do so in the sections on de-identification, retention and maintenance, and disclosure and dissemination.

The section on de-identification proposes one "minimization" method that can, in a sense, be substituted for the normal probable cause, reasonable suspicion, or relevance requirement. In short, as long as police adopt procedures and use technologies that strip (and keep out) any personally identifying information from the records they are examining, they are free to examine even "highly private" and "moderately private"

178. *Mitchell*, 652 F.3d at 399-400.

179. *Id.* at 407.

180. 133 S. Ct. 1958, 1976-77 (2013).

181. *Compare* Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 661 n.1 (1989) (noting that under HHS regulations an employee is required to provide prescription information "only *after* he is notified that his specimen tested positive for illicit drugs, at which time the Medical Review Officer reviews all records made available by the employee to determine whether the positive indication could have been caused by lawful use of drugs"), *with* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 659 (1995) (finding no problem where the school required students to submit prescription information "*in advance*" of the test and allowed the information to be seen by school officials and not simply medical personnel).

https://digitalcommons.law.ou.edu/olr/vol66/iss4/4

records without meeting any kind of individualized suspicion.[182] All that is needed in such a case is an "official certification" from the agency.[183] Of course, this de-identification rule is not intended to provide an end run around the normal court order requirement. If police wish to reconnect this de-identified data to any identifiable individual, they must first obtain the authorization that would normally be required for that type of data, given its level of privacy (i.e., highly, moderately, or minimally private).[184]

The section on retention and maintenance likewise demands protections paralleling, in many respects, the privacy protection measure I discussed above in the Federal DNA Act.[185] It requires among other things, that legislation protect against "unauthorized access"[186] and place limits on the personnel who have the required authorization, and that "[m]oderately and highly protected" records should be "subject to audit logs recording all attempted and successful access" and "destroyed according to an established schedule."[187] The section on disclosure bars further dissemination of the records police require, except for enumerated purposes, such as for purposes of the case the police are investigating, or in certain "other government investigations, or parallel civil investigations."[188]

For example, even when records are *not* de-identified, courts might demand that police find a way to minimize the amount of unnecessary information they obtain or, by subjecting the information first to certain algorithms in computers, the amount of information that any human views. After all, it is arguably not as invasive to have our data subjected to machine analysis as it is to have it subjected to analysis by a person. Just as wiretaps might meet minimization requirements, so too might third party record searches.

Alternatively, courts might allow police to use certain highly or moderately private data that they analyze only to address problems of a limited kind. This kind of limit combines the ends and means components of scrutiny-based review. Police might be barred, for example, from obtaining DNA records used to provide evidence of serious criminal activity and then repurposing them to investigate a less serious offense.

---

182. STANDARD 25-5.6.
183. *Id.*
184. *Id.*
185. *See supra* text accompanying notes 170-179.
186. STANDARD 25-6.1(a)(i).
187. STANDARD 25-6.1(b).
188. STANDARD 25-6.2.

Published by University of Oklahoma College of Law Digital Commons, 2014

In any event, my central point here is that apart from simply relying on the familiar categories of protection one finds in the probable cause, reasonable suspicion, and relevance standards, and then supplementing them with limited use and disclosure protections, the Standards' writers (and the legislators who follow their lead) could build upon the important work they began in setting forth such use and disclosure requirements and shape them into more robust means requirements, akin to those courts use in constitutional scrutiny-based review.

Conclusion

In her concurring opinion in *United States v. Jones*, Justice Sotomayor wrote that in light of modern technological developments, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[189] Consequently, just as the Supreme Court in *Katz v. United States* decided to heed Justice Brandeis's call forty years earlier to make wiretapping a subject of Fourth Amendment protection, it may, as Justice Sotomayor indicates, turn more than eighty years later to Justice Brandeis's prophetic worry that future technologies would pull "secret papers" out of well-guarded drawers and store them instead in places where they are easier for government to access on a whim, such as today's electronic, third party owned servers.

However, until that time comes, legislators can move to fill the gap, and the Standards can provide these legislators with an admirable template on which to do so. The Standards provide an appealing, orderly framework for protecting the vast territory of third party information, and rather than focusing single-mindedly on individuals' privacy interests, instead attend to "the critical need for striking the delicate balance between law enforcement's legitimate need for access to such records and the privacy rights of the subjects of those records."[190]

My point in this article has been that while the Standards have understandably turned legal thinkers' attention from constitutional law questions to legislation, it would be good for legislators to keep in mind—as they apply and elaborate upon the Standards' invaluable framework—that they might add to this framework by continuing to think about realms of constitutional law outside of the Fourth Amendment. In particular, courts' long-standing jurisprudence on heightened scrutiny might provide

189. 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).
190. LEATPR STANDARDS, *supra* note 5, at 16.

https://digitalcommons.law.ou.edu/olr/vol66/iss4/4

important guidance both on what sphere of informational lives deserve the strongest (default) privacy protections and on the form that those protections should take when it is important to give government some access to crucial investigation-related information while continuing to minimize the damage they do to privacy interests.

Published by University of Oklahoma College of Law Digital Commons, 2014