University of Maryland Francis King Carey School of Law
DigitalCommons@UM Carey Law

Faculty Scholarship | Francis King Carey School of Law Faculty

2010

Visionary Pragmatism and the Value of Privacy in the Twenty-First Century

Danielle Keats Citron
University of Maryland School of Law, dcitron@law.umaryland.edu

Leslie Meltzer Henry
University of Maryland School of Law, lhenry@law.umaryland.edu

Follow this and additional works at: https://digitalcommons.law.umaryland.edu/fac_pubs

 Part of the Constitutional Law Commons, Internet Law Commons, and the Jurisprudence Commons

Digital Commons Citation
108 Michigan Law Review 1107 (2010).

This Book Review is brought to you for free and open access by the Francis King Carey School of Law Faculty at DigitalCommons@UM Carey Law. It has been accepted for inclusion in Faculty Scholarship by an authorized administrator of DigitalCommons@UM Carey Law. For more information, please contact smccarty@law.umaryland.edu.

VISIONARY PRAGMATISM AND THE VALUE OF PRIVACY IN THE TWENTY-FIRST CENTURY

Danielle Keats Citron[*]
Leslie Meltzer Henry[**]

UNDERSTANDING PRIVACY. By *Daniel J. Solove*. Cambridge and London: Harvard University Press. 2008. Pp. x, 257. Cloth, $45; paper, $19.95.

INTRODUCTION

Conceptualizing privacy has long been a contested endeavor.[1] Some scholars argue that privacy protects important interests.[2] Julie Cohen and Paul Schwartz, for example, view privacy as essential to autonomy and deliberative democracy.[3] Others are skeptical as to whether privacy vindicates interests worthy of discourse at all.[4] Judge Richard Posner, for instance, contends that privacy permits individuals to conceal "discreditable facts" about

* Professor of Law, University of Maryland School of Law.

** Assistant Professor of Law, University of Maryland School of Law; Associate Faculty; Johns Hopkins Berman Institute of Bioethics. We owe many thanks to Dan Solove, James Grimmelmann, Paul Ohm, and Paul Schwartz for their helpful comments; and to Leah Litman, Megan Rodgers, Eli Savit, and Kathrina Syzmborski, and their colleagues on the *Michigan Law Review* for their superb editing. We are deeply grateful to Dean Phoebe Haddon and the University of Maryland School of Law for supporting our research.

1. *See, e.g.*, Harry Kalven, Jr., *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 LAW & CONTEMP. PROBS. 326, 327 (1966) (explaining that privacy cannot function as a practical concept to guide policy and constitutional interpretation because it "seems a less precise way of approaching more specific values").

2. ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY (1988); HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010); Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962 (1964); Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV.. 233 (1977); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998); Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957 (1989); Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195 (1992); Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008); Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005).

3. *Compare* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1424–28 (2000) (explaining that information privacy yields collective benefits because it promotes individual autonomy and self-development, which are central to robust public debate), *with* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1651–52 (1999) (arguing that information-privacy rules are a precondition for deliberative autonomy and deliberative democracy). *See also* Paul M. Schwartz, Commentary, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 837 (2000) (illustrating how surveillance impedes democratic dialogue).

4. Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 422 (1980); *see also* RICHARD A. POSNER, THE ECONOMICS OF JUSTICE 272–73 (1981) (arguing that privacy hides fraud).

them to society's detriment.[5] At the heart of this dispute is privacy's protean nature: it means "so many different things to so many different people"[6] that attempts to articulate just what it is, or why it is important, generally have failed or become unwieldy.[7] Without a framework with which to delineate its parameters, privacy remains a conceptual muddle.

This is a particularly dangerous proposition given the geometric growth of information technologies. Without a meaningful framework for understanding privacy and the various contexts in which privacy problems arise, decision makers will have great difficulty identifying, defining, and protecting against socially detrimental incursions on privacy. Indeed, we may soon find ourselves living in a world where internet service providers provide digital trails of our online activities to state and federal law enforcement; where government has access to our social-network profiles, photographs, and wall musings; where cell phone providers track our daily movements; where a vast network of public and private cameras record and analyze our daily activities with facial-recognition software to identify "threats"; and where employers track employees' movements with biometric data and radio-frequency identification.[8] One might say that we already live there.[9] As

---

5. RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 40 (7th ed. 2007).

6. 1 J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 5.59 (2d ed. 2009); *see also* JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 3 (1992) (describing privacy as a concept in chaos); ARTHUR R. MILLER, THE ASSAULT ON PRIVACY 25 (1971) (referring to privacy as "exasperatingly vague"). Philosophers, policymakers, and legal scholars are engaged in a similar struggle about the meaning of "dignity" in American law and policy. Leslie Meltzer Henry, *Deciphering Dignity*, 10 AM. J. BIOETHICS (forthcoming 2010); *see also* Leslie Meltzer Henry, *Spheres of Dignity: Conceptions and Functions in Constitutional Law* (draft on file with author) [hereinafter Henry, *Spheres of Dignity*] (explaining that despite dignity's frequent invocation, there is deep disagreement about its normative, practical, and jurisprudential value).

7. *See, e.g.*, COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 25 (1992) (explaining that efforts to conceptualize privacy "have generally not met with any success").

8. *See* CORY DOCTOROW, LITTLE BROTHER (2008).

9. HAL ABELSON ET AL.,, BLOWN TO BITS: YOUR LIFE, LIBERTY, AND HAPPINESS AFTER THE DIGITAL EXPLOSION (2008). Today, fusion centers analyze feeds of public and private cameras with facial-recognition software to identify threats to communities. Danielle Keats Citron & Frank Pasquale, *Fixing Fusion Centers* (forthcoming) (draft on file with authors). Broadband providers engage in deep-packet-inspection practices, inspecting all of customers' online activities, including emails, to produce better ads. Danielle Keats Citron, *The Privacy Implications of Deep Packet Inspection Practices*, *in* DEEP PACKET INSPECTION: A COLLECTION OF ESSAYS BY INDUSTRY EXPERTS (Office of the Privacy Comm'r of Can. 2009), http://dpi.priv.gc.ca/index.php/essays/the-privacy-implications-of-deep-packet-inspection/ [hereinafter Citron, *The Privacy Implications*]; Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, U. ILL. L. REV. (forthcoming). Through Government 2.0 sites, government agencies gain access to social-media friends' profiles, pictures, videos, wall musings, and other social-network data. Danielle Keats Citron, *The One-Way Mirror: Enhancing Participation and Securing Privacy for Government 2.0*, 78 GEO. WASH. L. REV. (forthcoming 2010) [hereinafter Citron, *One-Way Mirror*]; *cf.* James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137 (2009) (exploring privacy risks of social-network sites). Cell phone providers employ GPS devices that can track their customers' whereabouts. VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 9 (2009). Employers monitor employees' email and require employees to use biometric identification systems, enabling employers to track the whereabouts of employees. Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241 (2007) [hereinafter Citron, *Reservoirs of Danger*].

the founder of Sun Microsystems warned, "You have zero privacy anyway. . . . Get over it."[10]

Daniel J. Solove's newest book, *Understanding Privacy*,[11] seeks to reverse this course. Much as Samuel Warren and Louis Brandeis mapped the importance of privacy in the face of the changing technologies of their time, Solove has done the same (and then some) for ours. In a carefully crafted text, he illustrates the deficiencies of existing theories of privacy and then develops an alternative, pragmatic approach to mapping privacy's ever-changing terrain.

Solove's nuanced understanding of privacy and its immense complexities is refreshing in its thoroughness, but one should not mistake comprehension for completion. Solove does not intend for his theory of privacy to be the last word on the topic; indeed, because new privacy problems arise every day, the best we can hope for is a trustworthy guide. In this respect, Solove's visionary pragmatism navigates us through the twenty-first century "Information Privacy Law Project"[12] and beyond.

Part I of our Review discusses the central premises of *Understanding Privacy*, with particular attention paid to Solove's pragmatic methodology and his taxonomy of privacy. We introduce his pluralistic approach to conceptualizing privacy, which urges decision makers to assess privacy problems in context, and we explore his view that meaningful choices about privacy depend on an appreciation of how privacy benefits society as a whole. We also describe how Solove's taxonomy aims to account for the variety of activities that threaten privacy. In Part II, we analyze the strengths of Solove's pragmatism by demonstrating its functionality and flexibility in the face of evolving challenges like government-run fusion centers and the government's use of social-media technologies to interact with the public. Part III contends that Solove's pragmatic approach to balancing privacy against competing interests might benefit from more detailed instruction to policymakers. In this regard, we offer several suggestions to ensure the framework's continued vitality.

I. PRIVACY'S PRAGMATIC PATH

A. *(Re)Conceptualizing Privacy*

Although privacy is protected by hundreds of statutes in the United States and thousands of laws worldwide,[13] in Solove's view, privacy is "a

---

10. Polly Sprenger, *Sun on Privacy: 'Get Over It'*, WIRED, Jan. 26, 1999, http://www.wired.com/politics/law/news/1999/01/17538.

11. Professor of Law, George Washington University Law School.

12. Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087 (2006) (reviewing DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004)).

13. *E.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (2006) (imposing limits on federal agencies' ability to collect, use, and disclose personal information and providing individuals with right to access and correct records); Fair Credit Reporting Act, 15 U.S.C. § 1681b (2006); E-Government

concept in disarray" (p. 1). While individuals seem to know instinctively when they have suffered an invasion of privacy, lawmakers and jurists are considerably less certain about these violations. Legislatures and courts frequently struggle to find a compelling account of privacy's importance and a framework to guide them in balancing privacy against other legally protected interests. All too often, according to Solove, commentators, policymakers, and judges resort to a singular notion of privacy to evaluate activities that, in fact, have significantly different privacy implications. The result is that some privacy problems that are quite distinct are conflated, while other privacy problems are not recognized at all.

Solove recognizes the appeal of unitary theories of privacy, but he ultimately rejects them. Like many philosophers, legal scholars, and jurists before him, Solove acknowledges that he initially "sought to reach a definitive conclusion about what 'privacy' is" (p. ix). Solove realized, however, that "the quest for a singular essence of privacy leads to a dead end" (p. ix).

As Solove explains, traditional methods of conceptualizing privacy, which attempt to locate a common set of necessary and sufficient elements that distinguish privacy from other categories, will always come up short.[14] If the core of privacy is defined too narrowly, important privacy problems are ignored;[15] if the core is defined too broadly, the conception lacks the precision required to provide useful guidance.

According to Solove, an alternative to traditional methods of conceptualizing privacy is needed to understand privacy in a meaningful way. In lieu of existing, unitary theories of privacy, he offers a pluralistic vision, which views privacy as an "umbrella term that refers to a wide and disparate group of related things" (p. 45). He devotes the first half of his book to developing and defending this conceptualization of privacy, which he characterizes along four dimensions: method, generality, variability, and focus.

Solove's method involves setting aside traditional approaches to conceptualizing privacy in favor of an approach grounded in philosopher Ludwig Wittgenstein's idea of family resemblances.[16] Wittgenstein employs the term "family resemblances" to explain that certain concepts do not have a central defining characteristic; rather, they draw from a pool of similar, and at times

---

Act of 2002, 44 U.S.C. § 3501 (2006) (updating the Privacy Act by requiring agencies to conduct privacy impact assessments when developing or procuring information-technology systems that include personally identifiable information); Council Directive 95/46, art. 6, 1995 O.J. (L 281) 31 (EC) (permitting the collection of data only for specific, explicit, and legitimate purposes and forbidding processing of data in ways that are incompatible with those purposes).

14. *See* pp. 1–2; *see also* HANS-GEORG GADAMER, TRUTH AND METHOD 265–66 (Joel Weinsheimer & Donald G. Marshall trans., 2d rev. ed., Crossroad Publ'g Co. 1989) (1960). Gadamer's hermeneutics rejects traditional interpretative methodologies because they are not dialogical, practical, or situational. *Id.* Insofar as Solove's pragmatic conceptualization of privacy is grounded in concrete problems and open to revision, Gadamer would likely find it an acceptable approach to understanding.

15. As Solove explains, philosophical concepts like the right of "inviolate personality," "limited access to the self," or intimacy may justify privacy protections in certain situations, but none undergirds every instance that society deems privacy worth protecting. Pp. 17–31.

16. *Cf.* Henry, Spheres of Dignity, *supra* note 6 (applying Wittgenstein's notion of family resemblances to conceptualize dignity).

overlapping, "family" characteristics.[17] Solove contends that privacy is such a concept, the meaning of which cannot be reduced to any single thing because, in practice, it describes a cluster of related things (pp. 42–46). In adopting Wittgenstein's method, Solove suggests that we categorize "something as involving 'privacy' when it bears a resemblance to other things we classify in the same way" (p. 46). One benefit of such analogical reasoning, Solove argues, is that it reflects the way we actually talk about privacy; that is, as a family of interrelated yet distinct things (pp. 44–45).

Because one of Solove's aims in conceptualizing privacy is to aid policymakers, his theory must operate with enough generality to have extensive applicability. At the same time, he must avoid the pitfalls of standard approaches to privacy that frame the concept too generally to resolve specific privacy issues. Solove's answer to this thorny problem is to conceptualize privacy from the bottom up, rather than the top down. Instead of beginning with an overarching, fixed, and abstract notion of privacy into which all privacy issues must fit (or be overlooked), Solove suggests that we start with "working hypotheses" about privacy that are created from, and constantly reshaped by, interaction with concrete situations (p. 49).

If Solove's approach to the generality problem sounds reminiscent of his method, that is because the two are mutually reinforcing. His bottom-up theory is deeply informed by philosophical pragmatism,[18] which shares certain premises with Wittgenstein's idea of family resemblances. Like Wittgenstein, classical pragmatists reject the idea of broad universal truths. Instead, they emphasize context-specific information, which is always evolving. The resulting conceptual framework tends to be flexible rather than fixed and, like Wittgenstein's family resemblances, often reveals the extent to which facets of a concept are interrelated.

If we conceptualize privacy by reasoning from concrete circumstances, then what counts as private will change over time, along with our values, culture, lifestyles, and technologies. For example, when Samuel Warren and Louis Brandeis wrote *The Right to Privacy* in 1891, they criticized the intrusiveness of penny-press journalism that reported on the social engagements of society members.[19] By 1977, the Second Restatement of Torts reflected a less stringent view of privacy, noting that a newspaper's publication of an accurate description of a private wedding, to which only family members

---

17. *See* LUDWIG WITTGENSTEIN, PHILOSOPHICAL INVESTIGATIONS §§ 65–67 (G.E.M. Anscombe trans., 3d ed., Blackwell Publ'g 2001) (1953). Wittgenstein's notion of family resemblances suggests that within a family, members share certain characteristics, such as eye color, but not others. *Id.* Despite some differences, they resemble each other because they draw from the same pool of characteristics. *Id.*

18. Although there are different "brands" of pragmatism, Solove aligns himself with classical pragmatists such as John Dewey and William James. *See* JOHN DEWEY, LOGIC: THE THEORY OF INQUIRY (1938); WILLIAM JAMES, PRAGMATISM (Prometheus Books 1991) (1907).

19. MELVIN I. UROFSKY, LOUIS D. BRANDEIS: A LIFE 98–99 (2009); Samuel D. Warren & Louis D. Brandeis, *The Right to* Privacy, 4 HARV. L. REV. 193, 196 (1890) ("The press is overstepping in every direction the obvious bounds of propriety . . . . [C]olumn upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle.").

and a few intimate friends were invited, would not amount to an invasion of privacy.[20]

Rather than shunning privacy's contingent nature, however, Solove embraces it and incorporates a dimension of variability into his theory. For him, any workable conception of privacy must adapt to changing norms and attitudes.[21] By leaving room for future cultural and historical variability, Solove hopes to avoid a static theory of privacy that accounts only for present privacy problems.

The challenge in creating a theory of privacy that is pluralistic, contextual, and contingent is determining how to infuse it with enough stability to remain useful to law and policy. Solove introduces the fourth dimension of his approach—focus—to serve this purpose. He contends that we should view the privacy landscape through the lens of the privacy problems we want the law to address (p. 75). This proposal is grounded in the same pragmatism that undergirds the other dimensions of his project.

Relying on John Dewey's pragmatic philosophy, Solove focuses on specific situations that generate a desire for privacy protections (p. 75). Importantly, his approach identifies, and aims to resolve, real privacy problems, such as the use of surveillance cameras on public streets, drug testing in schools, and employers' monitoring of employees' social-networking activities. From Solove's perspective, his context-specific focus obviates concerns that his approach is too contingent to prove useful. In the last half of his book, Solove illustrates this point by providing a robust taxonomic framework that demonstrates how focusing on different kinds of activities that encroach on privacy can shape law and policy.

B. *The Search for Privacy's Value*

Solove recognizes that any successful theory of privacy must articulate why privacy is a value worth protecting (p. 78). Without such an explanation, judges and policymakers cannot meaningfully weigh privacy against countervailing interests, such as free speech, security, and transparency. Just as in earlier parts of his book, Solove eschews existing attempts to value privacy in the abstract, instead providing a pragmatic approach that ascribes value to privacy in specific contexts.

To that end, Solove's approach requires decision makers to balance privacy against opposing interests in specific contexts and to protect privacy when it produces the best outcome for society (pp. 84–88). Solove contends that decision makers must not view privacy as an individual right that exists in tension with societal interests. According to Solove, current approaches that emphasize privacy as a personal right fail to capture its importance because they obscure society's interest in privacy protections. Solove, again relying on pragmatist John Dewey, explains that "the individual is inextrica-

---

20. RESTATEMENT (SECOND) OF TORTS § 652D, cmt. a, illus. 9 (1977).

21. As Solove demonstrates, society has attached varying degrees of privacy to the family, body, sex, home, and communication throughout history. Pp. 50–65.

bly bound up in society" (p. 91). Accordingly, when privacy protects individuals, it does so not only for their benefit, but for the common good. Decision makers can make meaningful choices about privacy only when they appreciate the individual *and* societal interests that it serves.

For Solove, framing privacy in individualistic terms risks undervaluing it. Individual privacy harms generally fare poorly when weighed against society's interest in national security, law enforcement, or free speech (p. 93). Solove demonstrates this point by asking readers to imagine that law enforcement's invasive search of a person's home reveals that the person has committed a heinous crime (p. 99). As Solove explains, if we conceptualize privacy as an individual right, we might discount the person's interest in solitude when weighed against law enforcement's interest in solving crimes and society's interest in safety. A pragmatic vision of privacy, by contrast, produces a more complete account of privacy's value by assessing society's interest in ensuring that police follow proper procedures before conducting invasive searches. Society wants to avoid unjust searches not because of any particular individual's interest, but because society has an interest in rectifying the power imbalance between government and individuals (pp. 99, 179).

Importantly, Solove's societal view of privacy does not mean that "people's injured feelings, reputations, or embarrassment are irrelevant to the value of privacy" (p. 92). Rather, it means that to fully capture the privacy harms suffered by individuals, we must demonstrate the benefits to society of rectifying them. Privacy's value, therefore, is in many respects a measure of the social benefits accruing from safeguarding aspects of individuality. Characterized in this way, privacy is nothing less than a central feature of our social structure, one that "is valuable not only for our personal lives, but for our lives as citizens—our participation in public and community life" (p. 93).

C. *Mapping the Information Age's Privacy Problems*

Solove argues that our incomplete understanding of privacy has serious costs. Because we fail to appreciate privacy's value to society, our laws often fail to address privacy problems (p. 187). For instance, courts generally find "no privacy interest if information is in the public domain, if people are monitored in public, if information is gathered in a public place, if no intimate or embarrassing details are revealed, or if no new data is collected about a person," even though society and individuals suffer significant harm in the face of those privacy intrusions (pp. 187–88).

Solove responds to the inadequacies of our current approaches to privacy by offering a taxonomy of privacy problems. His taxonomy—which is intended to help policymakers tackle concrete privacy problems effectively—does three things. It categorizes privacy-invasive activities into four basic groups, examines the activities that different privacy problems compromise, and explores the nature of the harms that they inflict

(pp. 106–70).[22] At the heart of his taxonomy is the data subject whose life is "most directly affected" by current information practices and their privacy implications (p. 103).

The first group of activities that Solove addresses involves various entities gathering information about individuals. Information collection includes surveillance, the clandestine "watching, listening to, or recording of an individual's activities," and interrogation, the "questioning or probing for information" from individuals (pp. 104, 106–17). These activities can cause harms even if the collected information is never disseminated. They can, for example, dampen public discourse and chill behavior. People may refrain from associating with unpopular groups or expressing themselves freely (pp. 108–10, 177–78).

The second group in Solove's taxonomy tackles problems arising from information processing—the storage, use, and analysis of personal data. This includes five types of information processing: aggregation, identification, insecurity, secondary use, and exclusion (pp. 117–36). For instance, public and private entities aggregate people's personal data into "digital dossiers," such as credit reports, and use them to make important decisions about individuals, even though they include erroneous and incomplete data (pp. 119–20). While people often cannot access, correct, and control their digital dossiers (the "exclusion" problem) (pp. 133–36), database operators' security lapses and abuses result in the release of personal information to criminals and others bent on destructive activities (the "insecurity" problem) (pp. 126–29, 177). Moreover, the use of Social Security numbers and other strategies to link information to people in real space decreases individuals' power over personal information and chills their expressive activities (the "identification" problem) (pp. 125–26). Finally, little prevents entities from using personal data for purposes other than those that prompted its initial gathering (the "secondary use" concern) (pp. 129–33). When people are denied control over their information, others can apply it in unforeseen contexts, often to the detriment of the data subject herself. (p. 131).

The third and broadest group of privacy problems in Solove's taxonomy pertains to releasing or threatening to release personal data. Solove describes seven forms of "information dissemination": breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, and distortion (p. 136). Breach of confidentiality, for instance, concerns the release of information in violation of a trusted relationship, such as exists between a doctor and patient (pp. 138–40). Disclosure involves the release of true, personal information in ways that can jeopardize a person's safety, reputation, or desire to speak (pp. 140–43). Distortion concerns the manipulation and spread of information about individuals in ways that can lead to reputational harms as well as embarrassment, humiliation, and stigmatization (pp. 158–61).

---

22. The first three groups concern activities that interfere with individuals' ability to control information about themselves, and the last group contends with activities that undermine individuals' solitude.

The final group of activities that Solove highlights involves interference with someone's personal life. Unlike the previous three categories of activities, invasions of privacy do not always stem from information. Solove describes two forms of invasion: intrusion and decisional interference. Intrusions involve invasions into a person's daily activities (such as telemarketing, spam, and harassing telephone calls at home) that destroy her solitude and make her feel "uncomfortable and uneasy" (pp. 162–65). Decisional interference occurs when an entity—typically the government—interferes with personal affairs, such as the decision as to whether to have an abortion or engage in consensual homosexual sodomy (pp. 165–70).

Crucial to Solove's pluralistic, bottom-up theory of privacy is an improved understanding of the various ways that privacy problems injure individuals and society. Solove explains that although the law has at times recognized the physical, emotional, financial, and reputational harms associated with privacy problems, it routinely overlooks or underestimates other critical harms (pp. 174–80). Solove describes how information-collection practices can elicit information out of context, betray confidences, and facilitate sweeping governmental investigative power in ways that the law fails to recognize (pp. 114–15, 117).

Similarly, information-processing structures can become "architectures of vulnerability" that place individuals in "position[s] of powerlessness" (p. 178), leaving them susceptible to financial losses and identity theft.[23] Law also remains blind to the chilling effect of unwanted information dissemination. Solove explains that disclosures inhibit a person from engaging in certain activities, which reduces the range of viewpoints that are expressed and thwarts trust within relationships, which makes people less likely to confide in others (pp. 176–78). Solove suggests that many of these privacy injuries resemble environmental harms, which are "created not by singular egregious acts but by a gradual series of relatively minor acts that add up over time" (p. 177).

In short, Solove's pragmatism offers a taxonomic framework to guide policymakers as they identify and tackle emerging privacy problems and their resulting injuries. In the next two Parts, respectively, we highlight the theory's contributions to privacy law and policy and discuss ways that Solove might amend his theory to ensure its endurance through the twenty-first century.

II. PRAGMATISM'S PROMISE

Solove has long grappled with information-privacy issues. His previous work has explored modern phenomena that imperil privacy, from digital dossiers controlled by business and government entities[24] to user-generated

23. *See* pp. 133–35.

24. SOLOVE, *supra* note 12, at 96, 103–09 (2004). *See generally* Richards, *supra* note 12 (reviewing Solove's *The Digital Person*).

content that distorts reputations, harasses, and shames individuals.[25] Solove's analysis and proposed solutions to those problems have received considerable attention from scholars, media, and the courts.[26]

Understanding Privacy moves this century's privacy project forward by giving policymakers tools to identify and manage concrete problems. In the last chapter of his book, Solove applies his theory to several present-day privacy issues (pp. 187–96). These applications illustrate that Solove's theory is as dynamic as it is functional, poised to respond to existing dilemmas and yet nimble enough to tackle evolving problems.

Though Solove uses other examples to demonstrate the functionality of his framework, we think its flexibility is highlighted best by applying it to the issue of government fusion centers and to government's use of social media to enhance public participation, which both pose questions at the cutting edge of information privacy. Let's first consider fusion centers. The government increasingly uses data-mining programs to identify suspicious patterns of behavior from massive data sets. State-run fusion centers analyze vast databases of private- and public-sector information, including traffic tickets, property records, motor-vehicle registrations, immigration records, tax information, public-health data, car rentals, credit reports, postal services, utility bills, insurance claims, suspicious-activity reports, and data brokers' digital dossiers.[27] They produce intelligence on potential terrorists, criminals, and other "threats" and share it with their public and private partners.[28] Private firms participating in the information sharing include owners of critical infrastructure, such as transportation and telecommunications providers.[29]

To date, policymakers have trumpeted the value of fusion centers without careful attention to the privacy threats that they pose. In recent congressional testimony, Department of Homeland Security ("DHS") Secretary Janet Napolitano underscored fusion centers' central role in the nation's antiterrorism efforts, lauding their ability to generate intelligence and to fa-

---

25. DANIEL J. SOLOVE, THE FUTURE OF REPUTATION (2007); s*ee also* Paul M. Schwartz, *From Victorian Secrets to Cyberspace Shaming*, 76 U. CHI. L. REV. 1407 (2009) (reviewing SOLOVE, *supra*).

26. *See, e.g.*, Nat'l Cable & Telecomm. Ass'n v. FCC, 555 F.3d 996, 1001 (D.C. Cir. 2009) (relying on Solove's *Conceptualizing Privacy*). A Westlaw search of law review and journal articles reveals more than 800 citations to Solove's work.

27. Pp. 187–96; Michael Fickes, *The Power of Fusion*, GOV'T SECURITY, Mar. 1, 2008, http://govtsecurity.com/federal_homeland_security/power_fusion_nsa/; Posting of Ryan Singel to Wired Threat Level Blog, *Fusion Centers Analyzing Reams of Americans' Personal Information*, www.wired.com/threatlevel/2008/04/fusion-centers/ (Apr. 2, 2008, 10:16, EST).

28. Citron & Pasquale, *supra* note 9.

29. *Private Sector Information Sharing: What Is It, Who Does It, and What's Working at DHS?: Hearing Before the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment Subcommittee of the H. Comm. on Homeland Security*, 110th Cong. 7 (2007) (statement of James M. Chaparro, Deputy Assistant Secretary, Office of Intelligence & Analysis) *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_house_hearings&docid=f:48957.pdf; Alice Lipowicz, *CSX to share data with Kentucky fusion center*, WASH. TECH., Aug. 2, 2007, http://washingtontechnology.com/articles/2007/08/02/csx-to-share-data-with-kentucky-fusion-center.aspx.

cilitate the exchange of information.[30] While Napolitano noted that the DHS "works to ensure the highest regard for our Constitutional rights, especially the First Amendment freedoms of speech, religion, assembly, and protest," she made no mention of privacy concerns.[31] This is not to say that DHS has no interest in privacy; rather it is to suggest that privacy is not one of its chief concerns.[32]

So how can Solove's pragmatic theory help policymakers appreciate the privacy implications of fusion centers? Solove's taxonomy draws attention to the variety of privacy problems that fusion centers create. In collecting information, for example, fusion centers may gather digital dossiers that contain incorrect or incomplete information about individuals.[33] Knowing that a fusion center is engaged in surveillance of our digital footprints can chill conduct, making people less likely to speak freely or associate with potentially "targeted" groups.

Fusion centers also raise significant information-processing problems. According to recent reports, fusion centers incorrectly flag individuals as persons of interest,[34] which could lead to the erroneous labeling of

---

30. *Eight Years after 9/11: Confronting the Terrorist Threat to the Homeland: Testimony Before the S. Comm. on Homeland Security and Governmental Affairs*, 111th Cong. (2009) (written testimony of Janet Napolitano, Secretary, Department of Homeland Security), *available at* http://www.dhs.gov/ynews/testimony/testimony_1254321524430.shtm. Congress has allocated $250 million to upgrade, modify, or construct state and local fusion centers for the fiscal year 2010. Hilary Hylton, *Fusion Centers: Giving Cops Too Much Information?*, TIME, Mar. 9, 2009, *available at* http://www.time.com/time/nation/article/0,8599,1883101,00.html.

31. *Eight Years after 9/11*, *supra* note 30.

32. In its privacy impact assessment ("PIA") of fusion centers, DHS acknowledged that privacy concerns arise out of fusion centers' confusing lines of authority. *See* U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE DEPARTMENT OF HOMELAND SECURITY STATE, LOCAL, AND REGIONAL FUSION CENTER INITIATIVE 26–27 (2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ia_slrfci.pdf. The PIA noted that state and local fusion-center employees are "responsible for adhering to their own State laws and policies, including those relating to individual privacy" while federal agents working at fusion centers must adhere to federal laws and policy. *Id.* at 27. The PIA urged fusion centers to address this issue in their written privacy policies. *Id.* It also acknowledged that fusion centers' data mining raises privacy concerns. *Id.* at 28. In its nonbinding guidelines to ensure that fusion centers are established and operated consistently, DHS urged fusion centers to adopt privacy policies, but offered no concrete suggestions. BUREAU OF JUSTICE ASSISTANCE, U.S. DEP'T OF JUSTICE BUREAU & GLOBAL JUSTICE INFORMATION SHARING INITIATIVE, U.S. DEP'T OF HOMELAND SEC., FUSION CENTER GUIDELINES: DEVELOPING AND SHARING INFORMATION AND INTELLIGENCE IN A NEW ERA 41 (2006), *available at* http://www.it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.

33. For instance, a Texas fusion center collects suspicious-activity reports that describe people's interest in cameras, inappropriate attire, ownership of heavy vehicles, or espousal of extremist views. Forrest Wilder, *Dr. Bob's Terror Shop*, TEX. OBSERVER, Apr. 3, 2009, *available at* http://www.texasobserver.org/article.php?aid=3003.

34. *Homeland Security Intelligence: Its Relevance and Limitations: Hearing Before the Subcomm. on Intelligence, Information Sharing and Terrorism Risk Assessment of the H. Comm. on Homeland Security*, 111th Cong. 9 (2009) (statement of Gregory T. Nojeim, Director, Project on Freedom, Security & Technology of the Center for Democracy & Technology), *available at* http://homeland.house.gov/SiteDocuments/20090318101246-50012.pdf. For instance, a Minnesota fusion center labeled a state representative a "suspect" based on a suspicious-activity report filed by her neighbor concerning her parking habits. David E. Kaplan et al., *Spies Among Us*, U.S. NEWS & WORLD REP., May 8, 2006, at 40. The representative found out about her classification as a suspect

individuals as terrorists (a distortion problem).[35] Because individuals have no means to check the data's accuracy, they feel helpless (an exclusion problem), a problem that is further exacerbated when government entities use the information for purposes other than those initially envisioned (a secondary-use problem). Fusion-center practices contribute to individuals' vulnerability and erect power imbalances between individuals and government.

Lastly, fusion centers may disclose information in privacy-compromising ways. Sensitive personal information could be provided to private parties through the information-sharing environment.[36] With fusion-center intelligence, private firms could learn about an employee's medical conditions; a loan applicant's personal life;[37] or a potential hire's religious preferences or political leanings.[38] Based on information shared between private firms and fusion centers, individuals could lose their jobs, be denied loans, or face other unfair treatment.[39] Members of the public may decline to engage in certain discussions or to travel to certain places to avoid suspicion.[40]

The utility of Solove's taxonomy is also evident when it is applied to privacy problems arising from government's use of social media to interact with the public on policy matters. Today, people can "friend" the White House and scores of government agencies on social-network sites, virtual worlds, and video-sharing sites.[41] Through online comments, live chats, and message threads, government and citizens interact on legislative issues.[42] While governments adopt Web 2.0 technologies to enhance their transparency, public participation, and collaboration,[43] they often gain access to

---

by sheer coincidence—a hacker broke into the fusion center's system and informed her of his findings. *Id.*

35. Posting of Ryan Singel to Wired Threat Level Blog, *The Architecture Reaches Out To Arrest Activist*, http://blog.wired.com/27bstroke6/2007/01/the_architectur.html (Jan. 11, 2007, 11:09 EST).

36. Rebecca Andino, *The Privacy Challenges of U.S. Fusion Centers*, THE PRIVACY ADVISOR (Int'l Assoc. of Privacy Prof'ls, York, Me.), May 2008, *available at* http://www.highlighttech.com/FusionCenters-doc.pdf.

37. In August 2007, New York City Public Schools fired an employee because the location information produced by his employer-provided cell phone showed that he was not working when he claimed to be. David Seifman, *'Track' Man Is Sacked—GPS Nails Ed. Guy*, N.Y. POST, Aug. 31, 2007, at 27.

38. Andino, *supra* note 36.

39. MICHAEL GERMAN & JAY STANLEY, ACLU, WHAT'S WRONG WITH FUSION CENTERS? 14 (2007), *available at* http://www.aclu.org/pdfs/privacy/fusioncenter_20071212.pdf.

40. One imagines that individuals might reconsider visiting mosques or writing on political message boards.

41. The White House, http://www.whitehouse.gov/ (last visited Jan. 30, 2010) (urging the public to connect with the White House on MySpace, Facebook, Twitter, iTunes, YouTube, Vimeo, LinkedIn, and Flickr).

42. Posting of Saul Hansell to the New York Times Bits Blog, *The Nation's Chief Information Officer Speaks*, http://bits.blogs.nytimes.com/2009/03/05/the-nations-new-chief-information-officer-speaks/ (Mar. 5, 2009, 14:57 EST).

43. *See, e.g.*, Transparency and Open Government, 74 Fed. Reg. 4685 (Jan. 21, 2009); Posting of Beth Noveck to The White House Blog, *Enhancing Citizen Participation in Decision-Making*,

information that has nothing to do with civic engagement. Governments can even see their "friends'" personal information (e.g., photographs, videos, political and religious affiliations, contact lists, wall musings, and the like) if their friends' privacy settings permit.[44]

Solove's taxonomy can help agency officials and other policymakers identify privacy risks associated with these kinds of Government 2.0 activities.[45] The taxonomy draws attention, for example, to agencies that use individuals' social-media information for purposes other than garnering the public's input on policy matters, such as law enforcement, immigration, and tax purposes (Solove's secondary-use problem).[46] Solove's theory also recognizes the litany of harms that secondary use can pose for individuals: erroneous arrests, incorrect designations as terrorists, or even deportation.[47] Just as with fusion-center–generated intelligence, the information gleaned from social-media data can chill identity-forming and expressive activities.

To be sure, decision makers from the legislative and executive branches ultimately may continue fusion centers and Government 2.0 sites despite the privacy problems they create on the grounds that they serve other more important interests, such as national security or public participation. Nonetheless, Solove's taxonomy can help policymakers work through their decisions in a thorough and systematic manner. His pragmatic approach is a crucial step to developing thoughtful policy to address our networked age's privacy problems. To the extent that other countries conceptualize privacy problems in similar ways, Solove's taxonomy may be particularly persuasive to policymakers who aim to fashion internationally acceptable privacy standards (pp. 183–87).

III. The Evolutionary Process: Refining and Clarifying

Understanding Privacy does important work in cutting through the "fog of confusion that often envelops the concept of privacy" (p. 11). Solove's command of the literature, both philosophical and legal, is impressive. His thoroughness, however, risks giving the reader the impression that his theory, and its resulting taxonomy, is complete. To the contrary, Solove not

---

http://www.whitehouse.gov/blog/Enhancing-Citizen-Participation-in-Decision-Making/ (June 10, 2009, 13:08 EST) (explaining that Government 2.0 platforms allow government to benefit from the public's expertise on policy matters).

44. Citron, *One-Way Mirror*, *supra* note 9, at 6.

45. In June 2009, the Department of Homeland Security hosted a conference to address the privacy risks of Government 2.0, at which one of the authors spoke. Danielle Citron, Remarks at the U.S. Dep't of Homeland Sec. Workshop: Government 2.0: Privacy and Best Practices (June 22, 2009), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_gov20_June2009_transcripts_day1.pdf.

46. *See* Citron, *One-Way Mirror*, *supra* note 9 (employing Solove's taxonomy to assess privacy implications of Government 2.0). Agencies also could employ computer algorithms that infer a person's involvement in religious or political groups from her social contacts. Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. Rev. 741, 759–60 (2008).

47. *See, e.g.*, Citron, *One-Way Mirror*, *supra* note 9, at 2 n.3, 7 n.40.

only acknowledges that his framework is not the last word in this conversation; he invites others to test, doubt, criticize, amend, support, and reinterpret his vision of privacy (p. ix).

Although Solove seems confident that others are up to the task of applying and refining his understanding of privacy, we worry that without further guidance, they might upend the very approach he has crafted. In this regard, we would have liked for him to say more about the process of balancing and how his theory can resist ossification and remain dynamic over time. In the following Sections, we describe these issues, and begin to consider how Solove might shape his theory's evolution in the future.

A. *The Process of Balancing*

According to Solove, because the value of privacy cannot be found in the abstract, we must balance it against countervailing interests in concrete situations (p. 75–77). Solove is aware that balancing has its critics. Some detractors argue that privacy interests cannot be converted into quantifiable terms sufficient for balancing, while others contend that the process of balancing is itself too rudimentary to reconcile conflicts between opposing values in any meaningful way.

Solove's answer to the first qualm is persuasive: privacy is too multifaceted to fit into a single metric, as he demonstrates at length in his discussion of traditional approaches to conceptualizing privacy. Solove's response to concerns about the cursory nature of balancing also strikes us as largely correct: balancing must, and can, be conducted in a rigorous and thoughtful manner. If Solove could assure us that every decision maker had his deep understanding of privacy, we might be satisfied with this answer.

Given the difficult nature of these decisions, however, we think decision makers would benefit enormously from further guidance. In particular, we hope that in the future, Solove will consider adding (1) safeguards against nonpragmatic decision making, (2) "rules of thumb" for ordering competing privacy interests, and (3) a discussion of the negative externalities than can result from upholding certain privacy claims.

1. *Safeguards against Nonpragmatic Decision Making*

Solove's pragmatic, consequentialist account of balancing gives weight to outcomes that are best for society, but determining that society's stake in a particular privacy claim outweighs its interest in nonprivacy concerns may not always be obvious. Solove might answer, as some Wittgensteinian philosophers do, by saying, "Look to the circumstances!"[48] This response, however, supposes that all decision makers come to the circumstances as trained pragmatists (or tabula rasa).

To the contrary, when faced with the challenges of assessing what is best for society, decision makers may lapse into an approach that simply reflects

48. JUDITH GENOVA, WITTGENSTEIN: A WAY OF SEEING 44 (1995).

their overarching philosophies, preferences, or emotions.[49] Naturally, all decision making involves some degree of discretion, but many areas of privacy law embrace flexible standards that are particularly vulnerable to this concern.[50] Moreover, when decision makers employ unitary theories to render decisions, Solove's efforts to engage them in systematic and rigorous pragmatism are undermined.

One way to combat nonpragmatic balancing is to require decision makers, such as chief privacy officers ("CPOs") and legislators, to explain their assessment of the interests at stake and why society would be better off with a particular outcome.[51] In so doing, Solove's pragmatic approach could take cues from administrative[52] and criminal law,[53] which have long championed the prophylactic power of requiring hearing officers and judges to explicitly state the reasons for their decisions. If policymakers involved in privacy law were held to similar standards, two positive results would accrue.

First, a transparent process might reduce the likelihood that personal views and overarching philosophies would thwart the pragmatic balancing process that Solove espouses. Second, a well-documented record of privacy decisions could signal to Solove and others when certain aspects of his taxonomy require amendments, revisions, or additions. This type of "ongoing conversation," which is at the core of Solove's approach, will only be enhanced by the openness that transparency creates (p. ix).

---

49. *See generally* RICHARD A. POSNER, HOW JUDGES THINK 19–56 (2008) (describing nine positive theories of judicial behavior, including the attitudinal approach, which explains that "judge's decisions are best explained by the political preferences that they bring to their cases," and psychological theory, which views judges' choices as influenced by "nonrational drives and cognitive illusions"); Stefanie A. Lindquist & Frank B. Cross, *Empirically Testing Dworkin's Chain Novel Theory: Studying the Path of Precedent*, 80 N.Y.U. L. REV. 1156, 1205–06 (2005) (explaining that "[j]udicial decisionmaking is influenced by precedent, but also by ideology and other factors"); Maxwell L. Stearns, *The Public Choice Case Against the Item Veto*, 49 WASH. & LEE L. REV. 385, 400 (1992) (explaining that lawmakers provide legislative benefits to groups when it "best serves their goals, including their primary objective of being re-elected").

50. For instance, in intrusion on seclusion and public disclosure privacy claims, plaintiffs must prove that the defendant's conduct is "highly offensive to a reasonable person." RESTATEMENT (SECOND) OF TORTS §§ 652B, 652D (1977). Judges could simply base decisions on the assumption that little is sacred in our culture of reality television, risking the marginalization of privacy interests. On the other hand, they might base rulings on an intuitive preference for privacy without consideration of social norms and the public's best interest.

51. As Paul Schwartz explores in a recent study about global data sharing in the private sector, businesses increasingly take privacy seriously, hiring chief privacy officers and chief information security officers. PAUL M. SCHWARTZ, THE PRIVACY PROJECTS, MANAGING GLOBAL DATA PRIVACY (2009), *available at* http://theprivacyprojects.org/wp-content/uploads/2009/08/The-Privacy-Projects-Paul-Schwartz-Global-Data-Flows-20093.pdf. This has marked an increasing professionalization of the privacy field. *Id.* at 24–25. As more businesses worldwide hire privacy practitioners to manage data flows, privacy decision making will be brought to the fore. *Id.* at 36–39.

52. *See* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1307 (2008); *see also* SEC v. Chenery Corp., 332 U.S. 194, 196–97 (1947) (explaining that judicial review can occur only when agencies explain their decisions with precision for "[i]t will not do for a court to be compelled to guess at the theory underlying the agency's action").

53. *See* North Carolina v. Pearce, 395 U.S. 711, 725–26 (1969) (holding that the judge's reason for imposing a more severe sentence after retrial must affirmatively appear in the record to avoid retaliatory motivation on the part of the sentencing judge).

Of course, no amount of transparency can force decision makers to follow Solove's taxonomy, a point that skeptics of his theory may raise. In response, Solove may want to recommend that privacy decision makers explicitly incorporate his taxonomy into their decision-making process. In recent years, airplane pilots and surgeons have adopted profession-specific checklists to help them make decisions under demanding and complicated circumstances.[54] Data suggest that these checklists enhance decision-making transparency, improve communication between parties to decisions, significantly reduce risks, and create a consistent process for industry-wide decision making.[55] A similar "guidance document" could prove effective in the privacy context by rendering decisions that sidestep well-accepted norms more transparent.[56]

2. *Rules of Thumb for Competing Privacy Interests*

Increasing decision-maker accountability through improved transparency may, however, be the easy case. It assumes, as Solove largely does throughout the book, that decision makers weigh privacy interests against nonprivacy ones, such as free speech, law enforcement, or national security. A crucial question of process arises, however, when one privacy interest conflicts with another. Consider these clashing privacy interests. In *The Unwanted Gaze*, Jeffrey Rosen argues that employees have an interest in carving out spaces where they can joke, let down their hair, and form intimate relationships free from official scrutiny.[57] What if employee *A* tells colleagues over lunch or via email about a lurid sexual relationship with coworker *B* and asserts that *B* has a sexually transmitted disease? While *A* has an interest in seclusion (sharing stories with co-workers without official interference), *B* has an interest in preventing the disclosure and distortion of sensitive personal information.

Resolving this case and others like it may be as straightforward as protecting the privacy interest that yields the best outcome for society. But when such an outcome is difficult to measure, the decision maker is faced with the tricky question of how to balance two competing privacy interests. Although Solove does not rank privacy harms, doing so might provide decision makers with more guidance when balancing competing privacy claims.

---

54. *See, e.g.*, ATUL GAWANDE, THE CHECKLIST MANIFESTO: HOW TO GET THINGS RIGHT (2009); WORLD HEALTH ORG., SURGICAL SAFETY CHECKLIST (2009), *available at* http://whqlibdoc.who.int/publications/2009/9789241598590_eng_Checklist.pdf; Atul Gawande, *A Surgical Safety Checklist to Reduce Morbidity and Mortality in a Global Population*, 360 NEW ENG. J. MED. 491 (2009).

55. Gawande, *supra* note 54. While we advocate a uniform checklist to ensure that decision makers pragmatically apply Solove's taxonomy to the circumstances at hand, we support a variety of context-specific outcomes.

56. *See, e.g.*, *Morning Edition: Atul Gawande's 'Checklist' for Surgery Success* (NPR radio broadcast Jan. 5, 2010) (explaining that when surgical teams are introduced to each other by name, fewer adverse events occur because there is more accountability to an agreed-upon protocol).

57. JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 122–25 (2000).

Of course, Solove could not frame the proposed ordering as a formal set of rules to apply in all circumstances, since doing so would detract from the level of generality that is central to his approach. He could, however, frame them as "rules of thumb,"[58] intended to guide decision makers who assess privacy interests on a case-by-case basis. If, for example, he suggested that, as a rule of thumb, harms resulting from disclosure outweigh harms resulting from seclusion, decision makers faced with that conflict would have a starting point for their analysis. They would not have to follow his scheme, but their decision not to might require justification.[59]

3. *Negative Externalities and Privacy Claims*

A related concern is whether Solove's theory provides sufficient description of the negative externalities than can result from protecting privacy in certain circumstances. His discussion of balancing at times supposes that privacy is an unmitigated good to be weighed against other goods, such as national security, free speech, or law enforcement.[60] In some cases, however, privacy can produce harms that Solove's taxonomy does not explicitly account for.

Privacy scholar Anita Allen's recent work reminds us, for example, that private conduct that seems self-regarding can nevertheless have detrimental consequences for others if it remains in the private sphere.[61] She describes one particularly salient case in which the decision to preserve a drug user's privacy—rather than hold her socially, legally, and morally accountable for her actions—resulted in numerous negative externalities: for her son, whose safety in his home was compromised; for her siblings, who repeatedly provided her with money for clothes, medical care, and ultimately rehabilitation; and for her parents, who often needed to take on the responsibility of raising her son.[62] In this situation, as in others Allen discusses,[63] the privacy mantra—"None of your business!"—must be weighed against the harms that flow from its uncritical acceptance.[64]

Although Solove's theory currently focuses more on privacy's value than its potential costs, there is nothing about his pragmatic approach to prevent

---

58. John Rawls, *Two Concepts of Rules*, 64 PHIL. REV. 3, 23 (1955).

59. An added benefit of this refinement is that it provides some control over an otherwise entirely discretionary outcome. *See supra* text accompanying note 49. Unlike in Europe, where privacy laws are enforced through privacy agencies, privacy claims in the United States are often resolved by courts, legislators, or private entities. P. 186. Rules of thumb might encourage greater transparency about the basis for decisions and combat decision makers' inclination to eschew thoughtful balancing of competing privacy interests for their own views.

60. *See, e.g.*, pp. 89–92.

61. ANITA L. ALLEN, WHY PRIVACY ISN'T EVERYTHING: FEMINIST REFLECTIONS ON PERSONAL ACCOUNTABILITY 6–7 (2003).

62. *Id.* at 56–67.

63. Allen notes that although health-information privacy is highly regulated, too much health-related secrecy can endanger others. *Id.* at 117–27.

64. *Id.* at 7.

him from addressing privacy's negative externalities in his future work. In fact, his views about the social nature of privacy already align with Allen's notion that purely private conduct is a myth.[65] Like Allen, Solove sees our lives as contextually interconnected and interdependent.[66] It is for that very reason that he measures privacy's value in terms of the social benefits that accrue from its protection.[67] To calculate privacy's costs in terms of the social harms that result from its protection would be a natural development of his analysis.[68]

B. *Ensuring Future Amendments*

Solove's taxonomy, while dynamic in concept, could nonetheless become ossified in practice. Although legal forms help us solve difficult problems by directing our thinking about substantive issues,[69] they tend to cabin law in ways that can frustrate its objectives.[70] This was true for Dean Prosser's categorization of the tort of privacy as four related wrongs in his seminal 1960 *Privacy* article[71] and his work as reporter of the Second Restatement of Torts.[72] Although Prosser's taxonomy gave privacy "a doctrinal unity" that it previously lacked,[73] it effectively halted the "torts' evolution."[74]

---

65. *Id.* at 44.

66. In this respect, Solove's pragmatism has much in common with Allen's feminism: both are policy-oriented approaches attentive to context; interested in (re)covering voices, stories, and problems that are excluded from traditional philosophies; and wary of noncontextual epistemologies that invoke overarching theories to the exclusion of actual social problems. The intersection between pragmatism and feminism has strong historical roots. *See, e.g.*, CHARLENE HADDOCK SEIGFRIED, PRAGMATISM AND FEMINISM: REWEAVING THE SOCIAL FABRIC (1996) (describing how early feminists contributed to the development of pragmatism); Jane Duran, *The Intersection of Pragmatism and Feminism*, HYPATIA, Spring 1993, at 159 (noting that feminists, like pragmatists, are critical of the standard preoccupation with universals); Judy D. Whipps, *Jane Addams's Social Thought as a Model for a Pragmatist-Feminist Communitarianism*, HYPATIA, Spring 2004, at 118 (explaining how Jane Addams's work and friendship with John Dewey spawned a feminist–pragmatist philosophy).

67. *See supra* Section I.B.

68. In accounting for privacy's negative externalities in his theory, Solove can allay the fear, held by some feminists, that overprivileging privacy can harm vulnerable members of society by isolating them from external interventions. *See* JANE ADDAMS, DEMOCRACY AND SOCIAL ETHICS 7 (Univ. of Ill. Press 2002) (1902) (suggesting that a social ethic built on feminist pragmatism allows us to "see the size of one another's burdens" rather than embedding us in isolated individualism).

69. *See* Jay M. Feinman, *The Jurisprudence of Classification*, 41 STAN. L. REV. 661 (1989); Duncan Kennedy, *Form and Substance in Private Law Adjudication*, 89 HARV. L. REV. 1685 (1976).

70. *See* Nancy Levit, *Ethereal Torts*, 61 GEO. WASH. L. REV. 136, 164–65 (1992).

71. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

72. Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL. L. REV. (forthcoming 2010).

73. *See* G. EDWARD WHITE, TORT LAW IN AMERICA 173 (2003).

74. Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 152 (2007).

Prosser's privacy torts have hardened, permitting tort law's recognition of privacy, but *only* as to those wrongs.[75]

Much like Prosser, whose strong reputation guaranteed the popularity of his taxonomy, Solove garners similar respect from policymakers, courts, and privacy advocates. As a result, decision makers could rely on Solove's taxonomy to identify privacy problems to the exclusion of others. This would no doubt betray Solove's purpose in writing *Understanding Privacy*. Solove does not want his taxonomy to be the "final word" on privacy, but rather a framework that develops in the face of emerging technologies (p. 197). He wants "to shift the discussion from elucidating the inherent meaning of the term 'privacy' to discussing the nature of certain problems" (p. 106). That shift is both productive and important. But it is worth pointing out the taxonomy's risk of calcification, if only as a call to policymakers to pay heed to Solove's evolving and situational vision of privacy.

Solove's *Understanding Privacy* also might have profited from discussing technological solutions to today's privacy problems. Technical solutions ex ante may be more effective than ex post balancing in certain circumstances. Viktor Mayer-Schönberger proposes, for example, that we store information with digital expiration dates that users set. Digital-storage devices could be designed to automatically delete information that has reached or exceeded its expiration date.[76] Expiration dates might also limit the amount of information that companies and governments have available about individuals at any one point in time.[77]

Jack Balkin has similarly called for governmental amnesia "by requiring that some kinds of data be regularly destroyed after a certain amount of time unless there [are] good reasons for retaining [it]."[78] In his previous work, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*, Solove also explores how altering the architecture of social network sites, blogs, and other Web 2.0 platforms might privilege privacy.[79] *Understanding Privacy* would benefit from a similar consideration of the positive role that technological solutions can play in addressing the privacy problems described in his taxonomy.

---

75. *See* WHITE, supra note 73, at 176.

76. MAYER-SCHÖNBERGER, *supra* note 9, at 171.

77. *Id.* at 175.

78. Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 21 (2008).

79. SOLOVE, *supra* note 12, at 200–04. Solove suggests that social-network sites should change their default settings to inhibit the sharing of personal information widely. *Id.* at 201. In that sense, companies, instead of the law, would act as privacy entrepreneurs. *Id.*; *see also* Citron, *One-Way Mirror*, *supra* note 9 (explaining how the architecture of Facebook fan sites ensures that government agencies cannot view social media information of individuals).

CONCLUSION

In the last decade, Solove's scholarship has shaped how academics courts, politicians, and the public think about privacy.[80] *Understanding Privacy* advances his project by providing a functional and flexible framework for policy makers and judges to apply when assessing current and future privacy problems. The strength of Solove's pragmatism is its openness to contingencies, cultural change, and unforeseen concerns. Though safeguarding pragmatism's promise will pose challenges, Solove's willingness to amend and revise his theory suggests he is up to the task. In this regard, Solove's scholarship has delivered on his intellectual mentor John Dewey's promise that "a problem well put is half-solved."[81] Solove and others can, and must, continue to evaluate, reassess, and reconstruct the taxonomy in the face of new privacy challenges.

80. Solove's work has deepened our appreciation of the privacy problems that current law overlooks or cannot manage. *See* Richards, *supra* note 12.

81. SOLOVE, *supra* note 12, at 6.