THE BOUNDARIES OF PRIVACY HARM

M. Ryan Calo[*]

ABSTRACT

This Essay describes the outer boundaries and core properties of privacy harm, an important, unique, but chronically under-theorized injury. I argue that the vast majority of privacy harms fall into just two categories. The subjective category of privacy harm is the unwanted perception of observation. This category describes unwelcome mental states—anxiety, embarrassment, fear—that stem from the belief that one is being watched or monitored. Examples include everything from a landlord listening in on his tenants to generalized 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 anticipation of battery, so is the unwanted perception of observation largely an apprehension about information-driven consequences. The categories represent, respectively, the realization and consequence of a loss of control over personal information.

The approach usefully uncouples privacy harm from privacy violations, demonstrating that each can occur without the other. It creates a "limiting principle" capable of revealing when another value—autonomy or equality, for instance—is more directly at stake, and a "rule of recognition" that permits the identification of a privacy harm when no other harm is apparent. Finally, the approach permits the sizing of privacy harm in novel ways, pointing the way toward a better science of privacy harm.

---

[*] Senior Research Fellow, Stanford Center for Internet and Society, Lecturer in Law, 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 Privacy Law Scholars Conference 2010. Thanks also to Stefania Fusco, Samuel Bray, and Elizabeth Pollman for commenting on earlier drafts. Thanks to Katherine Merriam for research assistance.

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 on 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] Thought leaders 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.*, Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1980) (defining privacy as "the right to be left alone"); ALAN WESTIN, PRIVACY & FREEDOM (1967); Charles Fried, *Privacy*, 77 YALE L.J. 475 (1968); Richard Parker, *A Definition of Privacy*, 27 RUTGERS L. REV. 275 (1974) (defining privacy "control over who can sense us"). *But see* Daniel Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 482 (2007) (understanding privacy in terms of "specific activities that cause privacy problems") [hereinafter "*A Taxonomy of Privacy*"]; Joel Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877 (2003); Paul Ohm, *The Benefits of the Old Privacy: Restoring the Focus to Traditional Harm*, Privacy Law Scholars Conference, June 4, 2010 (work in progress). This Essay addresses Daniel Solove's inventive approach in Part I.A.

[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 626 (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 (Cir. 6th 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 Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1232 (noting that "privacy 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 Posner, *Privacy, Surveillance, and the Law*, 75 U. CHI. L. REV. 245, 251 (2008) ("Privacy is the terrorist's best friend."); Richard Posner, *The Right to Privacy*, 12 GEORGIA L. REV. 393, 398 (1978) ("At some point nondisclosure becomes fraud."). *See also* Stewart Baker, SKATING ON STILTS: WHY WE AREN'T STOPPING TOMORROW'S TERRORISM (2010) AMATAI ETZIONI, THE LIMITS OF PRIVACY (1999).

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 kind 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 and permits the sizing and redress of privacy harms in novels 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 unwanted perception of observation. This category describes unwelcome mental states—anxiety, for instance, or embarrassment—that accompany the belief that one is or will be watch or monitored. Examples include the harm experienced by the tenants in *Hamburger v. Eastman*,[6] to the unease caused by a massive data breach, to 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 uncover 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

---

[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 Allen, *Genetic Privacy: Emerging Concepts and Values*, *in* GENETIC SECRETS: PROTECTING PRIVACY AND CONFIDENTIALITY IN THE GENETIC ERA 31, 34 (1997) (describing four dimensions of privacy); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1202-04 (1998) (describing three dimensions to privacy). Nor does it attempt to create a list of the values that privacy protects. *See, e.g.*, WESTIN, *supra* note 1; DANIEL SOLOVE, UNDERSTANDING PRIVACY (2008) [hereinafter "UNDERSTANDING PRIVACY"]. Rather, it argues that privacy harm is unique in that it is a harm tied broadly to observation. *See infra* Part II (describing the relationship in detail).

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

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

[7] United States v. U.S. District Court, 407 U.S. 297 (1972).

[8] Laird v. Tatum, 408 U.S. 1 (1972).

[9] Wilson v. Libby, 498 F.Supp.2d 74 (2007) (dismissing for "special factors").

was drawn and introduced as evidence again 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 unwanted perception of 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 confrontation of other, more 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

---

[10] Schmerber v. California, 384 U. S. 757 (1966).

[11] According to Paul Schwartz, "the leading paradigm on the Internet and in the real, offline world conceives of privacy as personal right to control the use of one's data." Paul Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 820 (2000). *See, e.g.*, WESTIN, *supra* note 1 (conceiving of privacy as the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"); FRIED, *supra* note 1 (conceiving of privacy as "control over information about ourselves"); Parker, *supra* note 1 (defining privacy "control over who can sense us"); Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 236 (1977) (defining privacy as "control over the intimacies of personal identity"). *See also National Cable & Telecommunications Ass'n v. FCC*, 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.").

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

[13] *See infra* notes __ - __ and accompanying text. It plays out in other contexts as well. In *E.I. du Pont 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 it competitor constituted an invasion of "commercial privacy." Arguably the act was better described as an act of unfair competition.

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 sizing 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 observation. Thus, in *De May v. Roberts*, where a doctor's friend watched a woman give birth on the false assumption that the friend was a fellow medical professional, the degree of observation was limited but highly unwanted.[15] In contrast, observation in public is implicitly accepted, but public camera surveillance could still rise to the level of harm on 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 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.

---

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

[15] 46 Mich. 160 (1881).

[16] Daniel Solove is a prominent proponent of this view. *See, e.g., A Taxonomy of Privacy* at 487-88 (discussing risk of harm and power imbalance). *See also* Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, *supra* note 5 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 Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001); DANIEL SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 97-101 (2004). *See also* Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Review __ (forthcoming 2010) (describing the accretion problem: "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").

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 such boundary hunting worthwhile? What do we gain from distinguishing privacy harm from other harm or from the underlying concept of privacy? Section A argues that delimiting privacy harm helps address and protect privacy and other values. Section 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. A working definition of privacy harm gives us a "limiting principle" that guards against dilution and reveals other important harms. It also means having a "rule of recognition" that permits the identification of emerging privacy harms.

1. A limiting principle.

Misdiagnosing a problem makes it hard to fix. Imagine what would happen if a doctor confused heart burn 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 pain killer—but the treatment would not ultimately be effective.

Courts can also misdiagnose harm, leading to a topical salve in place of a permanent 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,

[17] *See generally A Taxonomy of Privacy*.

[18] *See* UNDERSTANDING PRIVACY 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 (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)

a court may not be inclined to revisit the diagnosis.

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

In *Lawrence v. Texas*, the Supreme Court invalidated a Texas statute criminalizing certain sexual acts between two people of the same gender.[23] Justice Kennedy's opinion began by acknowledging that "the instant case involves liberty of the person both in its special and its more transcendental 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 it is not. Yet a harm has still occurred. The restrictions at issue in *Roe* and *Lawrence* fell upon one group (women, gays) and hence could be said to implicate equality.[26] They certainly interfere with the proverbial "pursuit of

---

("[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] On another view, the equality is the value at stake in the abortion cases. *See* MARK GRABER, RETHINKING ABORTION: EQUAL CHOICE, THE CONSTITUTION, AND REPRODUCTIVE POLITICS.

[21] *Id.* at 485-86.

[22] Roe v. Wade, 410 U.S. 113, 153 (1973).

[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 Kaytal, *The Dissident Citizen*, 57 UCLA L. REV. 1415 (2010).

[26] *See id.*; Graber, *supra* note 20.

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]—is not a deep means to address these issues. It may be helpful in the short run, i.e., before society is prepared to recognize the real issues at stake. In the long run, however, it operates to obscure and perhaps demean these important harms.[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 catch all. Thus, a second advantage to having a limiting principle is that it helps protect against dilution of the concept.[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.

---

[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 preamble (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 is not like possessing obscenity. It should also be noted that privacy has operated at times to protect abhorant conduct such as domestic violence. *See* Reva Seigel, *"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. Many believe that privacy does not invoke the highest standards of scrutiny reserved for abrogation of equality or other values mentioned specifically in the Constitution and at the core of what it means to be a liberal democracy. *See supra* note 3 (listing examples). By delimiting privacy harm, we can rule out this layer and reveal the true value that is making our citizens and jurists rightly uncomfortable.

[30] *Cf. Griswald*, 381 U.S. at 509 (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 more or less flexible and more or less restricted in meaning.").

[31] This is also the reason that we protect commercial speech less than non-commercial 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).

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," i.e., 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 at offers to purchase critically. Setting aside actual fraud, there is extensive evidence that marketers assemble and trade lists of particularly vulnerable populations.[33] These lists are often compiled on the basis of sensitive and 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 outside world—all desirable outcomes. They are going to see 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 back 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 unsolicited spam emails as privacy harms, for instance, and federal law regulates it in part on this basis.[36] But the analogy is strained:

---

[32] *See, e.g.,* Danielle Keats Citron, *Law's Expressive Value In Combating Cyber Gender Harassment*, 108 Mich. L. Rev. 373, 393 (2009) (discussing the history of the emotional distress tort and the reticence of the courts to allow recovery).

[33] *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 and Commerce Collection of Consumer Information, *8 (Nov. 19, 2009).

[34] *See id.*

[35] *See id.*

[36] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. §§ 7701-7713 (2003); S. REP. 108-102 (referring to the impact of spam on privacy).

on what theory is getting unwanted commercial email any more a violation of privacy than getting your home mailbox stuffed with toilet paper as a prank? Moreover, the content of unsolicited email is entitled to some First Amendment protection making it harder to regulate.[37]

Seeing the privacy harm in unsolicited spam requires looking closely at the mechanism through a particular lens. As several scholars have pointed out, spam is often targeted on the basis of purchased or misappropriated private information.[38] Spam requires an email 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

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 quixotic search for a

---

[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* 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."); 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 junk mail to me may have involved access to and analysis of personal information…").

[39] *See, e.g.*, California Online Privacy Protection Act, CA. BUS. & PROF. CODE § 22577(a)(3) (2004) (defining email as personally identifiable information). Of course, much spam reaches inboxes through randomly generated email addresses—automated guesswork supported by variously private input.

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

[41] *See* Daniel Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002); *A Taxonomy of Privacy*; UNDERSTANDING PRIVACY. Solove's pragmatic and inclusive approach to privacy is widely cited, including by federal courts. *See, e.g.*, National Cable & Telecommunications Ass'n v. FCC, 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*. Solove uses one theory of privacy against another, i.e., he "survey[s] the criticisms of various schools regarding each other's conceptions of privacy and suggest[s] a number of [his] own." UNDERSTANDING PRIVACY

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 also disavows the utility of isolating privacy harms from other sorts of harms. In response to the anticipated argument that one subcategory of his taxonomy, that of "distortion," "really is not a privacy harm," Solove counters: "But does that matter? Regardless of whether distortion is classified as a privacy problem,

---

at 8. Generally speaking, Solove's 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] *Id.* at 46.

[44] *Id.* at 45.

[45] *Id.* at 42-43. *See also* Solove, *Conceptualizing Privacy* at 1096-99 (discussing Wittgenstein's theory of family resemblances).

[46] UNDERSTANDING PRIVACY at 42; *id.* at 9.

[47] *Id.* at 42.

[48] *Id.* at 43.

[49] *Id.* at 42.

it is nevertheless a problem."[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, i.e., "a framework for understanding privacy in a pluralistic and 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, 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]

---

[50] Daniel Solove, "*I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 San Diego L. Rev. 745, 760 (2007). 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.*

[51] UNDERSTANDING PRIVACY at 10.

[52] *Id.* at 105 ("My taxonomy's categories are not based on 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.*, Kang, *supra* note 4 (describing three dimensions to privacy); Anita Allen, *Genetic Privacy: Emerging Concepts and Values*, *in* GENETIC SECRETS PROTECTING PRIVACY AND CONFIDENTIALITY IN THE GENETIC ERA 31, 34 (describing four dimensions to privacy); JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY 75 (2007) (describing three privacy "clusters). *See also* Solove, *Conceptualizing Privacy* 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 clustered conception.").

[53] UNDERSTANDING PRIVACY at 101-02.

[54] *Id.* at 172.

[55] *Id.* at 102.

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 in the previous section that it would be useful to deny that limits on abortion, contraception, and sodomy concern privacy because doing so could reveal the real values, 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 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 of analysis and disagreement.

Conversely, we might want to deny that two phenomenon that resemble one another in certain ways are in fact the same. Skin burns and heart burn 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 resemblance one another in *the right ways*, i.e., 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 adds a great deal to the discussion. 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 give up the ability to deny that certain harms have anything to do with privacy or to argue that wholly novel privacy harms should be

---

[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, 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, *15 (2010).

[57] UNDERSTANDING PRIVACY at 42.

[58] We might say they all resemble one another in being a family. This would of course be circular.

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 where 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 unwanted perception of observation. Subjective privacy harms can be acute or ongoing, 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.

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,[61] or a neighbor forms a negative judgment from gossip. They can also occur when such information is used to commit a crime, such as identity theft. 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 information itself for it to be used against the victim.

---

[59] Samuel Warren and Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

[60] *See id.* at __ ("The right to privacy ceases upon the publication of the facts by the individual, or with his consent."); 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."); UNDERSTANDING PRIVACY at 102 ("When a person consents to these activities, there is no privacy violation.").

[61] *See infra* notes 117 to 126 and accompanying text.

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 linked, however: 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 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.

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

A. Subjective Privacy Harms

The subjective category of privacy harm is the unwanted perception of 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

---

[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 with 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] *Id.* at § 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] *Id.* at §13 cmt. a.

[66] By "sensory access," I just mean access to information in the form of sensory data. When a person loses sensory access, for purposes of this Essay, they lose the ability to keep someone from observing them 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, or voices, and the products of our bodies.").

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 Ruth Gavison's "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 back-scatter 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, *Reeves v. Equifax Information*

---

[67] Ruth Gavison, *Privacy and the Limits of the 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. 2 (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 Clarke, *Information Technology and Dataveillance*, *in* COMPUTERIZATION AND CONTROVERSY 496 (C. Dunlop and R. 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* UNDERSTANDING PRIVACY at 4.

[71] The federal government and several states have enacted so-called "up skirt laws" in recognition that privacy harm can occur even in public. *See, e.g.*, Video Voyeurism Prevention Act of 2004, 118 U.S.C.A. § 1801 (2000); H.R. Rep. No. 08-504, at 3-5 (2004) (referencing state laws and discussing legislative intent).

[72] For a discussion of back-scatter devices, see Jeffrey Rosen, *Nude Awakening*, THE NEW REPUBLIC (Feb. 10, 2010). *See also* Def.'s Emergency Mot. for Stay, Electronic Information Privacy Center *et al* v. Department of Homeland Security, No. 10-1157, at *3-7 (D.C. Cir. Jul. 13, 2010) (describing privacy issues with back-scatter devices in detail).

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

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 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 just the doctor's untrained acquaintance. Although she made no objection to the man's presence when she believe 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 (or even because) of discovery.[77]

An different privacy harm occurs where observation is systematic, i.e., part of a plan or pattern. Pervasive individual monitoring is, for instance, a key component in abusive control.[78] Repeated "checking in" throughout the day is thought to be an early sign of domestic abuse and there is evidence that the "learned helpless" experienced by some abuse victims stems in part from having internalized the feeling of being monitored.[79]

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 *United States v. United States*

---

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

[74] No. 09-CV-00043, 2010 BL 113325 (S.D. Miss. May 20, 2010).

[75] 46 Mich. 160, 161 (1881).

[76] *Id.* at 166.

[77] *See, e.g.*, Hamberger v. Eastman, 206 A.2d 239 (1965). *But see* [insert Disney case] (holding that the plaintiffs were not entitled to recovery from a photographer that followed them around a theme park because they were not aware of his presence at the time).

[78] One category of the "Power and Control Wheel" developed by the Domestic Abuse Intervention Project to detect abuse, is "isolation." *See* Domestic Abuse Intervention Project, *online at* http://www.duluth-model.org (last visited July 14, 2010). Isolation is sustained by, inter alia, tracking or monitoring activities and/or whereabouts." *Id.*

[79] *See* Melinda Smith and Dr. Jeanne Segal, *Signs of Abuse and Domestic Violence*, *online at* HelpGuide.org (last visited July 14, 2010). 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).

District Court.[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 of harm to support the plaintiffs' claim of excessive government surveillance, it note its recognition of "constitutional violations" arising from the "deterrent or 'chilling' effect of governmental regulations that falls short of direct prohibition."[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 stimulus of daily life. … To be 'always on' would destroy the human organism."[84] Charles Fried notes that, were our every action public, we might limit what we think and say.[85]

Indeed, the lack of any time away from others is a common feature of the modern dystopian novel. George Orwell's camera-televisions from *1984* continue to haunt the contemporary imagination.[86] In Yevgeny

---

[80] 407 U.S. 297, 314 (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.

[81] *Id.* *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 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* UNDERSTANDING PRIVACY at 163-64 (cataloguing the role of solitude in daily life). *See also* Lior Strahilevitz, *Reputation Nation: Law in an Era of Ubiquitous Personal Information*, 102 N.W. 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 better citizens."); Julie Cohen, *Cyberspace as/and Space*, 107 COLUM. L. REV. 210 (2007); Paul Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815 (2000); Julie Cohen, *Examined Lives: Information Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000); Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1640-41 (1999); BARRINGTON MOORE, PRIVACY: STUDIES IN SOCIAL AND CULTURAL HISTORY 73 (1984).

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

[85] 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 in we could be sure of keeping them to ourselves.").

[86] GEORGE ORWELL, 1984 (1949).

Zamyaten's *We*, the buildings are transparent.[87] The most frequently repeated act of mental conditioning in Aldus Huxley's *Brave New World* is the dislike of solitude.[88]

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.[89] This is the exact lesson of the infamous Panopticon. The tower is always visible, but the guard's gaze is never verifiable.[90] As Michel Foucault explores, prisoners behave not because they are actually being observed, but because they believe they might be.[91] The Panopticon works precisely because people can be mistaken about whether someone is watching them and nonetheless suffer similar or identical effects.[92]

A related point can be made regarding dummy cameras[93] and, as it turns out, mere representations of people. Even where we know intellectually that we're interacting with an image or a machine, our brains are hardwired to respond as though a person were actually there.[94] This reaction includes the feeling of being observed or evaluated.[95] People pay more for coffee on the honor system, for instance, if eyes are depicted over the collection

---

[87] YEVGENY ZAMYATIN, WE 28 (1927) (citizen D-503 praises the "splendid, transparent, eternal glass" that composes nearly every structure).

[88] ALDUS HUXLEY, BRAVE NEW WORLD 75 (1932).

[89] 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).

[90] MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 200 (1979).

[91] *Id*. at 200-01.

[92] *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 Miller, *Privacy: Is There Any Left?*, 3 FED. CT. L. REV. 87, 100 (2009) ("It 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.").

[93] 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 *et al.*, *The Eye of the Camera: Effects of Security Cameras on Prosocial Behavior*, 41 ENV'T & BEHAV. 1, 60-74 (2009).

[94] Calo, *supra* note 89 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.'").

[95] *Id.* at 838-42 (collecting studies).

box.[96] Our attitude, behavior, even our physiology can and do in circumstances where no real person is there.[97]

B. Objective Privacy Harms

Subjective privacy harms are all the harms individuals experience from observation. 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 arousal" that can be harmful if excessive and unwanted.[98] The embarrassment of being seen naked seems similarly ingrained, at least throughout Western society.[99]

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 identify theft.[100] Or the consequence could be the formation of a negative judgment about a person at issue in the tort of public disclosure of private fact.[101]

Objective privacy harms are those harms that are external to victim and involve the forced or unanticipated use of personal information. By "personal," I do not mean "personally identifiable" in the statutory sense.[102]

---

[96] *Id.* at 812.

[97] *Id.* at 813.

[98] Psychological arousal refers to the absence of relaxation and assurance which corresponds to the presence of others. *See* Rompay, *supra* note 93 at 62; Lee Sproull *et al*., *When the Interface is a Face*, 11 HUM.-COMPUTER INTERACTION 97, 112 (1996).

[99] UNDERSTANDING PRIVACY at 53, 147.

[100] In re TJX Companies Retail Sec. Breach Litigation, 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.").

[101] *See* William Prosser, *Privacy*, 48 CAL. L. REV. 383, 398 (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.

[102] Many statutory obligations only apply to "personally identifiable information," i.e., information such as name or social security number that can be used to identify a specific information. *See, e.g.*, California Online Privacy Protection Act, BUS & PROF. CODE §§

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—are 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 where he understood and agreed to the use.[103] Thus, it is not necessarily a privacy harm to trade an email address for a chance to win a sweepstakes where both parties understand that the email will be used for marketing purposes.[104] Nor is it a privacy harm for one person to decide not to speak to another at a party because he is not attractive. We expect and tacitly consent to these sorts of discriminations.

The problem enters where, 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 dramatically 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.[105] 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 emails.[106] 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.[107]

22575-22579 (2004) (privacy policy requirement for websites on pages where they collect personally identifiable information); CAL. CIV. CODE §§ 1785.11.2, 1798.29, 1798.82 (2009) (breach notification requirement in the event of compromised personally identifiable information); CONN. GEN. STAT. ANN. § 36a-701b (2009) (same); GA. CODE ANN. § 10-1-910, 911 (2009) (same).

[103] *See supra* note 60 (citing sources).

[104] Of course, it may run afoul of state anti-lottery statutes if furnishing an email constitutes "consideration." *See, e.g.*, CAL PEN. CODE § 319 ("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 …").

[105] *See* Fred Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PERCEPTION IN THE AGE OF INFORMATION 361 (2006); 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.").

[106] *Id.*

[107] A 2009 study showed that 45 percent of employers surveyed used social networks

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.[108]

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.[109] Although this system is increasingly seen as flawed,[110] 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 right not to self-incriminate guaranteed under the Fifth Amendment, though in practice this right is limited to statements.[111]

---

to vet potential hires. *See* Jenna Wortham, *More Employers Use Social Networks to Check Out Applicants*, N.Y. TIMES (Aug. 20, 2009). A more recent study commissioned by Microsoft found that 70 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* (Jan. 2010).

[108] *See* California Online Privacy Protection Act, BUS & PROF. CODE §§ 22575-22579 (2004).

[109] The four fair information practice principles are notice/awareness, choice/consent, access/participation, integrity/security and enforcement/redress. *See* Federal Trade Commission, *Fair Information Practice Principles*, *online at* http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited July 14, 2010). Most of the Commissions enforcement has focused on notice and security. *See* Cate, *supra* note 105. 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).

[110] *See, e.g.*, Cate, *supra* note 105 ("The FTC's approach … reduces notice and consent to a mere formality—a checkbox that consumers must select to obtain a desired product or service."); Schwartz, *supra* note 83 at 1661-64; Cohen, *Examined Lives*, *supra* note 83 at 1397-98.

[111] Thus, a suspect or defendant could be compelled to show his person in a line up or make a voice or handwriting sample. *See* United States v. Wade, 388 US 218 (1967) (line up); United States v. Dionisio, 410 U.S. 1 (1973) (voice); Gilbert v. California, 388 U.S.

The coercion at issue in *Schmerber v. California*, where a drunk driving suspect's blood was drawn and introduced as evidence again him,[112] was relatively straightforward. But coercion exists on a spectrum.[113] 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 be little to no alternative to surveillance in daily life. As Richard Posner observes, "[i]f an entire city is known to be under camera surveillance … submission to it is as a practical matter involuntary."[114]

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 word.[115] Doctors look at our bodies not to harm us but to protect our health. This is not always an easy question. Federal Trade Commission staff observe that targeted online ads benefit consumers,[116] for instance, whereas a recent study suggests that a majority of consumers find targeting worrisome.[117] But the question of whether an action is adverse is familiar. Courts and regulators confront the question of what is adverse in many statutes and standards without paralysis.[118]

Finally, as with subjective privacy harms, human beings do not necessarily need physically to 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.

---

263 (1967) (handwriting).

[112] 384 U.S. 757 (1966).

[113] At issue in *Nielson 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.

[114] Posner, *Privacy, Surveillance, and the Law*, *supra* note 3 at 247.

[115] For a detailed discussion of the concept of harm in the legal context, see Joel Feinberg, THE MORAL LIMITS OF CRIMINAL LAW (Vol. 1-4) (1987).

[116] *See* Federal Trade Commission, *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles*, *2 (Dec. 20, 2007) ("[B]ehavioral advertising provides benefits to consumers in the form of free web content and personalized ads that many consumers value."), *available online at* http://www.ftc.gov/opa/2007/12/principles.shtm (last visited July 14, 2010).

[117] Joseph Turow *et al*., *American Reject Tailored Advertising and Three Activities that Enable It*, Working Paper Series, Social Science Research Network (Sep. 29, 2009), *available online at* http://ssrn.com/abstract=1478214 (last visited July 14, 2010).

[118]

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 business are deemed ineligible for federal contracts.[119]

Citron explores the harm of automated decision making from the perspective of due process.[120] But such automated decisions can also constitute privacy harms where, as often, they involve the unanticipated or coerced use of sensitive personal information.[121]

Consider an example raise by Richard Posner and others to demonstrate that no privacy harm occurs unless and until a human sees the information at issue.[122] Google email service Gmail automatically scans users' emails and displays advertising on the basis of keywords it picks out.[123] Google assures users that no human ever sees the email, and we have no reason to disbelieve the claim.[124] Gmail users and the people that write to them are consequently unlikely to be judged, embarrassed, or otherwise harmed by Google employees on the basis of email content.

But imagine that a user of another email client is trying to sell something, say, a bicycle, to a Gmail user. Google automatically scans the sender's incoming email 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 email and use it, without

---

[119] Danielle Citron, *Technological Due Process*, at 1252.

[120] *Id.*

[121] I've 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.

[122] *See, e.g.*, Posner, *Privacy, Surveillance, and Law*, at 249 (discussing Gmail's automated ad delivery feature); Tokson, at *38-39 (discussing users of Gmail and Yahoo! Mail).

[123] Tokson at 39.

[124] *Id.*

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.[125]

Automated collection, processing, and decision making is not going anywhere.[126] 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.[127] Citron identifies a series of instances—airline travelers mislabeled by the data-matching programs that underpin the "No Fly" list; parents mislabeled as dead beats by an automated system—where machines use information in surprising ways.[128] 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.

C. The Advantages of Seeing Privacy Harm in This Way

I've 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 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.

---

[125] This hypothetical is a riff on Lawrence Lessig's example of a government worm that searches for contraband information.

[126] If anything, it will likely continue to grow. Citron, at 1251-52 (explaining the administrative forces that give rise to autonomous decision making).

[127] *Id.* at 1263-67.

[128] *Id.*

Importantly, the approach demonstrates the inadequacy of a widely held view about the nature of privacy harm—namely, that it can only occur when one human senses another. For Richard Posner and others, privacy harm only occurs when a person gets a hold of and misuses information that he should not. No harm occurs from the mere collection or even processing of information by, for instance, a computer.[129] The information must wind up in the hands (or eyes) of a "sentient being."[130] Even then, a robust "professionalism"—whether by a doctor or intelligence officer—can serve to mitigate the privacy harm.[131] And while observation alone registers on the scale,[132] real privacy harm seems to occur for Posner only where the observer takes an action they should not with physical on monetary consequences.

Posner is no 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."[133] Processing alone, if never "displayed to a human," leads to "no adverse consequence of any sort."[134] Orin Kerr's proposed test for a Fourth Amendment search is also "exposure-based" and denies, if not any harm, than any constitutional implication where information is merely processed by a computer.[135] Richard Parker defines privacy specifically and at length as "control over who can sense us,"[136] implying that a privacy harm only occurs when someone senses us when we do not want them to. Parker goes on to say that "the collection of data by government or other institutions … is not a loss of privacy per se per rather a threat to one's privacy."[137]

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 non-humans do not necessarily implicate the Fourth

---

[129] *Id.* at 253-43.

[130] Posner, *Our Domestic Intelligence Crisis*, at A31.

[131] Posner, *Privacy, Surveillance, and Law*, at 251 (analogizing intelligence officers looking at citizen's information to doctors looking at patient's bodies).

[132] *Id.* at 245 ("A woman (an [sic] 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.").

[133] Goldman, at 225-26.

[134] *Id.* at 228.

[135] Kerr, at 551.

[136] Parker, at 281.

[137] *Id.* at 285.

Amendment. In *United States v. Place* and *Illinois v. Caballes*, 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.[138] The argument has even been deployed to argue for *greater* privacy protection under the Fourth Amendment.[139]

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.[140] 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.[141] If anything, we have embarked upon ever greater automation.[142] 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 easier to recognize and to test. Courts and regulators are capable of asking whether a person felt observed, whether she consented to observation or collection, and whether she anticipated a given use of her information.[143] 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.[144]

The approach also furnishes criteria for "sizing" privacy harm and ranking their relative severity. In the case of subjective privacy harms, we

---

[138] 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.").

[139] 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." According to Tokson, it is the rare situation where a human being would ever see the content of an email or other electronic communication. The vast majority of information disclosed to online third parties is "processed entirely by automated equipment."

[140]

[141]

[142]

[143] *But see* Schwartz, *supra* note 83 at 1661-64 (describing the view that users consent to many of the terms they encounter online as an "autonomy trap").

[144] *See infra* Part I.C.

can look to the degree of aversion to observation as distinct from the extent of observation. High degrees of both translate into the greatest harm, but harm is possible if either are very high.[145]

This might be particularly useful in describing the notoriously difficult problem of "privacy in public."[146] 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.[147] In the absence of a privacy violation, we tend not even to look for privacy harm.

Having described the mechanics of privacy harm, however, we can now say that the degree of aversion is small—2 out of 10, 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 and so the harm can be quite large—2 times 10.[148]

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 the increased risk of harm, as in the case of a security breach, and so-called "architectural harm."[149]

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."[150] I've argued that an account must be able to rule out certain harms even if authorities have applied the label "privacy" to them. But even granting that privacy harm has boundaries, my approach may appear counterintuitive both in that

---

[145] This provides a hook for the contested claim of "privacy in public."

[146]

[147]

[148] Similarly, in the case of objective privacy harms, we can look to the degree of knowledge or consent, as distinct from the extent of impact of the information use.

[149] Solove

[150] Parker, at 276.

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 since January 2005.[151] 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.[152]

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, they increase the *risk* of negative outcomes. Isn't this increased risk privacy harm in its own right, one might argue? If it is, why doesn't my approach recognize 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 appear on this analysis that breach notification is a net evil in that it creates privacy harm where there would be none.

Here I disagree with the 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.[153] A

---

[151] http://www.privacyrights.org/ar/ChronDataBreaches.htm#Total

[152] *See supra* note __ (listing four).

[153] Paul Ohm refers more specifically to "the accretion problem." As he explains, "once an adversary has linked to anonymized databases together, he can add the newly

feeling of greater vulnerability can constitute privacy harm, just as the apprehension of battery can constitute a distinction tort. But there is no assault or battery without the elements apprehension or unwanted contact.

Note that it does not disparage the severity 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. As Sam Bray points out, some rules are in place to deter specific harms; others exist to empower the vulnerable or hinder the powerful in an effort to make harm less likely.[154] 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,[155] Daniel Solove agues convincingly that the dominant metaphor for privacy harm has too long been the aforementioned Big Brother of George Orwell's *1984*.[156] 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," i.e., institutions and individuals with a problematically extensive power to observe.[157] 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 *1984* but to Franz Kafka and *The Trial*. In *The Trial*, protagonist Josef K. is the subject of a mysterious legal proceeding.[158] 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.[159]

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

---

linked data to his collection of outside information and use it help unlock another anonymized database. Success breeds further success." *39. Although true, the "success" is only a privacy harm when some victim experiences an adverse affect.

[154]

[155] Solove, Digital Persons; Solove, Privacy and Power.

[156] George Orwell, 1984 (1949).

[157] Solove, The Digital Person, at __.

[158] Franz Kafka, The Trial (1925).

[159] *Id.* at __.

processes.[160] 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 the occasional 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[161] and interferes with citizen self-actualization.[162] These harms go to the very architecture or structure of our society.

There is no question that such architectural harms are important and real.[163] 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 people who are under surveillance will "tend toward the mainstream."[164] This effect is a consequence of the perception of observation, i.e., 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.[165] 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 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

---

[160]

[161] Solove, …

[162] Paul Schwartz.

[163] Paul Ohm questions whether such harms are measurable. [cite] I believe they are. We could look at civic engagement following a privacy law, for instance, or attempt to line up innovation metrics with privacy law.

[164] This is an observation on Cohen's part, not the central thesis of her article.

[165] Sadly, a recent study shows that Americans are becoming less creative according to one metric.

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.

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.[166] Under this view, a new technology—whether a snap camera in 1890[167] or a genetic algorithm in 2009[168]—endangers privacy insofar as it facilitates the watching of individuals.[169] This tendency is further reflected, as discussed above, in the accounts of Parker and others that view privacy harm basically in terms of unwanted sensing by a human being.[170] 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 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 on 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 their nose broken in self-defense by the person they attack. 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 these harm the values that privacy protects. Privacy harm does not disappear by virtue of being natural or autogenic.

D. Privacy Violations without Privacy Harms

---

[166] Calo, at __.
[167] Warren and Brandeis, *The Right to Privacy*.
[168] Tal Zarsky.
[169] *Id.*
[170]

Peeping Tom has a long, and in ways severe, history.[171] Tom was the unfortunate boy who stole a look at Lady Godiva as she road naked through the streets as a condition that her husband, the king, would cease to impose backbreaking taxes on the town. Tom was struck blind for his insolence.[172] The image of Peeping Tom has evolved today into something more lurid—a man looking into a woman'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 in her sauna."[173]

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.[174] But Tom obviously stands in for a particular case. As Peter Swire points out, today's "peeping" commonly involves improper access of a database.[175] Swire develops a taxonomy of "peeping" into records, subdividing the act into three levels of severity.[176] 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.[177]

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 that 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 certain 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

---

[171] Solove, Understanding Privacy.

[172] Tom may have gotten off easy; Lot's wife Sarah was turned to stone for looking back on Sodom. [cite]

[173]

[174]

[175]

[176]

[177]

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 here, "it becomes impossible to describe a person who has had his privacy temporarily invaded without his knowledge."[178]

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

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 perspective.[179] 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.[180] 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.[181] There is also a sense in which we as third parties might be harmed by the mere knowledge that such a thing as an inter-dimensional 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

---

[178] Parker at 278.

[179] This is a standard move. See e.g. HLA Hart; Orin Kerr.

[180] One need not resort to science fiction for an illustration of this concept. Consider the examples of memory or imagination.

[181] See supra Part III.A (discussing risk of privacy harm).

hypothetical, of course, the only time Peeping Toms come to light is after they are caught.[182]

CONCLUSION

Just as a burn is as specific and diagnosable condition, so is a 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 in some instances, thereby uncovering the real harm at issue, and to identify privacy harm as it emerges.

This Essay has further argued that, properly understood, privacy harm has two distinct but related components.

[We could look with Katherine Strandburg at the literature around will power, for instance, to size degree of consent. As to extent of impact, we could look with Lior Strahilavitz at social network theory. The approach, in short, advances the science of privacy harm.]

[182] 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* Joel _____, Harm To Others, ___ (denying the coherence of moral harm).