The Boundaries of Privacy Harm

M. RYAN CALO*

Just as a burn is an injury caused by heat, so is privacy harm a unique injury with specific boundaries and characteristics. This Essay describes privacy harm as falling into two related categories. The subjective category of privacy harm is the perception of unwanted observation. This category describes unwelcome mental states—anxiety, embarrassment, fear—that stem from the belief that one is being watched or monitored. Examples of subjective privacy harms include everything from a landlord eavesdropping on his tenants to generalized government surveillance.

The objective category of privacy harm is the unanticipated or coerced use of information concerning a person against that person. These are negative, external actions justified by reference to personal information. Examples include identity theft, the leaking of classified information that reveals an undercover agent, and the use of a drunk-driving suspect's blood as evidence against him.

The subjective and objective categories of privacy harm are distinct but related. Just as assault is the apprehension of battery, so is the perception of unwanted observation largely an apprehension of information-driven injury. The categories represent, respectively, the anticipation and consequence of a loss of control over personal information.

This approach offers several advantages. It uncouples privacy harm from privacy violations, demonstrating that no person need commit a privacy violation for privacy harm to occur (and vice versa). It creates a "limiting principle" capable of revealing when another value—autonomy or equality, for instance—is

---

* Director, Consumer Privacy Project, Center for Internet and Society, Stanford Law School. My sincere thanks to Danielle Keats Citron, Daniel Solove, Chris Hoofnagle, Siva Vaidhynathan, Paul Ohm, Neil Richards, Katherine Strandburg, Woodrow Hartzog, "Dissent," and other participants at the Privacy Law Scholars Conference 2010. Thanks also to Nicklas Lundblad, Stefania Fusco, Samuel Bray, and Elizabeth Pollman for commenting on earlier drafts. Thanks to Katherine Merriam for research assistance.

more directly at stake. It also creates a "rule of recognition" that permits the identification of a privacy harm when no other harm is apparent. Finally, this approach permits the measurement and redress of privacy harm in novel ways.

INTRODUCTION

A burn is an injury caused by heat. It has symptoms. It admits of degrees. When a doctor diagnoses a burn, she immediately gains insights into how best to treat it. She can rule out other causes. She can even make recommendations on how to avoid this particular harm in the future.

What is a privacy harm? What makes it distinct from a burn or some other harm? We are often at a loss to say.[1] Privacy harm is conceptualized, if at all, as the negative consequence of a privacy violation. Far from a source of leverage or insight, privacy harm often operates as a hurdle to reform or redress. A privacy harm must be "cognizable," "actual," "specific," "material," "fundamental," or "special" before a court will consider awarding compensation.[2] Leading commentators question whether privacy harm is much of a harm at all.[3]

---

1. Few have endeavored to define privacy harm. Instead, scholars mostly approach the topic by defining the underlying concept of privacy and describing privacy violation. *See, e.g.*, ALAN F. WESTIN, PRIVACY & FREEDOM (1967); Charles Fried, *Privacy*, 77 YALE L.J. 475 (1968); Richard B. Parker, *A Definition of Privacy*, 27 RUTGERS L. REV. 275, 280 (1974) (defining privacy as "control over who can sense us"); Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (defining privacy as "the right to be let alone"). *But see* Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877 (2003); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 482 (2006) [hereinafter Solove, *A Taxonomy of Privacy*] (understanding privacy in terms of "specific activities that pose privacy problems"); Paul Ohm, The Benefits of the Old Privacy: Restoring the Focus to Traditional Harm, Privacy Law Scholars Conference (June 4, 2010). This Essay addresses Daniel Solove's inventive approach in Part I.B.

2. *See* Doe v. Chao, 540 U.S. 614, 620 (2004) ("The Government claims the minimum guarantee [of the Privacy Act] goes only to victims who prove some actual damages. We think the Government has the better side of the argument."); *id.* at 625–26 (remarking on the intent of Congress of "avoiding giveaways to plaintiffs with nothing more than 'abstract injuries'" (quoting Los Angeles v. Lyons, 461 U.S. 95, 101–02 (1983))); *see also* Lambert v. Hartman, 517 F.3d 433 (6th Cir. 2008) (finding that loss of personal information at issue implicated neither liberty nor property); Doe I v. Individuals, 561 F. Supp. 2d 249, 257 (D. Conn. 2008) (requiring privacy harm to be "special" in order to proceed anonymously); *cf.* Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1232 (2003) [hereinafter Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*] ("[P]rivacy is most protected in situations where damages can be defined palpably . . . .").

3. Richard Posner in particular takes a dim view of privacy harm. *See, e.g.*, Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245, 251 (2008) [hereinafter Posner, *Privacy, Surveillance, and Law*] ("Privacy is the terrorist's best friend . . . ."); Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 398 (1978) ("At some point nondisclosure becomes fraud."); *see also* STEWART A. BAKER, SKATING ON STILTS: WHY WE AREN'T STOPPING TOMORROW'S TERRORISM (2010); AMATAI ETZIONI, THE LIMITS OF PRIVACY (1999); William J. Stuntz, *Secret Service: Against Privacy and Transparency*, NEW REPUBLIC, Apr. 17, 2006, at 12.

This Essay does not attempt to furnish a new definition of privacy, nor to catalogue the many values that privacy protects. Rather, it describes privacy harm as a unique type of injury with its own characteristics and mechanisms.[4] By delineating the specific boundaries of privacy harm, this Essay furnishes a defensible means by which to rule out and recognize privacy harms. It also permits measurement and redress of privacy harms in novel ways.

I argue here that the vast majority of privacy harms fall into just two categories—one subjective, the other objective.[5] The subjective category of privacy harm is the perception of unwanted observation. This category describes unwelcome mental states—anxiety, for instance, or embarrassment—that accompany the belief that one is or will be watched or monitored. Examples include the harm experienced by the tenants in *Hamberger v. Eastman*,[6] the unease caused by a massive data breach, and the concern over generalized surveillance at issue in the Keith case[7] and *Laird v. Tatum*.[8]

The objective category of privacy harm is the unanticipated or coerced use of information concerning a person against that person. These are negative, external actions justified by reference to personal information. Examples include the unanticipated sale of a user's contact information that results in spam and the leaking of classified information that exposes an undercover intelligence agent.[9] An example of a known but coerced use might be found in *Schmerber v. California*, where a drunk-driving suspect's blood was drawn without his consent and then introduced at trial as evidence against him.[10]

The subjective and objective categories of privacy harm are distinct but related. Just as assault is the anticipation of battery, so is the perception of unwanted

---

4. This Essay does not attempt to capture all of the senses—"spatial," "decisional," "proprietary," "physical"—in which commenters use the word "privacy." *See* Anita L. Allen, *Genetic Privacy: Emerging Concepts and Values*, *in* GENETIC SECRETS: PROTECTING PRIVACY AND CONFIDENTIALITY IN THE GENETIC ERA 31, 34 (Mark A. Rothstein ed., 1997) (describing four dimensions of privacy); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1202–05 (1998) (describing three dimensions to privacy). Nor does it attempt to create a list of the values that privacy protects. *See, e.g.*, DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008) [hereinafter SOLOVE, UNDERSTANDING PRIVACY]; WESTIN, *supra* note 1. Rather, it argues that privacy harm is unique in that it is a harm tied broadly to observation. *See infra* Part II (describing this relationship in detail).

5. By "subjective," I mean internal to the mind of the victim. By "objective," I mean external. My use of the terms generally comports with their usage in traditional psychology, see Jay Moore, *Radical Behaviorism and the Subjective-Objective Distinction*, 18 BEHAV. ANALYST 33, 33 (1995), with an important exception: I am counting events that are subjective to person A as objective to person B. *See infra* note 11.

6. 206 A.2d 239, 241 (N.H. 1964) (landlord surreptitiously recorded the conversations of his tenants).

7. United States v. U.S. District Court (*Keith*), 407 U.S. 297 (1972). This case is sometimes referred to as the "Keith case" after the district court judge, Judge Damon Keith, who ordered the government to turn over the results of its surveillance.

8. 408 U.S. 1 (1972).

9. *See, e.g.*, Wilson v. Libby, 498 F. Supp. 2d 74 (D.D.C. 2007) (dismissing for "special factors").

10. 384 U.S. 757 (1966).

observation largely an apprehension of information misuse. This Essay is not a metaphysical inquiry into the nature of privacy. But the approach does build upon a standard conception. The subjective and objective components of privacy harm are two sides of a well-worn coin: the loss of control over information about oneself or one's attributes.[11]

This Essay begins in Part I by exploring the advantages of describing boundaries in the first place. Delimiting privacy harm furnishes both a "limiting principle" and a "rule of recognition."[12] There are circumstances when ruling out privacy harm may force courts and theorists to confront other basic values such as autonomy or equality. We see this most vividly in the context of contraception, abortion, and sodomy regulation, where privacy obviates the perceived need to grapple with other crucial, yet perhaps more politically contestable, values.[13] Conversely, courts sometimes resist recognition of an unfamiliar harm in the absence of a concrete test or an obvious perpetrator.

Part II describes a set of actual boundaries and properties in detail and discusses the relative advantages of this approach. The approach "fits" the facts in the sense that it captures most situations we think of as causing privacy harm.[14] It adds conceptual clarity by unifying psychological and material injuries in ways we have not before. By uncoupling privacy *harms* from privacy *violations*, moreover, the approach debunks a widely held view—that privacy harm can only occur when one human being observes another. Privacy harm can and does occur in the absence of a human perpetrator.

Understanding its mechanics also permits the measurement of privacy harms in novel ways. With subjective privacy harms, for instance, we can ask about the degree of antipathy toward the observation, as well as the extent of perceived

---

11. *See, e.g.*, WESTIN, *supra* note 1, at 7 ("Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."); Fried, *supra* note 1, at 483 (conceiving of privacy as "control over knowledge about oneself"); Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 236 (1977) (defining privacy as "autonomy or control over the intimacies of personal identity"); Parker, *supra* note 1, at 280 (defining privacy as "control over who can sense us"); *see also* Nat'l Cable & Telecomms. Ass'n v. Fed. Commc'ns Comm'n, 555 F.3d 996, 1001 (D.C. Cir. 2009) ("It is widely accepted that privacy deals with determining for oneself when, how, and to whom personal information will be disclosed to others."). According to Paul Schwartz, "[t]he leading paradigm on the Internet and in the real, or offline world, conceives of privacy as personal right to control the use of one's data." Paul A. Schwartz, Commentary, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 820 (2000).

12. *See* H.L.A. HART, THE CONCEPT OF LAW 97–107 (1961) (introducing the concept of a rule of recognition to distinguish law from mere commands backed by threats).

13. *See infra* notes 19–29 and accompanying text. Identifying a privacy harm obviates the need to grapple with different values in other contexts as well. In *E.I. duPont de Nemours & Co. v. Christopher*, 431 F.2d 1012, 1016 (5th Cir. 1970), for instance, the court found that aerial photographs of a plant by a competitor constituted an invasion of "commercial privacy." Arguably, the act was better described as an instance of unfair competition.

14. *See* Parker, *supra* note 1, at 276 (describing the importance that a theory of privacy "fit the data").

observation. Thus, in *De May v. Roberts*, where a woman allowed a doctor's friend to watch her give birth on the false assumption that the friend was a fellow medical professional, the degree of observation was limited but highly unwanted.[15] Conversely, observation in a public place is implicitly accepted. Yet closed-circuit television ("CCTV") surveillance of public streets could still rise to the level of harm in my view if extensive.

Part III addresses various counterarguments. Scholars have included "threats," "risks," and "architectural harms" as privacy harms.[16] I would not, and I believe it will be easier to understand and avoid such harms once they are distinguished from the privacy harms that partly constitute them. I also hold that privacy harms can occur without privacy violations and vice versa. I defend this approach, acknowledging the possibility of accidental or even autogenic privacy harm, as when a paranoid schizophrenic holds the mistaken belief that he is under surveillance, and questioning the harm of the classic privacy violation—the hidden Peeping Tom.

I. WHY DELIMIT PRIVACY HARM?

The purpose of this Essay is to delineate the boundaries of privacy harm and describe its inner mechanics. But why is the search for a boundary worthwhile? What do we gain from distinguishing privacy harm from other harm or from the underlying concept of privacy? Part I.A argues that delimiting privacy harm helps to address and protect privacy and other values. Part I.B addresses an influential approach to conceptualizing privacy—Daniel Solove's "taxonomy" of privacy problems—that is implicitly skeptical of the possibility and usefulness of delimiting privacy harm.[17]

A. Why Setting Boundaries Matters

Privacy harm is a crucial but under-theorized aspect of an important issue. We should understand its mechanism and scope if only for the sake of conceptual clarity. But identifying its boundaries will also be of practical use to scholars, courts, and regulators attempting to vindicate and protect privacy and other values.

---

15. 9 N.W. 146 (Mich. 1881).

16. Daniel Solove is a prominent proponent of this view. *See, e.g.*, Solove, *A Taxonomy of Privacy*, *supra* note 1, at 487–88 (discussing risk of harm and power imbalance); *see also* DANIEL SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 97–101 (2004) [hereinafter SOLOVE, THE DIGITAL PERSON]; Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, *supra* note 2, at 1232 ("A number of privacy problems do not consist merely of a series of isolated and discrete invasions or harms, but are systemic in nature."); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001) [hereinafter Solove, *Privacy and Power*]; Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1706 ("The accretion problem is this: Once an adversary has linked to anonymized databases together, he can add the newly linked data to his collection of outside information and use it to unlock other anonymized databases.").

17. *See generally* Solove, *A Taxonomy of Privacy*, *supra* note 1.

A working definition of privacy harm gives us a "limiting principle" that guards against dilution and may reveal other important harms. It also means having a "rule of recognition" that permits the identification of novel privacy harms as they emerge.

1. A Limiting Principle

Misdiagnosing a problem makes it hard to fix. Imagine what would happen if a doctor confused heartburn with a first-degree burn. Our unlikely doctor might prescribe antibiotic ointment and ibuprofen in place of antacids and diet change. The patient might actually feel better at first—reassured by the visit to the doctor or desensitized by the painkiller—but the treatment would not ultimately be effective.

Courts can also misdiagnose harm, leading to a topical salve in place of a true cure. In the absence of a limiting principle, mistake or hesitance can lead courts to see privacy harm in situations where privacy is arguably not the primary value at stake.[18] And, having identified the harm, a court may not be inclined to revisit the diagnosis.

In *Griswold v. Connecticut*, for instance, the Supreme Court struck down a Connecticut statute prohibiting the use of contraception.[19] Arguably what was at issue in *Griswold* was the basic liberty of a woman or a couple to decide whether to procreate. But the Court understood—and continues to understand—contraception regulation in terms of marital privacy.[20] Appellant "Jane Roe" argued against the infamous restriction at issue in *Roe v. Wade* on the ground that it restricted her liberty.[21] The Court struck the regulation down on the basis that the "right of privacy . . . is broad enough to encompass a woman's decision whether or not to terminate her pregnancy."[22]

---

18. *See* Solove, *A Taxonomy of Privacy*, *supra* note 1, at 563 (noting the "common pitfall" that a court might identify privacy harm "to the exclusion of all others"). The absence of a limiting principle is generally frowned upon at law, forming the basis of many counter-arguments and adverse rulings. *See, e.g.*, Wilkie v. Robbins, 551 U.S. 537, 561 n.11 (2007) ("We ground our judgment on the elusiveness of a limiting principle . . . ."); IBP, Inc. v. Alvarez, 546 U.S. 21, 23 (2005) ("No limiting principle allows this Court to conclude that the waiting time here is such an activity . . . ."); United States v. Winstar Corp., 518 U.S. 839, 886 (1996) ("[I]ts failure to advance any limiting principle at all would effectively compromise the Government's capacity as a reliable, straightforward contractor whenever the subject matter of a contract might be subject to subsequent regulation, which is most if not all of the time.").

19. 381 U.S. 479 (1965).

20. *Id.* at 485–86.

21. *See* Roe v. Wade, 410 U.S. 113, 129 (1973). On another view, equality is the value at stake in the abortion cases. *See* MARK A. GRABER, RETHINKING ABORTION: EQUAL CHOICE, THE CONSTITUTION, AND REPRODUCTIVE POLITICS 11 (1999) ("Equal choice provides broader constitutional grounds for attacking pro-life policies than do conventional pro-choice defenses of *Roe*."). *But see* Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1106 (2006) (book review) (arguing that decisional privacy cases can be read as "telling an information privacy story as well").

22. *Roe*, 410 U.S. at 153.

In *Lawrence v. Texas*, the Supreme Court invalidated a Texas statute criminalizing certain sexual acts between two people of the same gender.[23] The Court began by acknowledging that "[t]he instant case involves liberty of the person both in its spatial and its more transcendent dimensions."[24] Rather than rely on liberty alone, however, or invoke the notion of equality, the Court again turned to the private nature of the activity to strike down the restriction as applied.[25]

One might reasonably question whether denying women or homosexuals the right to exercise control over their own bodies is best understood as a privacy harm. This Essay will argue in the next Part that a privacy harm is something else entirely. Nevertheless, a harm has occurred. The restrictions at issue in *Roe* and *Lawrence* fell upon a specific group (women, gays) and hence could be said to implicate equality.[26] Such rules also interfere with the proverbial "pursuit of happiness" on free terms. These are very basic values that eventually must surface and be confronted.[27]

Protecting the right to use contraception or choose sexual partners merely because they happen to take place in private—the same approach we take with the possession of obscenity[28]—does not actually address these issues by legitimizing the underlying conduct. Quite the opposite. This approach may be helpful in the short run, that is, before society is prepared to recognize the real issues at stake. In the long run, however, it operates to obscure and perhaps demean the important harms taking place.[29]

This is not to deny that privacy has value. If anything, it is overuse of the term that risks its diffusion into a meaningless catchall. Thus, a second advantage to having a limiting principle is that it helps protect against dilution of the concept of

---

23. 539 U.S. 558 (2003).

24. *Id.* at 562.

25. *Id.* at 578 ("The petitioners are entitled to respect for their private lives. The State cannot demean their existence or control their destiny by making their private sexual conduct a crime."). For an insightful discussion of *Lawrence* and its implications for equality and citizenship, see Sonia K. Kaytal, *The Dissident Citizen*, 57 UCLA L. REV. 1415 (2010).

26. *See* GRABER, *supra* note 21, at 11; Kaytal, *supra* note 25.

27. Both equality under the law and the right to the free pursuit of happiness are specifically mentioned in our founding documents (as amended). Privacy is not. *See* U.S. CONST. amend. XIV, § 1; THE DECLARATION OF INDEPENDENCE pmbl. (U.S. 1776).

28. *See* Stanley v. Georgia, 394 U.S. 557, 568 (1969) ("As we have said, the States retain broad power to regulate obscenity; that power simply does not extend to mere possession by the individual in the privacy of his own home."). Having sex with one's preferred partner, using contraception, and terminating a pregnancy are not like possessing obscenity. It should also be noted that claims of privacy harm have operated at times to protect abhorrent conduct such as domestic violence. *See* Reva B. Siegel, *"The Rule of Love": Wife Beating as Prerogative and Privacy*, 105 YALE L.J. 2117 (1996).

29. Privacy is a value we are notoriously—and increasingly—comfortable balancing against other values. Many believe that privacy does not invoke the highest standards of scrutiny reserved for the abrogation of equality or other values mentioned specifically in the Constitution that are at the core of what it means to be a liberal democracy. *See supra* note 3 (listing examples of scholars who do not view privacy harm as deserving a high level of scrutiny). By delimiting privacy harm, we can rule out this layer and reveal the true value that makes our citizens and jurists rightly uncomfortable.

privacy.[30] If too many problems come to be included under the rubric of privacy harm—everything from contraception to nuisance—we risk losing sight of what is important and uniquely worrisome about the loss of privacy.[31] Setting boundaries concentrates the notion of privacy harm and bolsters the case for why privacy deserves to be enforced in its own right.

2. A Rule of Recognition

A hasty diagnosis may obscure a serious medical problem. But sometimes doctors look at a constellation of symptoms and see no disease at all. Courts, too, can resist recognition of an unfamiliar harm.[32] Understanding the boundaries and mechanics of privacy harm may also allow for a "rule of recognition," that is, a means to identify and evidence a non-obvious problem.

Take as an example the singling out of vulnerable populations for marketing. The elderly and other groups can experience difficulty looking critically at offers to purchase. Setting aside actual fraud, there is extensive evidence that marketers assemble and trade lists of individuals who are members of these particularly vulnerable populations.[33] These lists are often compiled on the basis of sensitive information such as age and disability, and generally contain the person's name, address, and other personally identifiable information.[34]

Without looking at the underlying privacy issue, however, it becomes hard to understand and regulate this problem. The elderly and the disabled live in society just as everyone else. They consume goods, vote, and communicate with the outside world—all desirable outcomes. The elderly will inevitably encounter offers and ads. But once we recognize that vulnerable populations are specifically located, targeted, and pitched on the basis of sensitive personal information,[35] we can move to secure that information and reduce their exposure to advertising to random chance.

In other instances, a principled approach to recognizing privacy harm will make it possible to bolster and evidence our initial intuitions. We tend to think of

---

30. *Cf*. Griswold v. Connecticut, 381 U.S. 479, 509 (1965) (Black, J., dissenting) ("One of the most effective ways of diluting or expanding a constitutionally guaranteed right is to substitute for the crucial word or words of a constitutional guarantee another word or words, more or less flexible and more or less restricted in meaning.").

31. This is also the reason that we protect commercial speech less than noncommercial speech under the First Amendment; we wish to avoid the dilution of the force of First Amendment protection "simply by a leveling process." Board of Trustees v. Fox, 492 U.S. 469, 481 (1989).

32. *See, e.g.*, Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373, 392–95 (2009) (discussing the history of the emotional distress tort and the reticence of the courts to allow recovery).

33. *See The Modern Permanent Record and Consumer Impacts from the Offline and Online*, *Testimony of Pam Dixon Before the Subcommittee on Communications, Technology, and the Internet, and the Subcommittee on Commerce, Trade, and Consumer Protection of the House Committee on Energy*, WORLD PRIVACY FORUM (Nov. 19, 2009), www.worldprivacyforum.org/pdf/TestimonyofPamDixonfs.pdf.

34. *See id.*

35. *See id.*

unsolicited spam e-mail as a privacy harm, for instance, and federal law regulates it in part on this basis.[36] But the analogy is strained: on what theory is getting unwanted commercial e-mail any more a violation of privacy than getting your home mailbox stuffed with toilet paper as a prank? Moreover, the content of unsolicited e-mail is entitled to some First Amendment protection, which makes it harder to regulate.[37]

Seeing the privacy harm in unsolicited e-mail requires looking closely at how mass spam is generated through a particular lens. As several scholars point out, spam is often targeted on the basis of purchased or misappropriated private information.[38] Spam requires an e-mail address, generally considered personally identifiable information, to reach an inbox.[39] This suggests a novel way to regulate spam or junk mail: directly as "objective privacy harm."[40]

B. The Taxonomic Approach: A Critique

At least one leading privacy scholar has questioned both the possibility and usefulness of defining privacy or privacy harm. In a series of influential articles and books, Daniel Solove rejects the notion that privacy can or should be reduced to any one, or even multiple, concept(s).[41] According to Solove, all previous attempts to do so have failed for being over- or underinclusive.[42] Solove abandons the

---

36. *See* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM"), 15 U.S.C. §§ 7701–7713 (2006); S. REP. NO. 108-102 (2003) (legislative history referring to the impact of spam on privacy).

37. *See, e.g.*, Jaynes v. Commonwealth, 666 S.E.2d 303, 314 (Va. 2008), *cert. denied*, 129 S. Ct. 1670 (2009) (striking down state anti-spam law as overbroad).

38. *See* Kang, *supra* note 4, at 1204 ("The junk mail, phone call, or message invades my space, spamming my physical, voice, and electronic mailboxes. More importantly but less obviously, the initial targeting of that junk mail to me may have involved access to and analysis of personal information . . . ." (citation omitted)); Reidenberg, *supra* note 1, at 881–82 ("[T]he receipt of junk mail or junk telemarketing calls are nuisances for most people. They are intrusive, though infrequently at the level of noxiousness. The annoyance is a derivative consequence of an underlying privacy wrong. The underlying privacy wrong is the misuse of personal information that gives rise to the unwanted solicitation.").

39. *See, e.g.*, California Online Privacy Protection Act, CA. BUS. & PROF. CODE § 22577(a)(3) (West 2008) (defining e-mail as personally identifiable information). Of course, much spam reaches inboxes through randomly generated e-mail addresses—automated guesswork supported by various inputs.

40. *See infra* Part II.B (defining objective privacy harm).

41. *See* SOLOVE, UNDERSTANDING PRIVACY, *supra* note 4, at 1–38; Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002) [hereinafter Solove, *Conceptualizing Privacy*]; Solove, *A Taxonomy of Privacy*, *supra* note 1, at 479–84. Solove's pragmatic and inclusive approach to privacy is widely cited, including by federal courts. *See, e.g.*, Nat'l Cable & Telecomms. Ass'n v. Fed. Commc'ns Comm'n, 555 F.3d 996, 1001 (D.C. Cir. 2009); Doe v. Biang, 494 F. Supp. 2d 880, 892 (N.D. Ill. 2006). Over seventy secondary sources have cited to *A Taxonomy of Privacy* since its publication in 2006.

42. *See generally* Solove, *Conceptualizing Privacy*, *supra* note 41. Solove uses one theory of privacy against another, that is, he "survey[s] the criticisms of various scholars regarding each other's conceptions of privacy and suggest[s] a number of [his] own." SOLOVE, UNDERSTANDING PRIVACY, *supra* note 4, at 8. Generally speaking, Solove's

quixotic search for a definition of privacy and instead develops a "taxonomy" of related but distinct activities that raise privacy problems, selected on the basis of what the right sorts of authorities associate with the concept.

For Solove, it is "no accident" that we refer to each of his sixteen subcategories of privacy harms "under the rubric of 'privacy.'"[43] But at the same time, "privacy issues are different from one another and do not have a core characteristic in common."[44] To reconcile this tension, Solove turns to philosopher Ludwig Wittgenstein's notion of "family resemblances."[45] Wittgenstein has denied that concepts necessarily share one common characteristic; "rather, they draw from a common pool of similar characteristics."[46]

Solove offers Wittgenstein's example of a family with common characteristics such as "build, features, colour of eyes, gait, temperament, etc."[47] "[E]ach child may have certain features similar to each parent, and the children may share similar features with each other, but they may not resemble each other in the same way. Nevertheless, they all bear a resemblance to each other."[48] The different aspects of privacy are like the members of the Wittgenstein family that share no common characteristic but instead create "a complicated network of similarities overlapping and crisscrossing: sometimes overall similarities, sometimes similarities of detail."[49]

In this way, Solove suggests the irrelevance and improvidence of attempting to set boundaries around the concept of privacy or privacy harm. Those boundaries will always fail by including activities that do not deserve the label "privacy," or leaving out ones that do. Solove specifically disavows the utility of isolating privacy harms from other sorts of harms. He is far more interested, he notes, in identifying problems than in classifying them as privacy problems per se.[50]

There is no denying the value of the complete, nuanced, and interconnected picture of privacy that Solove's taxonomy presents. Solove delivers what he promises, that is, "a framework for understanding privacy in a pluralistic and

---

criticisms "boil down to claims that the theories are too narrow, too broad, or too vague." *Id.* Having arranged a circular firing squad that leaves no scholar standing, Solove sets about his own conceptual project.

43. SOLOVE, UNDERSTANDING PRIVACY, supra note 4, at 46.

44. *Id.* at 45.

45. *Id.* at 42–44; *see also* Solove, *Conceptualizing Privacy*, *supra* note 41, at 1096–99 (discussing Wittgenstein's theory of family resemblances).

46. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 4, at 42; *see also id.* at 9.

47. *Id.* at 42.

48. *Id.* at 42–43.

49. *Id.* at 42.

50. In response to the anticipated argument that one subcategory of his taxonomy, that of "distortion," is not a true privacy harm, Solove counters: "But does it matter? Regardless of whether distortion is classified as a privacy problem, it is nevertheless a problem." Daniel J. Solove, "*I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 760 (2007) ("Whether a particular problem is classified as one of privacy is not as important as whether it is recognized as a problem."). Solove goes on to say that "[c]lassifying [distortion] as a privacy problem is merely saying that it bears some resemblance to other privacy problems, and viewing them together might be helpful in addressing them." *Id.*

contextual manner."[51] To see the limitations of this approach, however, and the lingering need for principles that delimit privacy harm, we need to examine how privacy problems come to be included in the taxonomy in the first place.

A taxonomy is a means of classification. Wittgenstein's notion of family resemblances notwithstanding, it turns out to be impossible to classify without reference to an "overarching principle."[52] A grocery list is a simple example. It contains items one needs that can be found in a grocery store. Oil does not go on a grocery list, tomatoes do. The same is true of a list or taxonomy of privacy harms. Criteria for inclusion or exclusion are essential.

Solove's criteria for inclusion involve recognition by the right sorts of authorities. His taxonomy "accounts for privacy problems that have achieved a significant degree of social recognition."[53] It captures "the kinds of privacy problems that are addressed in various discussions about privacy, laws, cases, constitutions, guidelines, and other sources."[54] Solove specifically turns to the law because "it provides concrete evidence of what problems societies have recognized as warranting attention."[55]

But what happens if someone disagrees with these sources? How does one go about *denying* that a given harm is a privacy harm? I've argued that it would be useful to deny that limits on abortion, contraception, and sodomy concern privacy because doing so could reveal the real values of, for instance, autonomy and equality. Conversely, how does one go about arguing that a new harm should be included as a privacy harm, before the right sorts of authorities have recognized it as such? We would have to wait until they do.[56]

Mere resemblance to other privacy harms is not enough. Sometimes we want to include something on a list that resembles no other item on it. We might want to say, for instance, that a foster or adopted child is part of a family, even in the

---

51. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 4, at 10.

52. *Id.* at 105 ("My taxonomy's categories are not based upon any overarching principle. We do not need overarching principles to understand and recognize problems."). Of course, a list could have more than one principle. A shopping list could contain both clothing and groceries. Indeed, several theories of privacy have more than one principle or dimension. *See, e.g.*, JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY 73–80 (2007) (describing three privacy "clusters"); Allen, *supra* note 4, at 34 (describing four dimensions to privacy); Kang, *supra* note 4 (describing three dimensions to privacy); *see also* Solove, *Conceptualizing Privacy*, *supra* note 41, at 1125–26 ("Other scholars also recognize that privacy cannot be consolidated into a single conception . . . . [Yet] they still circumscribe privacy based on the boundaries of each of the clustered conceptions.").

53. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 4, at 101–02.

54. *Id.* at 172.

55. *Id.* at 102.

56. Solove might argue that we recognize new harms by analogy to existing ones. But we would still need criteria for claiming something is a good or a bad analogy. As Danielle Keats Citron and Leslie Meltzer Henry point out in their review of *Understanding Privacy*, Solove must "say more about . . . how his theory can resist ossification and remain dynamic over time." Danielle Keats Citron & Leslie Meltzer Henry, *Visionary Pragmatism and the Value of Privacy in the Twenty-First Century*, 108 MICH. L. REV. 1107, 1120 (2010) (book review).

absence of overlapping "build, features, colour of eyes, gait, temperament, etc."[57] We might want to argue that a gay couple is a family so that one can visit the other in the hospital. The concept of family requires more than an ex post description of resemblances.[58] It necessitates a thick definition, predicated on normative and political commitments that permit analysis and disagreement.

Conversely, we might want to deny that two phenomena that resemble one another in certain ways are in fact the same. Skin burns and heartburn resemble one another in certain ways—they cause pain, for instance, and are both referred to as "burns" by the medical community. But they do not resemble one another in *the right ways*, that is, the ways that permit proper diagnosis and treatment. Resemblance is not enough in the face of disagreement; the question becomes *what resemblances matter*.

To be sure, Solove's approach makes many wise turns. It eschews the elusive search for a concept of privacy in favor of a pragmatic approach that focuses specifically on privacy problems and their resulting harms to individuals and society. But without a limiting principle or rule of recognition, we lack the ability to deny that certain harms have anything to do with privacy or to argue that wholly novel privacy harms should be included, which in turn can be useful in protecting privacy and other values. The next Part accordingly bites the proverbial bullet and defends a theory of privacy harm on its own terms.

II. THE OUTER BOUNDARIES AND CORE PROPERTIES OF PRIVACY HARM

Describing the outer boundaries and core properties of privacy harm helps to reveal values, identify and address new problems, and guard against dilution. But exactly what are those boundaries and properties? Little scholarship is devoted specifically to this question. This Part describes the contours and mechanics of privacy harm in detail.

I maintain that privacy harms fall into two categories. The first category is "subjective" in the sense of being internal to the person harmed. Subjective privacy harms are those that flow from the perception of unwanted observation. Subjective privacy harms can be acute or ongoing, and can accrue to one individual or to many. They can range in severity from mild discomfort at the presence of a security camera to "mental pain and distress[] far greater than could be inflicted by mere bodily injury."[59] Generally, to be considered harmful the observation must be *unwanted*. We hesitate to see subjective harm where, as often, the observation is welcome.[60] But actual observation need not occur to cause harm; perception of observation can be enough.

---

57. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 4, at 42 (citation omitted).

58. We might say that all families resemble one another in that they are a family. This would of course be circular.

59. Warren & Brandeis, *supra* note 1, at 196 (describing the harm associated with invasive journalism).

60. *See* SOLOVE, UNDERSTANDING PRIVACY, *supra* note 4, at 102 ("When a person consents to . . . these activities, there is no privacy violation."); Parker, *supra* note 1, at 282 ("If we tell someone that we are homosexual, we lose control over private information, but we do not necessarily lose privacy."); Warren & Brandeis, *supra* note 1, at 218 ("The right

The second category is "objective" in the sense of being external to the person harmed. This set of harms involves the forced or unanticipated use of information about a person against that person. Objective privacy harms can occur when personal information is used to justify an adverse action against a person, as when the government leverages data mining of sensitive personal information to block a citizen from air travel, or when one neighbor forms a negative judgment about another based on gossip. Objective harms can also occur when such information is used to commit a crime, such as identity theft or murder.[61] To constitute harm, the use must be *unanticipated* or, if known to the victim, *coerced*. Again, however, no human being actually needs to see the personal information itself for it to be used against the victim.

The subjective and objective categories of privacy harm are distinct but not entirely separate. Assault and battery are two distinct torts.[62] Each can occur without the other. They have different elements.[63] These two torts are nevertheless linked in that one is the apprehension of the other. The harm of assault is an internal or subjective state, specifically, the apprehension of unwanted touching.[64] The harm of battery is the unwanted physical contact itself.[65]

The two components of privacy harm are related in an analogous way. Objective privacy harm is the actual adverse consequence—the theft of identity itself or the formation of a negative opinion—that flows from the loss of control over information or sensory access.[66] Subjective privacy harm is, by and large, the perception of loss of control that results in fear or discomfort. The two categories are distinct but related. They are two sides of the same coin: loss of control over personal information.

Part II.A describes the subjective component of privacy harms. Part II.B describes the objective component. Thinking about privacy harm in this way confers multiple advantages, discussed in detail in Part II.C.

---

to privacy ceases upon the publication of the facts by the individual, or with his consent.").

61. *See* Remsburg v. Docusearch, Inc., 816 A.2d 1001 (N.H. 2003) (stalker killed woman after obtaining her work address from a data broker).

62. *Compare* RESTATEMENT (SECOND) OF TORTS § 21 (1965) (describing the tort of assault), *with id.* at § 13 (describing the tort of battery).

63. The elements of battery are (a) an act intended to cause a harmful or offensive contact with a person, (b) resulting directly or indirectly in actual harmful contact with that person or a third party. *Id.* at § 13. The elements of assault are (a) an act intended to cause a harmful or offensive contact, or an imminent apprehension of such a contact, (b) resulting in such imminent apprehension. *Id.* at § 21.

64. *See id.* § 21 cmt. c. ("In order that the actor shall be liable under the rule stated in this Section, it is only necessary that his act should cause an apprehension of an immediate contact, whether harmful or merely offensive. It is not necessary that it should directly or indirectly cause any tangible and material harm to the other.").

65. *See id.* § 13 cmt. a.

66. By "sensory access," I mean access to information in the form of sensory data. When a person loses sensory access, for purposes of this Essay, he loses the ability to keep someone from observing him physically. *Cf.* Parker, *supra* note 1, at 281 ("By 'sensed,' is meant simply seen, heard, touched, smelled, or tasted. By 'parts of us,' is meant the parts of our bodies, our voices, and the products of our bodies.").

A. Subjective Privacy Harms

The subjective category of privacy harm is the perception of unwanted observation, broadly defined. Watching a person directly—their body, brain waves, or behavior—is observation. So, too, is reading a report of their preferences, associations, and whereabouts. Observation can also include inference, as when we make "an observation" about someone on the basis of what we know about them. Observation, as this Essay understands the term, may include everything from a "casual observation" with an "inhibitive effect on most individuals that makes them more formal and uneasy,"[67] to Roger Clarke's concept of encompassing "dataveillance."[68]

The observation at issue must be "unwanted" to constitute a harm, lest almost any interaction rise to the level of a privacy problem. The law often considers consent to be binary;[69] aversion to observation, however, naturally admits of degrees. We can welcome observation or be neutral as to it. We can object to observation but a little or quite a lot. We may hold a slight antipathy for the bulk of observation that takes place in public, for instance, but be very upset by the prospect of observation in an intimate location[70] or during an embarrassing moment.[71]

The underlying cause of subjective privacy harm can be acute or ongoing. A person may feel embarrassed in the moment by a single act of observation, as when she walks through a backscatter device in airport security that creates a picture of her naked body.[72] Or she may feel an ongoing sense of regret about an embarrassing revelation lingering somewhere online.[73] In one recent example,

---

67. Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 447 (1980).

68. Roger Clarke, *Profiling: A Hidden Challenge to the Regulation of Data Surveillance*, 4 J.L. & INFO. SCI. 4032 (1993). Clarke defines dataveillance as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons." *Id.*; *see also* Roger A. Clarke, *Information Technology and Dataveillance*, *in* COMPUTERIZATION AND CONTROVERSY: VALUE CONFLICTS AND SOCIAL CHOICES 496 (Charles Dunlop & Rob Kling eds., 1991).

69. *See* Joshua Fairfield, *The Cost of Consent: Optimal Standardization in the Law of Contract*, 58 EMORY L.J. 1401, 1446 (2009) (bemoaning the "take it or leave it" nature of many contracts); *id.* at 1456 (urging courts to "stop treating contractual consent as binary—as existing or not existing").

70. The home in particular has been treated as sacrosanct under the law. *See* SOLOVE, UNDERSTANDING PRIVACY, *supra* note 4, at 3–4.

71. The federal government and several states have enacted so-called "up-skirt laws" in recognition that privacy violations can occur even in public places. *See, e.g.*, Video Voyeurism Prevention Act of 2004, 118 U.S.C. § 1801 (2006); H.R. REP. NO. 108-504, at 2–3 (2004) (referencing state laws and discussing legislative intent).

72. These devices immediately delete the image in most cases. For a discussion of backscatter devices, see Jeffrey Rosen, *Nude Awakening*, NEW REPUBLIC, Feb. 10, 2010, at 8; *see also* Emergency Motion for Stay of Agency Rule Decision Needed No Later than July 13, 2010, at 3–8, Electronic Privacy Information Center v. Napolitano, No. 10-1157 (D.C. Cir. July 2, 2010) (describing privacy issues with backscatter devices in detail).

73. *See generally* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET (2007). Subject to a few exceptions, websites and other

Reeves v. Equifax Information Services, a federal trial court denied a credit agency defendant's motion for summary judgment where the alleged harm was the emotional distress associated with the mere knowledge that a credit report remained uncorrected.[74]

Subjective harms need not occur in the moment; many feelings of violation have a delayed effect. In a seminal privacy case, *De May v. Roberts*, a woman gave birth in the presence of a doctor and a man she believed to be the doctor's medical assistant.[75] She learned only later that the man was the doctor's untrained acquaintance. Although she made no objection to the man's presence when she believed he was a medical professional, the court permitted her to recover for a privacy violation "upon afterwards ascertaining his true character."[76] It follows that many subjective privacy harms—a landlord's hidden microphone, for instance—will be backward looking insofar as the offending observation has already ended at the time of discovery (or because of it).[77]

A different privacy harm occurs where observation is systematic, that is, part of a plan or pattern. Pervasive individual monitoring is, for instance, a key component of control in domestic abuse situations.[78] Repeated "checking in" throughout the day is thought to be an early sign of domestic abuse.[79] It may also be that the so-called "learned helplessness" experienced by some abuse victims stems in part from having internalized the feeling of being monitored.

The Supreme Court has recognized the threat systematized governmental surveillance can impose on a citizenry. "The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power," the Court noted in the Keith case.[80] "Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation."[81] Although the Court in *Laird v. Tatum* found insufficient evidence

---

intermediaries are under no obligation to take pictures down even if they are adjudged by a court to be unlawful.

74. No. 2:09cv45KS-MTP, 2010 WL 2036661 (S.D. Miss. May 20, 2010).

75. 9 N.W. 146, 146 (Mich. 1881).

76. *Id.* at 149.

77. *See, e.g.*, Hamberger v. Eastman, 206 A.2d 239 (N.H. 1964) (landlord surveillance of tenants).

78. One category of the "Power and Control Wheel" developed by the Domestic Abuse Intervention Programs to detect abuse is "isolation." *See Power and Control Wheel*, DOMESTIC ABUSE INTERVENTION PROGRAMS, http://www.theduluthmodel.org/wheelgallery.php. Isolation is sustained by, inter alia, "tracking or monitoring activities and/or whereabouts." *Domestic Violence, Identifying Abuse and Abusers, Power and Control*, CITY OF RENTON, http://rentonwa.gov/living/default.aspx?id=1614.

79. *See* Melinda Smith & Jeanne Segal, *Domestic Violence and Abuse: Signs of Abuse and Abusive Relationships*, HELPGUIDE.ORG (Oct. 2010), http://helpguide.org/mental/domestic_violence_ abuse_types_signs_causes_effects.htm. The notion of a "gendered" or "male" gaze also underpins certain feminist scholarship around privacy. *See, e.g.*, Jeannie Suk, *Is Privacy a Woman?*, 97 GEO. L.J. 485, 489–91 (2009).

80. United States v. U.S. District Court (*Keith*), 407 U.S. 297, 314 (1972); *see supra* note 7 (describing why this case is commonly called the "Keith case").

81. *Keith*, 407 U.S. at 314; *see also id.* at 320 ("Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech. Security surveillances are especially sensitive

of harm to support the plaintiffs' claim of excessive government surveillance, it also noted its recognition of "constitutional violations" arising from the "deterrent or 'chilling' effect of governmental regulations that fall short of a direct prohibition against the exercise of First Amendment rights."[82]

Episodic solitude—in essence, the periodic absence of the perception of observation—is a crucial aspect of daily life. People need solitude for comfort, curiosity, self-development, even mental health.[83] As Alan Westin argues: privacy allows for "respite from the emotional stimulation of daily life";[84] "[t]o be always 'on' would destroy the human organism."[85] Charles Fried notes that, were our every action public, we might limit what we think and say.[86]

Indeed, the lack of any time away from others is a common feature of the modern dystopian novel. George Orwell's "telescreens" from *Nineteen Eighty-Four* continue to haunt the contemporary imagination.[87] In Yevgeny Zamyatin's *We*, the buildings are completely transparent.[88] The most frequently repeated act of mental conditioning in Aldus Huxley's *Brave New World* is the dislike of solitude.[89]

Importantly, the observation at issue need not be actual, only perceived or suspected. Many of the harms we associate with a person seeing us—embarrassment, chilling effects, loss of solitude—flow from the mere belief that one is being observed.[90] This is the exact lesson of the infamous Panopticon.[91] The

---

because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent.").

82. 408 U.S. 1, 11 (1972).

83. *See* SOLOVE, UNDERSTANDING PRIVACY, *supra* note 4, at 163–64 (cataloguing the role of solitude in daily life); *see also* BARRINGTON MOORE, JR., PRIVACY: STUDIES IN SOCIAL AND CULTURAL HISTORY 73 (1984); Julie E. Cohen, *Cyberspace as/and Space*, 107 COLUM. L. REV. 210 (2007); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject As Object*, 52 STAN. L. REV. 1373, 1423–28 (2000) [hereinafter Cohen, *Examined Lives*]; Schwartz, *supra* note 11, 834–43; Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1640–41 (1999) [hereinafter Schwartz, *Privacy and Democracy*]; Lior Strahilevitz, *Reputation Nation: Law in an Era of Ubiquitous Personal Information*, 102 NW. U. L. REV. 1667, 1736 (2008) ("Privacy theorists have long argued that protecting privacy is essential so that individuals can relax, experiment with different personalities to figure out who they truly are, or develop the insights that will make them more productive citizens." (footnotes omitted)).

84. WESTIN, *supra* note 1, at 35.

85. *Id.*

86. Fried, *supra* note 1, at 483–84 ("If we thought that our every word and deed were public, fear of disapproval or more tangible retaliation might keep us from doing or saying things which we would do or say if we could be sure of keeping them to ourselves.").

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

88. YEVGENY ZAMYATIN, WE 28 (Clarence Brown trans., Penguin Books 1993) (1924) (citizen D-503 refers to the "splendid, transparent, eternal glass" that composes nearly every structure).

89. ALDUS HUXLEY, BRAVE NEW WORLD 241 (Harper Perennial 1946).

90. *See* M. Ryan Calo, *People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship*, 114 PENN. ST. L. REV. 809, 842–48 (2010).

91. *See* MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 200 (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1977). The Panopticon was designed by early nineteenth century philosopher Jeremy Bentham. JEREMY BENTHAM, THE

tower is always visible, but the guard's gaze is never verifiable. As Michel Foucault explores, prisoners behave not because they are actually being observed, but because they believe they might be.[92] The Panopticon works precisely because people can be mistaken about whether someone is watching them and nonetheless suffer similar or identical effects.[93]

A related point can be made regarding dummy cameras[94] and, as it turns out, mere representations of people. Even where we know intellectually that we are interacting with an image or a machine, our brains are hardwired to respond as though a person were actually there.[95] This reaction includes the feeling of being observed or evaluated.[96] People pay more for coffee on the honor system, for instance, if eyes are depicted over the collection box.[97] Our attitude, our behavior, even our physiology can and do change in circumstances where no real person is there.[98]

B. Objective Privacy Harms

Subjective privacy harms are injuries individuals experience from being observed. But why does the belief that one is being observed cause discomfort or apprehension? In some instances, the response seems to be reflexive or physical. The presence of another person, real or imagined, creates a state of "psychological

---

PANOPTICONIC WRITINGS (Mirin Bozovic ed., 1995).

92. *See* FOUCAULT, *supra* note 91, at 200–01.

93. *Id.* at 201 ("Hence the major effect of the Panopticon: to induce in the inmate a state of consciousness and permanent visibility that assures the automatic functioning of power."). *Cf.* Arthur R. Miller, *Privacy: Is There Any Left?*, 3 FED. CT. L. REV. 87, 100 (2009) ("[I]t does not matter if there really is a Big Brother on a screen watching us. It does not matter in the slightest. The only thing that matters is that people think there is a Big Brother watching them."). It may be argued that this harm is not one of privacy but of discipline. I believe it is both: privacy can be harmed by observation in service of discipline, just as the body can be harmed by the application of disciplinary force.

94. Customers purchasing certain "awkward" products experienced measurably higher levels of discomfort when a dummy camera was trained on the register. *See* Thomas J.L. van Rompay, Dorette J. Vonk & Marieke L. Fransen, *The Eye of the Camera: Effects of Security Cameras on Prosocial Behavior*, 41 ENV'T & BEHAV. 1, 60–74 (2009).

95. Calo, *supra* note 90, at 811 ("Study after study shows that humans are hardwired to react to technological facsimiles . . . as though a person were actually present. . . . We of course understand intellectually the difference between a person and a computer-generated image. But a deep literature in communications and psychology evidences that we 'rarely make[] distinctions between speaking to a machine and speaking to a person' . . . . " (alteration in original) (quoting CLIFFORD NASS & SCOTT BRAVE, WIRED FOR SPEECH: HOW VOICE ACTIVATES AND ADVANCES THE HUMAN-COMPUTER RELATIONSHIP 4 (2005))).

96. *Id.* at 838–42 (collecting studies).

97. *Id.* at 812.

98. *Id.* at 813. This means that even a robot can invade solitude.

arousal" that can be harmful if excessive and unwanted.[99] The embarrassment of being seen naked seems similarly ingrained, at least throughout Western society.[100]

Often, however, we are apprehensive about being observed due to the concern that such observation will lead to some adverse, real-world consequence. The consequence could be concrete: TJX customers worry about that company's data breach, for instance, because it could lead to costly identity theft.[101] Or the consequence could be more diffuse, as in the formation of a negative judgment about a person at issue in the tort of public disclosure of private fact.[102]

Objective privacy harms are those harms that are external to the victim and involve the forced or unanticipated use of personal information. By "personal," I do not mean "personally identifiable" in the statutory sense.[103] Rather, I mean specifically related to a person. The use of general information to justify an action is not a privacy harm. Advertisers might use the "fact" that a beautiful spokesperson makes a product more attractive in an effort to sell everyone cars. It is only when specific information about a person—age, preferences, vulnerabilities—is used to market to that person that privacy is implicated.

The use must also be unanticipated. It is not a privacy harm to use a person's information if he himself publicized it or if he understood and agreed to the use.[104]

---

99. Psychological arousal refers to the absence of relaxation and assurance that correlates with the presence of others. *See* Lee Sproull, Mani Subramani, Sara Kiesler, Janet H. Walker & Keith Waters, *When the Interface Is a Face*, 11 HUM.-COMPUTER INTERACTION 97, 112 (1996); van Rompay et al., *supra* note 94, at 62.

100. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 4, at 53, 147; Posner, *Privacy, Surveillance, and Law*, *supra* note 3, at 245 ("In many cultures, including our own, there is a nudity taboo.").

101. *In re* TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 491 (1st Cir. 2009) ("In January 2007, TJX Companies, Inc. ('TJX'), headquartered in Massachusetts and a major operator of discount stores, revealed that its computer systems had been hacked. Credit or debit card data for millions of its customers had been stolen. Harm resulted not only to customers but, it appears, also to banks that had issued the cards ('issuing banks'), which were forced to reimburse customers for fraudulent use of the cards and incurred other expenses.").

102. *See* William Prosser, *Privacy*, 48 CALIF. L. REV. 383, 392–98 (1960). Note that the event may be internal to the person forming the negative opinion, but external, and hence "objective" as I'm using the term, to the subject of the opinion. Moreover, subjective and objective harms are not always easily severable. Blackmail, for instance, involves the adverse use of information in the form of a threat to disclose.

103. Many statutory obligations only apply to "personally identifiable information," that is, information such as name or social security number that can be used to identify a specific individual. *See, e.g.*, California Online Privacy Protection Act, CAL. BUS & PROF. CODE §§ 22575–22579 (West 2004) (privacy policy requirement for websites on pages where they collect personally identifiable information); CAL. CIV. CODE §§ 1785.11.2, 1798.29, 1798.82 (West 2009) (breach notification requirement in the event of compromised personally identifiable information); CONN. GEN. STAT. ANN. § 36a-701b (West 2009 & Supp. 2010) (same); GA. CODE ANN. § 10-1-910, 911 (2009) (same).

104. *See supra* note 60 (citing sources). Agreement exists on a spectrum. There can be privacy harm where, as often, the subject had little choice but to disclose. *Cf.* Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full Disclosure Future*, 105 NW. U. L. REV. (forthcoming 2011) (arguing that trends in the information

Thus, it is not necessarily a privacy harm to trade an e-mail address for a chance to win a sweepstakes where both parties understand that the e-mail will be used for marketing purposes.[105] Nor is it a privacy harm for one person to decide not to speak to another at a party because that person is not attractive. We expect and tacitly consent to these sorts of discriminations.

The problem arises when, as often, an individual has no idea that the information was even collected or, if she does, how it will be used. This fundamental tension plays out vividly in the context of online privacy. Many consumers have little idea how much of their information they are giving up or how it will be used.[106] A consumer may sign up for a sweepstakes and never realize that doing so places him on a marketing list and increases his volume of unsolicited e-mails.[107] Or a person may share information on a social networking website and not realize that it could be used to deny her a job or admission to college.[108]

American privacy law addresses this problem not by preventing people from sharing data or companies from using it, but by attempting to ensure that uses are anticipated and, to a lesser degree, chosen. At least one state law requires websites that collect personally identifiable information to disclose what they collect, how it is used, and with whom it is shared.[109]

The Federal Trade Commission has also emphasized the "fair information practice principle" of notice in its enforcement activity around privacy, practically to the exclusion of the other principles.[110] Although this system is increasingly seen

---

economy will make disclosure mandatory as a practical matter).

105. Of course, it may run afoul of state anti-lottery statutes if furnishing an e-mail constitutes "consideration." *See, e.g.*, CAL. PENAL CODE § 319 (2010) ("A lottery is any scheme for the disposal or distribution of property by chance, among persons who have paid or promised to pay any valuable consideration for the chance of obtaining such property or a portion of it . . . .").

106. *See* Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE "INFORMATION ECONOMY" 341, 360–61 (Jane K. Winn ed., 2006) (explaining that privacy policies are difficult to understand and that most Americans therefore do not read them); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1502 (2000) ("In theory, the parties to a transaction can always contract for confidentiality. This is unrealistic due because consumers suffer from *privacy myopia*: they will sell their data too often and too cheaply. Modest assumptions about consumer privacy myopia suggest that even Americans who place a high value on information privacy will sell their privacy bit by bit for frequent flyer miles." (emphasis in original)).

107. *See* Froomkin, *supra* note 106, at 1502.

108. A 2009 study showed that forty-five percent of employers surveyed used social networks to vet potential hires. *See* Jenna Wortham, *More Employers Use Social Networks to Check Out Applicants*, N.Y. TIMES (Aug. 20, 2009), http://bits.blogs.nytimes.com/2009/08/20/more-employers-use-social-networks-to-check-out-applicants. A more recent study commissioned by Microsoft found that seventy percent of human resource professionals surveyed (n = 1200) have turned down a potential job application based solely on online reputation information. CROSSTAB, INC., ONLINE REPUTATION IN A CONNECTED WORLD 3 (2010).

109. *See* California Online Privacy Protection Act, CAL. BUS & PROF. CODE §§ 22575–22579 (West 2004).

110. The five fair information practice principles are notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress. *See* Fed. Trade Comm'n, *Fair Information Practice Principles*, *in* PRIVACY ONLINE: A REPORT TO CONGRESS (1998),

as flawed,[111] it reflects the liberal intuition that free and anticipated uses of personal information do not constitute privacy harms and must remain unregulated.

Alternatively, a person might suspect how information will be used and would not give the information up willingly precisely for that reason. She is nevertheless coerced into doing so. This concern appears to inform the privacy dimension of the Fourth Amendment right to be free from unreasonable searches and seizures. We permit such coercion but, recognizing the harm, we require adequate process. The concern may even animate the age-old right not to self-incriminate, though in practice this right is limited to statements.[112]

The coercion at issue in *Schmerber v. California*, where a drunk driving suspect's blood was drawn and introduced as evidence against him,[113] was relatively straightforward. But coercion exists on a spectrum.[114] Many important activities, from air travel to medical care, are premised upon giving up information or revealing one's body in potentially demeaning and uncomfortable ways. There may indeed be little alternative to surveillance in daily life. As Richard Posner observes, "If an entire city is known to be under camera surveillance . . . submission to it is as a practical matter involuntary . . . ."[115]

The action justified by reference to personal information must of course be adverse; otherwise, it is likely not a "harm" in the common understanding of the word.[116] Doctors look at our bodies not to harm us but to protect our health. Adversity is not always an easy question. Federal Trade Commission staff observe that targeted online ads benefit consumers,[117] for instance, whereas a recent study

---

available at http://www.ftc.gov/reports/privacy3/fairinfo.shtm. Most of the Commission's enforcement has focused on notice and security. *See* Cate, *supra* note 106. For an excellent survey of relevant Federal Trade Commission enforcement activity, see Marcia Hofmann, *Federal Trade Commission Enforcement of Privacy*, *in* PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE (1st ed. 2009).

111. *See, e.g.*, Cate, *supra* note 106, at 358 ("[T]he FTC's approach . . . reduces notice and consent to a mere formality—a checkbox that consumers must select to obtain a desired product or service."); Cohen, *Examined Lives*, *supra* note 83, at 1397–98; Schwartz, *Privacy and Democracy*, *supra* note 83, at 1661–64.

112. Thus, a suspect or defendant could be compelled to show his person in a lineup or make a voice or handwriting sample. *See* United States v. Wade, 388 U.S. 218 (1967) (lineup); United States v. Dionisio, 410 U.S. 1 (1973) (voice sample); Gilbert v. California, 388 U.S. 263 (1967) (handwriting sample). We might think of these and similar cases as involving objective privacy harm.

113. 384 U.S. 757 (1966).

114. At issue in *Nelson v. NASA*, for instance, was whether a certain category of scientist could be subjected to a rigorous background investigation on pain of termination. 512 F.3d 1134 (9th Cir. 2008). The case is pending before the Supreme Court.

115. Posner, *Privacy, Surveillance, and the Law*, *supra* note 3, at 247.

116. For a detailed discussion of the concept of harm in the legal context, see 1–4 JOEL FEINBERG, THE MORAL LIMITS OF THE CRIMINAL LAW (1987).

117. *See* FED. TRADE COMM'N, ONLINE BEHAVIORAL ADVERTISING: MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES 2 (2007), *available at* http://www.ftc.gov/opa/2007/12/principles.shtm ("[B]ehavioral advertising provides benefits to consumers in the form of free web content and personalized ads that many consumers value . . . .").

suggests that a majority of consumers find targeting problematic.[118] But the question of whether an action is adverse is basically familiar. Courts and regulators confront the question of what is adverse in many statutes and standards without paralysis.[119]

Finally, as with subjective privacy harms, human beings need not physically review personal information for that information to form the basis of an adverse action. There does not have to be a human observer who gathers and misuses information. Machines are perfectly competent to comb through private information and use it to make automatic decisions that affect us in tangible and negative ways.

As Danielle Keats Citron explains in another context:

> In the past, computer systems helped humans apply rules to individual cases. Now, automated systems have become the *primary* decision makers. These systems often take human decision making out of the process of terminating individuals' Medicaid, food stamp, and other welfare benefits. . . . Computer programs identify parents believed to owe child support and instruct state agencies to file collection proceedings against those individuals. Voters are purged from the rolls without notice, and small businesses are deemed ineligible for federal contracts.[120]

Citron explores the harm of automated decision making from the perspective of due process.[121] But such automated decisions can also constitute privacy harms where, as often, they involve the unanticipated or coerced use of sensitive personal information.[122]

Consider an example raised by Richard Posner and others to demonstrate that no privacy harm occurs unless and until a human sees the information at issue.[123] Google's e-mail service Gmail automatically scans users' e-mails and displays

---

118. Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley & Michael Hennessey, *Americans Reject Tailored Advertising and Three Activities That Enable It*, Working Paper Series, Social Science Research Network (Sep. 29, 2009), *available at* http://ssrn.com/abstract=1478214.

119. *See, e.g.*, Padilla v. Kentucky, 130 S. Ct. 1473, 1483 (2010) (requiring component counsel to inform client of potential "adverse immigration consequences"); Ricci v. DeStefano, 129 S. Ct. 2658, 2672 (2009) (defining "disparate impact" as having a "disproportionately adverse effect on minorities"); Safeco Ins. Co. of America v. Burr, 551 U.S. 47, 62 (2007) (discussing "adverse effects" under the Fair Credit Reporting Act).

120. Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1252 (2008) (emphasis in original) (footnotes omitted).

121. *Id.* at 1281–88.

122. I have argued that knowing the boundaries of privacy harm can help reveal the real value at stake. *See supra* Part I.A. This is not to deny that more than one value can be implicated at a time.

123. *See* Posner, *Privacy, Surveillance, and Law*, *supra* note 3, at 249 (discussing Gmail's automated ad delivery feature); Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 627 (2011) (same).

advertising on the basis of keywords it picks out.[124] Google assures users that no human ever sees the e-mail, and we have no reason to disbelieve the claim.[125] Gmail users and the people who write to them are consequently unlikely to be judged, embarrassed, or otherwise harmed by Google employees on the basis of e-mail content.

But imagine that a user of another e-mail client is trying to sell something, say, a bicycle, to a Gmail user. Google automatically scans the sender's incoming e-mail, and, alongside the offer of sale, Google might display links to bicycles sold by its paid advertisers. In other words, Google in some cases may scan the content of an incoming e-mail and use it, without notice or consent, to compete directly with its author. The harm here may be negligible, but there is no basis to rule out even the *theoretical* possibility that this unwanted use of private information against its subject could implicate privacy.

Or take a more dramatic example. The police ask a psychologist for her patient session notes. The psychologist objects, citing the Constitution, professional privilege, and general privacy concerns—this is really intimate information after all. The police respond: "Don't worry. No one is going to look at this. We're going to scan all the notes and anytime someone mentions smoking marijuana or a few other illegal things we'll use the address on the file to send them a ticket. But no police officer will ever see anything in the notes." We may object for other, distinct reasons, but again, it makes no sense to remove this scenario from consideration as a privacy harm.[126]

Automated collection, processing, and decision making are not going anywhere.[127] Citron's work evidences the phenomenon and how it is even today serving to deny citizens tangible benefits, assess penalties, and even restrict travel on the basis of sometimes intimate information.[128] Citron identifies a series of instances—airline travelers mislabeled by the data-matching programs that underpin the "No Fly" list; parents mislabeled as deadbeats by an automated system—where machines use information in surprising ways.[129] We do not know the exact source of the information these systems rely upon, but there is every indication that it includes personal information not supplied by citizens for this purpose.

---

124. Tokson, *supra* note 123, at 627.

125. *Id.*

126. This hypothetical can be seen as a riff on Lawrence Lessig's example of a government computer virus that searches across citizens' computers for contraband information. *See* LAWRENCE LESSIG, CODE VERSION 2.0, at 20–23 (2006). For Lessig, the virus hypothetical reveals a "latent" constitutional problem—namely, whether the program's activities implicate the Fourth Amendment. *Id.*

127. If anything, it will likely continue to grow. *See* Citron, *supra* note 120, at 1251–52 (explaining the administrative forces that give rise to autonomous decision making); Tokson, *supra* note 123, at 602−04 (chronicling the extensive nature of automation).

128. Citron, *supra* note 120, at 1263–67.

129. *Id.*

C. The Advantages of Seeing Privacy Harm in This Way

I have argued that privacy harms fall into two distinct but meaningfully related categories. There are several advantages to this approach. It represents a tolerable "fit": most recognized privacy harms can be described in terms of the subjective perception of unwanted observation or the unanticipated or coerced use of a person's information against them. And yet it also draws boundaries, thus guarding against dilution, uncovering other values, and permitting recognition of undocumented privacy problems.

The approach also demonstrates the inadequacy of a widely held view about the nature of privacy harm: that it can only occur when one human senses another. For Richard Posner, privacy harm only occurs when a person accesses and misuses information that he should not.[130] No harm occurs from the mere collection or even processing of information by, for instance, a computer.[131] The information must wind up in the hands (or eyes) of a "sentient being."[132] Even then, a robust "professionalism"—whether by a doctor or intelligence officer—can serve to mitigate the privacy harm.[133] And while observation alone registers on the scale,[134] real privacy harm seems to occur for Posner only where the observer takes an action they should not with physical or monetary consequences.

Posner is not alone in arguing that human access to sensory or other personal information is a necessary component of privacy harm. Eric Goldman "question[s] how data mining, without more, creates consequential harm."[135] Processing alone, if never "displayed to a human," leads to "no adverse consequence of any sort."[136] Orin Kerr's proposed test for a Fourth Amendment search is also "exposure-based" and denies, if not any harm, then any constitutional implication where information is merely processed by a computer.[137] Richard Parker defines privacy specifically and at length as "control over who can sense us,"[138] implying that a privacy harm only occurs when a human senses us when we do not want them to. Parker goes on to say that "the collection of data by government and other institutions . . . is not a loss of privacy per se, but rather a threat to one's privacy."[139]

---

130. Posner, *Privacy, Surveillance, and Law*, *supra* note 3, at 253–54.

131. *Id.* at 254.

132. Richard Posner, Editorial, *Our Domestic Intelligence Crisis*, WASH. POST, Dec. 21, 2005, at A31.

133. Posner, *Privacy, Surveillance, and Law*, *supra* note 3, at 251 (analogizing intelligence officers looking at citizens' information to doctors looking at patients' bodies).

134. *Id.* at 245 ("A woman (an occasional man as well) might be disturbed to learn that nude photographs taken surreptitiously of her had been seen by a stranger in a remote country before being destroyed.").

135. Eric Goldman, *Data Mining and Attention Consumption*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY 225–26 (Katherine Strandburg & Daniela Stan Raicu eds., 2005).

136. *Id.* at 228.

137. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 551 (2005).

138. Parker, *supra* note 1, at 281.

139. *Id.* at 285.

The requirement that a human see the person or information at issue for a privacy harm to occur also finds expression in the law to the extent that searches by nonhumans do not necessarily implicate the Fourth Amendment. In a pair of seminal Fourth Amendment cases, the Supreme Court held that the use of a police dog to determine whether drugs were present in a container was not a search because the dog only alerted when it came upon an illegal substance and no officer saw the container's contents until he knew there was contraband.[140] The argument has even been deployed to argue for greater privacy protection under the Fourth Amendment.[141]

One advantage of this Essay's approach is that it captures the full range of harms from observation. First, the *perception* of observation can still be harmful even if no human being ever sees the information.[142] It is enough to believe that one is being watched to trigger adverse effects. Second, machines are clearly capable of collecting, processing, and acting upon private information in harmful ways without any human being ever seeing it.[143] If anything, we have embarked upon ever greater automation.[144] Both components of my approach capture this potential harm in a way that privacy harm as "unwanted sensing" cannot.

This approach enjoys other advantages. The two components of privacy harm are testable. Courts and regulators are capable of investigating—particularly with the help of experts—whether a person felt observed, whether she consented to observation or collection, and whether she anticipated a given use of her information.[145] The categories are explicit and, for the most part, uncontroversial. But they are sufficiently unmoored from any particular activities so as to apply to novel phenomena and situations.[146]

The approach also furnishes criteria for ranking the relative severity of privacy harm. In the case of subjective privacy harms, we can look to the degree of aversion to any observation as distinct from the extent of observation experienced. High degrees of both translate into the greatest harm, but harm is possible if either is very high.[147]

---

140. Illinois v. Caballes, 543 U.S. 405 (2005); United States v. Place, 462 U.S. 696, 707 (1983) ("A 'canine sniff' by a well-trained narcotics detection dog, however, does not require opening the luggage. It does not expose noncontraband items that otherwise would remain hidden from public view, as does, for example, an officer's rummaging through the contents of the luggage.").

141. In *Automation and the Fourth Amendment*, Matthew Tokson makes the case that "users whose information is exposed only to automated Internet systems incur no loss of privacy and only a minimal risk of eventual exposure to humans." Tokson, *supra* note 123, at 586. He concludes on this basis that the third-party doctrine should not apply. *Id.* at 586–87.

142. *See supra* notes 90–98 and accompanying text.

143. *See supra* notes 120–129 and accompanying text.

144. *See supra* note 127.

145. *But see* Schwartz, *Privacy and Democracy*, *supra* note 83, at 1661–64 (describing the view that users consent to the terms they encounter online as the "autonomy trap").

146. *See supra* Part I.B.

147. The two are, obviously, related. Extensive surveillance can breed greater aversion. The idea here is that each context, state, or activity may be attended by a specific level of aversion to observation that can in turn be invaded to a lesser or greater degree.

This insight is useful in describing the notoriously difficult problem of "privacy in public."[148] The law's approach to privacy in public is monolithic: it generally refuses to see a privacy violation where the observation takes place in public on the theory that people in public have no reasonable expectation of privacy.[149] In the absence of a privacy violation, meanwhile, we tend not even to look for privacy harm.

Having described the properties of subjective privacy harm, however, we can now say that the degree of aversion is small—two out of ten, for instance. But we do not stop here: we must multiply the degree of aversion by the extent of surveillance. In the case of massive outdoor surveillance by closed-circuit television camera (CCTV) or pervasive aerial photography, especially where the footage is stored and processed, the *extent* of the surveillance is enormous. Thus, the ultimate harm can be quite large (eight out of ten).[150]

Similarly, we can calculate objective privacy harms by reference to the degree of knowledge or consent, as distinct from the severity of the information use. Consider the Federal Trade Commission's recent complaint against Sears.[151] The Commission conceded that Sears gave notice to consumers that the software they were downloading would track them in some measure.[152] The Commission still found Sears to have engaged in an unfair and deceptive trade practice, however, due to the extensive nature of that tracking.[153] This Essay's approach permits the formalization and expansion of this intuition.

---

148. This is the notion that public information, or events that take place in public, should nevertheless enjoy a measure of privacy. *See* Josh Blackman, *Omniveillance, Google, Privacy in Public, and the Right to Your Digital Identity: A Tort for Recording and Disseminating an Individual's Image over the Internet*, 49 SANTA CLARA L. REV. 313, 323–24 (2009).

149. *See, e.g.*, Shulman v. Grp. W Prods., Inc., 955 P.2d 469, 490 (1998) ("[T]here is no liability for . . . . observing [a person] or even taking his photograph while he is walking on the public highway." (alteration in original) (quoting RESTATEMENT (SECOND) OF TORTS § 652B cmt. C)); *see also* Andrew Jay McClurg, *Bringing Privacy Law out of the Closet: A Tort Theory of Liability for Intrusions in Public Places*, 73 N.C. L. REV. 989, 990–91 (1995) ("Tort law clings stubbornly to the principle that privacy cannot be invaded in or from a public place."); Joseph Siprut, *Privacy Through Anonymity: An Economic Argument for Expanding the Right of Privacy in Public Places*, 33 PEPP. L. REV. 311, 320 (2006) ("[A]lthough individuals are afforded some degree of protection based on privacy rights while in public, the scope of this protection is narrower than one might expect.").

150. *Compare* De May v. Roberts, 9 N.W. 146 (Mich. 1881), *with* Laird v. Tatum, 408 U.S. 1 (1972). In *De May*, the surveillance involved only one man (the doctor's friend) but during a particularly intimate time (birth). *De May*, 9 N.W. at 146. In *Laird*, the surveillance complained of largely involved "the collection of information about public activities." *Laird*, 408 U.S. at 6. Although the information in *Laird* was not intimate in the same sense, the plaintiffs still objected enough to its systematic monitoring by the government to file a lawsuit. *Id.* at 10; *see also* Blackman, *supra* note 148, at 323.

151. In the Matter of Sears Holdings Management Corporation, FTC File No. 082 3099 (Sept. 9, 2009).

152. *Id.* ¶ 8.

153. *Id.* ¶¶ 13–14.

III. OBJECTIONS

This Essay has defended the project of delimiting privacy harm and argued that most privacy harms, properly understood, fall into two categories. A number of objections could be leveled. One pertains to scope: the approach deals only with specific instances of individual or, at most, group harm. It does not appear to deal with the increased risk of harm, as in the case of a security breach, and so-called "architectural harm."[154]

A second objection is that the approach does violence to some of our shared understandings. There is a basic sense in which a theory of privacy harm should *feel* right. It should to the extent possible "fit with . . . our shared intuitions of when privacy is or is not gained or lost."[155] I argued in Part I that we should be able to rule out certain harms as being privacy harms, even where authorities have used the rubric of privacy to address a particular problem. But even granting that privacy harm has boundaries, my approach may appear counterintuitive both in that it admits of autogenic, in the sense of causeless, privacy harm and that it appears to deny any harm in a paradigmatic privacy villain, the hidden Peeping Tom. This Part deals with each objection in turn.

A. The Risk of Harm Objection

California-based non-profit Privacy Rights Clearinghouse keeps track of data breaches. As of this writing, the organization estimates that over 355 million records containing personal information have been exposed to the public since January 2005.[156] Nearly every state has a data breach notification law that requires individuals or firms to notify victims or the government in the event of a breach.[157]

Data breaches do not automatically lead to identity theft, blackmail, or other malfeasance. Many of the 355 million records presumably have not been misused. Rather, the exposure increases the *risk* of negative outcomes. Isn't this increased risk privacy harm in its own right, one might argue? If so, why do I not account for it?

As an initial matter, data breaches register as subjective privacy harms. When a consumer receives a notice in the mail telling her that her personal information has leaked out into the open, she experiences the exact sort of apprehension and feeling of vulnerability the first category of privacy harm is concerned about. That is, she believes that there has been or could be unwanted sensing of her private information. The same is true, to a lesser degree, when any of us read about a data breach—we feel less secure in our privacy overall.

But what if there is a data breach or other increased risk of adverse consequence and the "victim" never knows about it? Then there has been neither subjective nor objective privacy harm, unless or until the information is used. Worse still, it would

---

154. *See supra* note 16.

155. *See* Parker, *supra* note 1, at 276.

156. *See Chronology of Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/ar/ChronDataBreaches.htm#Total.

157. *See supra* note 103 (listing four examples of state statutes requiring notification).

appear on this analysis that breach notification is a net evil in that it creates (subjective) privacy harm where there would be none.

Here I disagree with this premise. A risk of privacy harm is no more a privacy harm than a chance of a burn is a burn. They are conceptually distinct: one is the thing itself, the other the likelihood of that thing.[158] A feeling of greater vulnerability can constitute privacy harm, just as the apprehension of battery can constitute a distinct tort. But there is no assault or battery without the elements of apprehension or unwanted contact.

Consider another example outside of privacy: a disease that compromises the afflicted's immune system but causes no other adverse physical consequence.[159] Clearly there is a harm: the sufferer lives in a state of panic and cannot travel in the world as before. But we gain little and lose much by conflating AIDS—an immunosuppressant—with the seasonal flu. Each virus has its own mechanism, characteristics, and treatment, even if the former makes the latter more deadly.

Similarly, it does not disparage the seriousness of a data breach, nor the inconvenience of having to protect against identity theft, to deny that any objective privacy harm has yet occurred. If anything, clarifying the nature of the harm at risk should help us protect against that harm actually occurring by selecting the appropriate remedy. The goal of some rules is to deter specific harms, for instance; others exist to empower the vulnerable or hinder the powerful in an effort to make harm less likely.[160] Data breach notification laws fulfill both functions, even if they are technically the "but for" cause of one category of privacy harm.

B. The Architectural Harm Objection

In *The Digital Person* and elsewhere,[161] Daniel Solove argues convincingly that the dominant metaphor for privacy harm has too long been the aforementioned Big Brother of George Orwell's *Nineteen Eighty-Four*.[162] This is the notion of a monolithic power engaged in massive surveillance. The metaphor has morphed in recent years to a concern over many "Little Brothers," that is, institutions and individuals with a problematically extensive power to observe.[163] But it remains inadequate.

Solove believes that the correct way to think about privacy in the contemporary world is not by reference to Orwell and *Nineteen Eighty-Four* but to Franz Kafka and *The Trial*. In *The Trial*, protagonist Josef K. is the subject of a mysterious legal

---

158. Paul Ohm refers more specifically to "the accretion problem." As he explains, "[o]nce an adversary has linked two anonymized databases together, he can add the newly linked data to his collection of outside information and use it help unlock other anonymized databases. Success breeds further success." Ohm, *supra* note 16, at 1746. Although true, the "success" the accretion problem worries about is only a privacy harm when some victim experiences an adverse effect.

159. I owe this example to Daniel Solove.

160. Samuel Bray, *Power Rules*, 110 COLUM. L. REV. 1172, 1173 (2010).

161. SOLOVE, THE DIGITAL PERSON, *supra* note 16; SOLOVE, UNDERSTANDING PRIVACY, *supra* note 4, at 133; Solove, *Privacy and Power*, supra note 16.

162. ORWELL, *supra* note 87.

163. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 4, at 133.

proceeding.[164] He lacks information with which to assess, let alone combat, his condition. Josef K. eventually succumbs to the state without ever understanding what has occurred.[165]

For Solove, this is the risk we face as a society. We know information about us is being collected, processed, and used—sometimes against our interest. But we have no choice about, or understanding of, the underlying processes. Privacy harm in the contemporary world is less a function of top-down surveillance by a known entity for a reasonably clear if controversial purpose. It is characterized instead by an absence of understanding, a vague discomfort punctuated by the occasional act of disruption, unfairness, or violence.

Another way to say this is that privacy harm is not merely individual, as this Essay has appeared to assume, but can lead to societal harms that are in a sense "architectural." The absence of privacy creates and reinforces unhealthy power imbalances[166] and interferes with citizen self-actualization.[167] These harms go to the very architecture or structure of our society.

There is no question that such architectural harms are important. They are not, however, best thought of as privacy harms. Rather, architectural harms are distinct harms—harms to societal cohesion and trust—that happen to be *composed* of privacy harms, and often not exclusively.

Consider Julie Cohen's concern, for instance, that "pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream."[168] This effect is a consequence of the perception of observation, that is, of a subjective privacy harm. Were a critical mass of society to experience this harm, we could imagine an "architectural" threat to civic, artistic, and technological innovation.[169] *But this does not mean that the loss of these values per se is a privacy harm.* Lack of privacy could be a contributor—along with a failed intellectual property regime or inadequate public schools—for instance, to a serious but distinct problem.

Or imagine the effects of an overzealous and unethical police force on the neighborhood it patrols. Its hypothetical officers monitor people without cause, issue undeserved citations, and engage in acts of police brutality. Each of these acts is distinct and generates a specific and different harm, worthy of individual study. But collectively, these harms add up to another: the erosion of community trust. This harm results from individual acts of excessive surveillance, but also abuse of discretion and unwarranted force. And it is itself none of these things.

---

164. FRANZ KAFKA, THE TRIAL (1925).

165. *Id.* at 227–29. This reading is, of course, open to interpretation.

166. *See* Solove, *Privacy and Power*, *supra* note 16.

167. *See* Schwartz, *supra* note 11.

168. Cohen, *Examined Lives*, *supra* note 83, at 1426.

169. Sadly, a recent study shows that Americans may in fact be less and less creative. *See* Po Bronson & Ashley Merryman, *The Creativity Crisis*, NEWSWEEK, July 10, 2010, at 44 ("Kim found creativity scores had been steadily rising, just like IQ scores, until 1990. Since then, creativity scores have consistently inched downward.").

C. Privacy Harms Without Privacy Violations

There is a tendency among courts, regulators, and privacy scholars to focus on the collection, processing, and dissemination of information.[170] Under this approach, a new technology—whether a snap camera in 1890[171] or a genetic algorithm in 2009[172]—endangers privacy insofar as it facilitates the watching of individuals.[173] This tendency is further reflected, as discussed above, in the accounts of Parker and others who view privacy harm basically in terms of unwanted sensing by a human being.[174] Privacy harms in the main features an observer and an unwary or unwilling victim.

On my account, however, there could be privacy harms without observers. I mean this in the weak sense that no human being needs to be doing the observing or decision making—the former could be merely perceived and the latter autonomous. But I also mean in it the strong sense that no human need *ever* be involved, even at the stage of design or implementation, for a privacy harm to occur. A subjective privacy harm could occur under my view because of mental illness or coincidence.

Surely it would not make sense to talk of a hallucination as a privacy violation, the objection runs. I'm not troubled by this consequence of my theory. The concept of harm is not linked to the concept of violation anywhere else; why should privacy be any different? A person can start a fight out of malice and get his nose broken in self-defense by the person he attacks. The broken nose still amounts to a harm. Or a tree branch could fall on a person because of high winds. Again, there is clearly a harm. Observational harm is no different. Paranoia, hallucination, guilt associated with the belief that God is watching—all of these harm the values that privacy protects. Privacy harm does not disappear by virtue of being natural or autogenic.[175]

D. Privacy Violations Without Privacy Harms

Peeping Tom has a long, and in ways severe, history.[176] Tom was the unfortunate boy who stole a look at Lady Godiva as she rode naked through the streets as a condition that her husband, the king, would cease to impose

---

170. Calo, *supra* note 90, at 817–25 (evidencing this tendency).

171. Warren & Brandeis, *supra* note 1, at 195 (opening with a concern over "[r]ecent inventions" such as "instantaneous photography").

172. Tal Z. Zarsky, *"Mine Your Own Business!": Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion*, 5 YALE J.L. & TECH. 1, 4–6 (2002–2003) (opening with a concern of new "complex algorithms" and "artificial intelligence" capable of drawing inferences).

173. Calo, *supra* note 90, at 824.

174. *See supra* notes 130–39 and accompanying text.

175. Such harms may not be actionable as a matter of law. But does that mean we should not attempt to understand them? We attempt to understand earthquakes without the ability to sue tectonic plates.

176. *See* SOLOVE, UNDERSTANDING PRIVACY, *supra* note 4, at 107 (telling the original story).

backbreaking taxes on the town. Tom was blinded for his insolence.[177] The image of Peeping Tom has evolved today into something more lurid—a man looking into a women's restroom, for instance—and is commonly invoked to highlight privacy harm. Sometimes the reference is merely implicit, as when Justice Scalia imagines the officers in *Kyllo v. United States* spying on the unsuspecting "lady of the house."[178]

Were Tom alive today, he would keep his eyes. We would say that Lady Godiva had no reasonable expectation of privacy and could not prove damages.[179] But Tom obviously stands in for a particular case. As Peter Swire points out, today's "peeping" commonly involves improper access of a database.[180] Swire develops a taxonomy of "peeping" into records, subdividing the act into three levels of severity.[181] There is the "gaze," where the perpetrator looks at another without permission, causing embarrassment. There is the slightly more problematic "gossip," where information that has been collected is shared with others. And there is the "grab," where information is retrieved and used against its subject—for instance, to blackmail.[182]

To map my own framework onto Swire's categories, I would say that the gaze involves a subjective or first category privacy harm whereas gossip and grab implicate second category harms. But what of the instance—surely very common—wherein an employee looks at a record, forms no judgment, and no one ever knows? Relatedly, what of the Peeping Tom who observes the infamous lady in her sauna but neither she nor Justice Scalia ever finds out?

On one view, the hidden or undiscovered observer represents the *quintessential* privacy harm because of the unfairness of his actions and the asymmetry between his and his victim's perspective. We certainly bristle at the thought of someone watching us unseen in the shower. Yet my theory would not capture this activity as a privacy harm unless and until the observed found out about it. Without that, there is no perception of unwanted observation, nor is there use of information adverse to the individual being observed. As Richard Parker puts it: "If privacy is defined as a psychological state," as I have defined it here, "it becomes impossible to describe a person who has had his privacy temporarily invaded without his knowledge."[183]

I do not see this disconnect as necessarily fatal to my account. Note that there are multiple parties involved in any Peeping Tom hypothetical, each with their own perspective. The participants are the perpetrator, the victim, and the audience for the hypothetical's narrative. Only two of these three parties to the violation know about it.

---

177. *Id.* Tom may have gotten off easy; Lot's wife Sarah was turned to stone for looking back on Sodom. *Genesis* 19:26 (King James) ("But Lot's wife did not obey God. She turned and looked at Sodom burning, sorrowfully. She turned into a pillar of salt.").

178. 533 U.S. 27, 39 (2001) ("The Agema Thermovision 210 might disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath . . . .").

179. *See supra* note 60.

180. Peter P. Swire, *Peeping*, 24 BERKELEY TECH. L.J. 1167, 1168 (2009).

181. *Id.* at 1173.

182. *Id.*

183. Parker, *supra* note 1, at 278.

I believe our tendency to see a privacy harm in the example of the hidden Peeping Tom in fact rests on a conflation between the internal and external perspectives.[184] The victim within the hypothetical is not aware of the observation and hence suffers no harm. We who are external to the hypothetical do, however, and experience a natural empathy with the observed as we project our superior knowledge upon them.

Consider the following thought experiment: an inventor creates a telescope so powerful that she can watch life forms on a distant planet. Or she creates a means by which to look at another dimension.[185] In either case, she can watch any aspect of private life but she can never have any impact on the observed (quantum mechanics notwithstanding). My intuition on these "facts" is not to be concerned, even though the activity is functionally equivalent to the standard undetected peeping. Nothing more is seen by the inventor than by the peeper, and we have stipulated that no real world adverse action is taken against the observed in either case.

There is clearly a threat that the observation will be discovered or its fruits will be abused.[186] There is also a sense in which we as third parties might be harmed by the mere knowledge that such a thing as an interdimensional telescope is possible. We might be a little less certain of being alone in such a world. The same is true of the Peeping Tom: we fast forward mentally to the moment at which the deed is discovered and the subject is retroactively embarrassed, frightened, and shamed. Outside of a hypothetical, of course, the only time Peeping Toms come to light is after they are caught.[187]

CONCLUSION

Just as a burn is a specific and diagnosable condition, so is privacy harm a distinct injury with particular boundaries and properties. This Essay has argued that by delimiting privacy harm, we gain the ability both to rule out privacy harm where appropriate and to identify novel privacy harms as they emerge. By looking at privacy harm in the way this Essay suggests, we gain practical insight into the nature and range of this unique injury. Of course, the subjective and objective components of privacy harm are each amenable to further analysis. Privacy is in

---

184. *Cf.* Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357, 357 (2003) ("The Internet's ability to generate a virtual reality creates what I will call the problem of perspective in Internet law. The problem is that whenever we apply law to the Internet, we must first decide whether to apply the law to the facts as seen from the viewpoint of physical reality or virtual reality. In this Essay, I will refer to the viewpoint of virtual reality as the 'internal perspective' of the Internet, and the viewpoint of physical reality as the 'external perspective.'").

185. One need not resort to science fiction for an illustration of this concept. Consider the example of accurate memory of a previous intimate event.

186. *See supra* Part III.A (discussing risks of privacy harm).

187. We might say that Tom himself suffers a "moral harm" in that he is morally impoverished by engaging in conduct he knows to be wrong if discovered. *But see* 1 FEINBERG, *supra* note 116, at 65–70 (denying the coherence of moral harm).

many ways on the cusp of a greater science.[188] The hope is that by describing the outer boundaries and core properties of privacy harm in detail, this Essay has served to open an additional avenue of investigation.

188. *See, e.g.*, Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005) (looking to social network theory to provide guidance to courts on the question of whether an individual has a reasonable expectation of privacy in a particular fact that he has shared); Katherine J. Strandburg, *Privacy, Rationality, and Temptation: A Theory of Willpower Norms*, 57 RUTGERS L. REV. 1235 (2005) (leveraging behavioral economics and psychology to explain why and when people disclose personal information).