THE NEW INTRUSION

88 NOTRE DAME L. REV. __ (forthcoming 2012)

Jane Yakowitz Bambauer[*]

The tort of intrusion upon seclusion offers the best theory to target legitimate privacy harms in the information age. This Article introduces a new taxonomy that organizes privacy regulations across four key stages of information flow—observation, capture (the creation of a record), dissemination, and use. Privacy scholars typically propose placing constraints on the dissemination and re-use of personal information, and these dominant models are at the heart of President Obama's Consumer Privacy Bill of Rights. But these restrictions conflict with the First Amendment and other important shared values. Instead, observation is the most promising stage for legal intervention.

Intrusion imposes liability for conduct — offensive observations. The tort is theoretically coherent and constitutionally sound because an individual's interests in seclusion co-exist comfortably with society's interests in data dissemination. This puts intrusion in stark contrast with other privacy models, where the alleged harm is a direct consequence of an increase in knowledge. The classic intrusion tort can adapt sensibly to new technologies when it is reduced to two essential elements: (1) an observation, (2) that is offensive. This approach vindicates privacy law's historical roots in torts and offers a path to principled privacy regulation.

[*] Visiting Assistant Professor of Law, Brooklyn Law School; Associate Professor of Law, University of Arizona James E. Rogers College of Law starting fall 2012. B.S., Yale College; J.D., Yale Law School. The author is grateful for the top notch research assistance of John Randall, John Teufel, and Drew Rausa, and for invaluable feedback from Derek Bambauer, Paul Schwartz, Neil Richards, Peter Swire, George Priest, Christine Jolls, James Grimmelmann, Brian Lee, Margo Kaplan, Rebecca Kysar, Jim Park, Sarah Light, Alan Trammell, Cynthia Godsoe, Mark Noferi, Gregg Macey, Miriam Baer, Irina Manta, Robin Effron, Kathie Barnes, Chris Robertson, Marc Miller, Ellie Bublick, Simone Sepe, David Gantz, Bill Sjostrom, Michelle Boardman, Joshua Wright, Tun-Jen Chiang, Bruce Kobayashi, Christopher Newman, Ilya Somin, Jeffrey Parker, Heidi Anderson, Berin Szoka, Mark Noferi, and Annie Decker. This article was generously supported by the Brooklyn Law School Dean's Summer Research Stipend Program.

Contents

I. INTRODUCTION

Before Ralph Nader became a household name for his exposé of the American automobile industry, *Unsafe at Any Speed*, General Motors caught wind of the project and mounted an ill-fated intimidation campaign.[1] GM's agents interviewed Nader's friends and acquaintances to gather information that might be embarrassing for the activist — his political, social, and religious views, sexual proclivities, and odd personal habits.[2] GM hired people to shadow Nader incessantly. At one point, an agent followed Nader into a bank and got sufficiently close to see the exact denomination of bills Nader received from the teller. GM also arranged for young women to proposition him with the hopes of entrapping him into an affair.[3] Nader sued the car manufacturer. The New York Court of Appeals found the surveillance practices of GM's agents to be intrusive and tortious.[4] In assessing GM's conduct, the court famously opined that "a person does not automatically make public everything he does merely by being in a public place."[5]

The tort of intrusion imposes liability on anyone who intentionally intrudes on the seclusion of another if the intrusion would be "highly offensive to a reasonable person."[6] The interest protected by the tort is the right to respite from observation and judgment so that, when we do participate socially, we can be more engaged and ethical participants.[7] Importantly, liability for intrusion has nothing to do with the content of the information discovered. When GM's spy leaned in to observe the exact denominations of bills that Nader was receiving from the bank teller, it constituted an intrusion regardless of whether Nader received twenty dollars, two thousand dollars, or a kitten.[8] The tort's focus on behavior, as

[1] Nader v. General Motors Corp., 25 N.Y.2d 560, 563-65 (N.Y. 1970).
[2] *Id.*
[3] *Id.*
[4] *Id.* The other conduct, while relevant to Nader's claim for Intentional Infliction of Emotional Distress, did not constitute intrusion upon seclusion. *Id.*
[5] *Id.* at 570.
[6] REST. (2D) TORTS §652B.
[7] *See* the discussion of the theoretical underpinnings of a right to seclusion, *infra* Part III.
[8] "Where there is intrusion, the intruder should generally be liable whatever the content of what he learns." Pearson v. Dodd, 410 F.2d 701, (1969). The tort "consists solely of an intentional interference with his interest in solitude or seclusion, either as to his person or as to his private affairs or concerns, of a kind that would be highly offensive to a reasonable man." REST. (2D) TORTS §652B, comment (a). "The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the photograph or information outlined." *Id.*, comment (b). A few courts and jurisdictions have gotten this wrong, and have found that seclusion cannot be intruded if the same information could have been learned through proper means. *See*, *e.g.,* Fletcher v. Price Chopper Foods of Trumann, Inc., 220 F.3d 871 (8th Cir. 2000); Remsburg v.

opposed to content, allows intrusion to coexist comfortably with the First Amendment and other core liberal values that safeguard information exchange. The intrusion tort penalizes conduct—offensive observations—not revelations.

Intrusion has great, untapped potential to address privacy harms created by advances in information technology. Though the tort is associated with conduct in real space, its prinicples apply just as well to operations in the era of Big Data. Suppose GM's agents followed Nader into a large retail store. There, they observed not only Nader's general movement throughout the store, but his specific shopping habits. Suppose they made note of every product Nader browsed, even if he did not put them in his shopping cart. They recorded that he replaced the box of (generically branded) Colossal Crunch with Cap'n Crunch after seeing that the name brand cereal was on sale. And, inexplicably, they knew he decided to come to the store after seeing an advertisement in a newspaper he had been reading earlier in the day. Outlandish as this scenario would be in the physical world, it is entirely consistent with common practices in e-commerce.

Mind-boggling quantities of personal data are logged and collected every time we use our iPhones, tablets, and other gadgets. As companies have increasing access to our data exhaust—data detailing what we have looked at, where we have been, and what we have bought—scholars have become understandably concerned that the information economy has thrust consumers into a new frontier with very little rule of law or consensus of ethics to guide the treatment of personal data.

Contemporary privacy scholarship shuns the old common law privacy torts, contending they are not relevant in the era of ubiquitous computing.[9] Instead, privacy scholars aim to give consumers control over the information that describes them. Paul Schwartz advocates for a right to limit the dissemination of our personal information through quasi-property

---

Docusearch, Inc., 816 A.2d 1001 (N.H. 2003). These opinions miss the heart of the tort, and are anomalous. Some courts also use the tort of intrusion to address harassing behavior that fits the tort of intentional infliction of emotional distress better, as when a debt collector makes incessant, hostile phone calls to a person believed to be the debtor. *See, e.g.,* Hogin v. Cottingham*,* 533 So.2d 525 (Ala. 1988). These, too, are not representative of the tort. Moreover, statutes that outlaw similar behavior (so-called "trespass by telephone" statutes) are on constitutionally infirm ground. *See* People v. Louis, 2011 NY Slip Op 21254 (N.Y. 2011).

[9] Neil Richards, *The Limits of Tort Privacy,* 9 J. ON TELECOMM. & HIGHT TECH L. 357 (2011); Neil Richards & Daniel Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1918 (2010); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1304 (2000); Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1634 (1999); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1231 (1998); Danielle Keats Citron*, Mainstreaming Privacy Torts*, 99 CAL. L. REV. __ (forthcoming 2011).

rights and, in some circumstances, to claw it back from the companies that have it.[10] Joel Reidenberg argues that the United States should pass comprehensive data privacy legislation comparable to the European Union's Data Protection Directive.[11] And anticipating a First Amendment challenge to expansive privacy laws, Neil Richards argues that policymakers can (and should) regulate personal information the way they regulate any other commodity.[12] Efforts by the legal academy and consumer advocates have inspired lawmakers, including the Obama administration, to put forward new laws creating property interests in our personal information.[13] President Obama's Consumer Bill of Rights aims to give consumers "the right to control personal information about themselves."[14] But these laws and proposals create rigid restrictions on the dissemination and re-use of accurate information without fully accounting for the significant social costs of propertizing facts.

This Article makes two contributions to the scholarly discourse—one organizational, and one normative. First, it develops a new taxonomy that tracks the flow of data. Personal information passes through four distinct states where regulation can apply: observation, capture (when a record is created), dissemination, and use. While existing taxonomies organize the theories of information privacy across the harms experienced[15], the framework introduced here flips the orientation. First it determines *how* information can be regulated, and then it analyzes the nature of the harm. By focusing on the practical effects of regulation, the competing interests in privacy and information flow can be evaluated in a consistent manner.

Second, the Article employs the taxonomy to make normative claims about the current and future state of American privacy law among

---

[10] Paul Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2095 (2004).

[11] Joel Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L. J. 771 (1999).

[12] Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149 (2005). The First Circuit adopted Richards' strategy, and ruled that prescription data held by a large data aggregator could be regulated for the same reasons that beef jerky can. IMS Health Inc. v. Ayotte, 550 F.3d 42 (1st Cir. 2008). The opinion was effectively overruled by the Supreme Court's decision in Sorrell v. IMS Health Inc., 131 S.Ct. 2653 (2011). *But see* Neil Richards, *The Limits of Tort Privacy,* 9 J. ON TELECOMM. & HIGH TECH L. 357, 376 (2011) (noting that First Amendment rights must trump privacy interests, at least in the context of the public disclosure tort, because free speech is the more important value).

[13] THE WHITE HOUSE, FACT SHEET: PLAN TO PROTECT PRIVACY IN THE INTERNET AGE BY ADOPTING A CONSUMER PRIVACY BILL OF RIGHTS (press release, February 23, 2012) (hereinafter "Consumer Privacy Bill of Rights"); COMMERCIAL PRIVACY BILL OF RIGHTS ACT OF 2011, S. 799, 112th Cong. (2011).

[14] Consumer Privacy Bill of Rights, *supra* note 13.

[15] Daniel Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002).

private actors.[16] Popular privacy proposals, though politically expedient, will undermine the public's interests in innovation and knowledge-production. In contrast, regulation targeting information flow at its source—at the point of observation—can be significantly expanded without running into conceptual pitfalls.

The intrusion tort is the quintessential example of a restriction on observation.[17] This Article proposes an expansion of the intrusion tort to fit the modern technological landscape. Intrusion should provide recourse not for the creation of personal data, which is a necessary byproduct of well-functioning technologies, but for the *observation* of that data. Since the intrusion tort is conceptually adaptable to changing technology, legal enforcement of the right to seclusion can expand sensibly, outlawing the most disconcerting data practices without imposing unrealistic demands on industry and regulatory enforcement agencies.[18]

---

[16] Future work will use the taxonomy to assess privacy policies for information in the state's possession.

[17] Other scholars laud the intrusion tort, though none fully develop it. Andrew Jay McClurg touted the virtues of intrusion and gave definition to the aims of the tort, but ultimately gave up on the tort as helpful for any actions taken in public that are voluntarily revealed. Andrew Jay McClurg, *Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places*, 73 N.C. L. REV. 989 (1995). Lyrissa Lidsky proposes the expansion of the intrusion tort through the creation of a newsgatherer's privilege, which could take pressure off courts that might be reluctant to impose intrusion liability for fear of interfering with the news media's important functions. Lyrissa Barnett Lidsky, *Prying, Spying, and Lying: Intrusive Newsgathering and What the Law Should Do About It,* 73 TULANE L. REV. 173 (1998). More recently, in describing the limitations on the tort of public disclosure, Neil Richards has concluded that "the law should focus on preventing unwanted collections or accumulations of information, rather than preventing the dissemination of already-collected information" and recommends turning to the tort of intrusion to do so. Neil Richards, *The Limits of Tort Privacy,* 9 J. ON TELECOMM. & HIGH TECH L. 357, 383 (2011).

[18] Europe is experiencing increasing difficulty enforcing its strict data privacy laws without forcing European websites and devices to adopt needlessly clunky interfaces. Marisa Taylor, *Europe Approves New Cookie Law*, WALL ST. J., November 11, 2009. The European Union is struggling to enact and make sense of the Privacy and Electronic Communications Directive (E-Directive), which requires all European countries to enact laws requiring websites to obtain consent before placing cookies on computer users' machines. Implementation of the Directive has been so difficult that the Information Commissioner's Office in the United Kingdom issued a press release announcing that enforcement would not begin for another year. INFORMATION COMMISSIONER'S OFFICE, NEWS RELEASE: ICO GIVES WEBSITE OWNERS ONE YEAR TO COMPLY WITH COOKIES LAW (May 25, 2011); Siobhain Butterworth, *Cookie Law Shambles Really Takes the Biscuit*, GUARDIAN, May 27, 2011. Some commentators have criticized the cookie law, arguing that enforcement is bound to be either arbitrary and capricious or a fool's errand. *See, e.g., The Stupid EU Cookie Law in 2 ½ Minutes*, *available at* http://www.youtube.com/watch?v=arWJA0jVPAc.

A valuable side effect of this project is its vindication of American privacy law's origins in tort.[19] Because the contours of tort law are designed in reference to broader societal interests rather than the interest of a single particular victim, tort is in the best position to address new information problems. It can target and deter practices that eventually reveal themselves to be truly harmful without taking a premature position on how much data is "too much."[20] The Article joins a new wave of pragmatic privacy scholarship bringing precision and rigor to the discourse.[21] It does not recycle the First Amendment critiques of Eugene Volokh[22] or the skepticism of Richard Posner[23]. Rather, it recognizes that if privacy proposals continue to eschew rigorous analysis and to ignore countervailing commitments to the free flow of facts, they will dilute the salience of concrete problems.

We proceed in five parts. Part II introduces the taxonomy and shows why the dominant, property-based privacy law approach has floundered. Part III articulates the virtues of regulating personal information at the source of information flow—the point of observation. The tort of intrusion is already conceptually flexible and is poised to be adapted to new types of invasive observations. Part IV shows how intrusion can be applied to modern settings such as Web tracking technologies and GPS. Part V shows why American law will have difficulty crafting principled regulations on information flow after a legitimate, legal observation has been made. Part VI concludes.

II. PERSONAL INFORMATION PROBLEMS

This Article starts from the assumption that true personal information can cause problems. That is, the subjects described by accurate

[19] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); Neil Richards & Daniel Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CAL. L. REV. 1887 (2010).

[20] The HEW Report, drafted in 1973 and heralded as the seminal source of fair information practices, has a subsection titled "Too Much Data." SEC. ADV. COMM. ON AUTOMATED PERSONAL DATA SYSTEMS, REPORT ON RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS [hereinafter HEW Report].

[21] M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L. REV. 1 (2011); Jacqueline D. Lipton, *Mapping Online Privacy*, 104 NW. U. L. REV. 407 (acknowledging that many privacy responses, including the European Union's Data Protection Directive are ill equipped to respond to privacy issues inherent to user-generated Web content); Felix Wu, *Privacy and Utility in Data Sets* (manuscript on file with author).

[22] Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You*, 52 STAN. L. REV. 1049 (2000).

[23] RICHARD A. POSNER, THE ECONOMICS OF JUSTICE 272 (1981)

personal information can suffer losses that satisfy Ruth Gavison's definition of "actionable violations of privacy" because they are predictable in advance and undesirable for society.[24]

This Part organizes the potential risks and harms caused by personal information into a model of information flow. It then summarizes the most common scholarly responses, and concludes by showing that the privacy law scholars' attachment to a property-style theory of privacy protection has blinded the Academy to better solutions that sound in tort.

A. The Four Regulable States of Personal Information Flow

Personal information flows pass through four regulable stages: observation, capture, dissemination, and use. *Observation* occurs when information is perceived by another. *Capture* is the creation of a record of the information in any medium, such as a photograph, an audio recording, a writing, or a digital log. *Dissemination* is the transmission of the information from one person or entity to another. And *use* occurs when a piece of information directly affects an outcome or determination about the person described by the information.[25] These four stages need not occur in any particular order. In fact, a stage need not occur at all. If a police officer sees a man selling narcotics (observation), he will likely arrest the man (use), and only later complete a police report documenting the incident (capture). If Annie observes Lucy with a piece of toilet paper stuck to her shoe, she might tell Candice, who then tells Lindsay. The information will have been observed and disseminated, but it can dissolve into the ether without ever having passed through the stages of capture and use.

Privacy regulations place restrictions on personal information at one or more of these four stages of information flow. For example, the Wiretap Act prohibits the observation of other peoples' telephone conversations.[26] Video voyeurism laws prohibit certain types of video capture.[27] The Health Insurance Portability and Accountability Act ("HIPAA") restricts the dissemination of health records.[28] The Americans with Disabilities Act prohibits the use of disability information in employment decisions.[29] Some privacy laws craft complex restrictions over multiple stages, but the varied

---

[24] Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L. J. 421, 423 (1980).
[25] This matches the European Union Data Protection Directive, which imposes limitations when data is "used for taking measures or decisions regarding any particular individual." Data Protection Directive, European Union Organization for Economic Cooperation and Development Directive 95/46/EC Article 13(2) [hereinafter *EU Data Protection Directive*].
[26] REST. (2D) TORTS §652B.
[27] Video Voyeurism Prevention Act, 18 U.S.C. § 1801.
[28] 42 U.S.C. § 201 et seq.
[29] 42 U.S.C. § 12101 et seq.

parts of these regulations nevertheless can be organized across these four stages.[30]

The stages are natural points for regulation because the risk of harm associated with a piece of information changes when it enters each new stage. A personal fact can only cause so much damage if it is never captured in a medium that can be easily shared and stored. Likewise, the chance of harm is limited if a piece of information is constrained from flowing beyond a narrow set of people (such as a person's attorney or physician.) These four stages thus provide us with sensible points at which to assess the risk of privacy harms and the wisdom of public laws that might operate on each stage.[31]

B. The Privacy Law Solutions

Privacy scholarship promotes the use of law to protect interests in dignity, autonomy, and self-determinism. These interests are served by giving people some control over others' acquaintance with their personal

[30] The EU Data Protection Directive bans the "processing" of data without the subjects' consent. Processing is the re-organization or analysis of data in order to use existing facts to generate inferences, predictions, or hypotheses. Article (2)(b), EU Data Protection Directive, *supra* note 25. Processing could constitute a distinct stage in the information flow, along with observation, capture, dissemination, and use. But while processing might mark a distinct phase, it is not one that is "regulable" under the First Amendment or the American normative commitments to information. Regulations proscribing the analysis of accurate data do not weed out inferences and heuristics. Instead, they invite inferences based on hunch. Moreover, if a relationship between two characteristics is very strong, processing can be so unavoidable as to be indistinguishable from thought. Since processing is so difficult to detect, as a practical matter privacy laws are better off operating earlier or later in the information stream.

[31] Daniel Solove's taxonomy of privacy problems can map directly onto these four stages. Surveillance (clandestine observation), identification, and fruitful interrogations occur at the "observation" stage. ("Identification" is the attachment of an identity to a previously anonymous piece of information, so it allows an observation about the identified person for the first time, even if the information were already observed in anonymized form.) Aggregation occurs at the "capture" stage since the stage includes the presumed indefinite storage of a record. Exclusion and security occur at the "dissemination" stage, as do all of the privacy problems in Solove's "information dissemination" family—breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, and distortion. Secondary uses are, obviously, "uses" under my framework. Solove's interference family of privacy problems do not map cleanly onto my framework because "intrusions" as Solove categorizes them include harassing acts that are best treated as something other than information-related. "Decisional interferences" are actually observation harms—the chilling effects that can result from government inquiry or surveillance of certain types of acts. Daniel Solove, *A Taxonomy of Privacy*, 154 PENN. L. REV. 477 (2008).

affairs.[32] By exercising control over other's knowledge of ourselves, we can avoid judgment, ridicule, or stereotyping (preserving dignity) while we comfortably pursue the activities we'd like (maintaining autonomy).

Given this orientation, it is not surprising that the solutions put forward by privacy scholars tend to impose stringent restrictions at the dissemination and use stages of information flow.[33] They demand that ultimate control over the fate of personal information be left in the hands of the information subject. In *Code*, Lawrence Lessig asks what presumptive controls consumers should have over the data that they deliberately reveal to others.[34] His legal proposals include a ban on the sale of consumer data unless the customers expressly consent to the transfer.[35] In some cases Lessig suggests privacy should be inalienable; that is, consumers should be legally incapable of consenting to the dissemination of information.[36] Paul Schwartz has argued that Americans should have a sort of property right in information that describes them—that is, they should have an exclusive right to determine where their personal information goes, and how it is used.[37] Recognizing that a simple property model could lead rationally ignorant consumers to sell their information for too little compensation, Schwartz also argues that government regulation should provide a mechanism for the data subject to claw back information they had previously consented to release. In Schwartz's scheme, certain types of especially sensitive information should be subject to inalienable prohibitions on the reuse or dissemination. Jerry Kang's proposals are very similar.[38]

These proposals and others coming out of the privacy literature reflexively reach for the broad-sweeping prohibitions on disclosure and repurposing incorporated into the European Union's Data Protection Directive.[39] Use limitations, notice, and consent are central tenets in

---

[32] Gavison, *supra* note 24 at 426 (quoting Hyman Gross). Gavison finds this definition unhelpful and puts forward her own definition of privacy interests, which break into the categories of secrecy, anonymity, and solitude. *Id*.

[33] *See, e.g.,* Solove, *supra* note 31 (fully half of the privacy problems identified in Daniel Solove's influential privacy taxonomy take place at the dissemination stage, which implies that the regulatory solutions would have to constrain these disseminations.).

[34] LAWRENCE LESSIG, CODE V.2, at 215.

[35] *Id.* at 223.

[36] *Id.* at 227.

[37] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 142-163 (1999); Jerry Kang, *Privacy in Atlantis*, 18 HARV. J. L. & TECH. 229, 255 (2004). Paul Schwartz challenges a Schwartz, *supra* note 10.

[38] Jerry Kang, *Privacy in Atlantis*, 18 HARV. J. L. & TECH. 229, 255-56.

[39] LESSIG, CODE at 227-228; Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1290 (2000); Marc Rotenberg, *Fair Information Practices and the Architechture of Privacy: (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 36 (2001); Froomkin, *supra* note 149 at 1461; Kang, *supra* note __ at 246, 255 (Kang notes

European data privacy laws.[40] These tenets were originally developed by the U.S. Department of Health, Education, and Welfare in the influential Fair Information Practice Principles ("FIPs"), but American law has never required private (non-state) actors to adhere to FIPs.[41] Both the EU's Data Protection Directive and FIPs require notice and consent before information may be disseminated or used for any purpose other than the one for which the information was collected, so regulation that implements these rules necessarily place near-complete restrictions on the regulable stages of *dissemination* and *use*.[42]

The differences between the American and European treatments of information privacy are essentially differences in initial entitlements. In Europe, information *about* a person is *theirs*. The EU Data Protection directive and President Obama's proposed Consumer Privacy Bill grant a property entitlement over personal information to the person described by it. The entitlement does not necessarily incorporate the full "bundle of sticks" we have in our chattels and real property, but it does include the most important ones—exclusive control over use and transfer. An entity is required to obtain consent or negotiate a license before storing, sharing, or reusing personal information, even when that information is revealed in the course of a transaction. Current American privacy law, by contrast, was developed through tort, where privacy interests are protected only when

several differences between the property model and the EU data protection directive, believing that the former springs from an orientation toward market solutions while the latter is designed to protect dignity. But Kang recognizes that the two models both place initial entitlements in the hands of the individuals described in the data. The property proposals from the privacy literature incorporate other protections to prevent the completely free alienability of personal information, so in practice the difference between these approaches would not be as distinct as Kang suggests.)

[40] EU Data Protection Directive, *supra* note 25. The European Commission's recently released draft regulations would amend the EU Data Protection Directive to add a new right to data deletion, a "right to be forgotten", which requires data controllers to delete information upon request, even if the data subject had consented to the collection of the information. EUROPEAN COMMISSION, PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND THE COUNCIL, VERSION 56 (draft of Nov. 29, 2011).

[41] SEC. ADV. COMM. ON AUTOMATED PERSONAL DATA SYSTEMS, REPORT ON RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS [hereinafter HEW Report]; Rotenburg, *supra* note 39 at 41-43. (Rotenburg laments that industry lobbyists do not appreciate and account for the fact that Fair Information Practices were developed by American congressmen. This is an odd criticism since, as Rotenburg acknowledges, FIPs were designed to be an agreement about how the federal government should treat personal data, not private parties.) Some sectors of American enterprise are governed by industry-specific privacy regulations such as the Video Privacy Protection Act and the Health Insurance Portability and Accountability Act ("HIPAA"). These are discussed at length in Part V.

[42] HEW Report, *id*.; EU Data Protection Directive, *supra* note 25.

courts recognize an actionable injury and fault-worthy behavior outweighing other public policy considerations.[43]

The property rights trend in the literature shows that scholars have grown frustrated with American privacy law's roots in tort.[44] Though the earliest vindications of privacy rights emanated from common law tort claims and coalesced, eventually, into the recognizable set that William Prosser dubbed the "privacy torts,"[45] the most influential American privacy scholars have become increasingly frustrated by the void in uniform, overarching privacy policy.[46] They fear that courts are standing idly by as "the Internet guarantees a Nietzchean 'eternal return' of damaging disclosures."[47] They advocate for a fundamental shift in the model for privacy protection to combat a perpetual threat. As Jacqueline Lipton puts it, "We may not have time to develop expectations of privacy that are reasonable before the new wave of privacy-threatening technologies develops and overtakes those expectations."[48]

The property approach certainly has its appeal. A property rule would allow consumers who have strong preferences for privacy to opt out of data aggregations. This works well if society prefers for Americans to decide for themselves what the value of their privacy may be.[49] And, as

---

[43] William Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960); Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (contemplating several restrictions on the right to privacy, including the need to show special damages.)

[44] Murphy, *supra* note 50 at 2388-2393; Neil Richards, *The Limits of Tort Privacy,* 9 J. ON TELECOMM. & HIGHT TECH L. 357 (2011); Neil Richards & Daniel Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1918 (2010); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1304 (2000); Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1634 (1999); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1231 (1998); Danielle Keats Citron*, Mainstreaming Privacy Torts*, 99 CAL. L. REV. __ (forthcoming 2011) (criticizing the privacy torts for failing to recognize new, increased quantities of harm, but also encouraging privacy law to expand from its common law tort roots. Her recommendations focus on expansion of the disclosure tort, with the same end goal as other privacy scholars to restrict information flows and re-uses); Patricia Sanchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J. L. & TECH. 1 (2007) (reconstructing the tort of public disclosure to avoid the "scattershot" nature of existing precedent). Daniel Solove believes that tort law continues to play an important role as a deterrent for individuals who spread rumors or spill secrets. DANIEL SOLOVE, THE FUTURE OF REPUTATION 122-29 (2007).

[45] Prosser, *supra* note 43.

[46] Kang, *supra* note at 235-36; Solove, *supra* note 31; Froomkin, *supra* note 149; Neil M. Richards, *The Limits of Tort Privacy*, 9 J. TELECOMM. & HIGH TECH. L. 357 (2011) (Richards is less pessimistic about tort law, and suggests that other torts and the expansion of confidentiality duties can be used to meet new privacy demands.) *See also*

[47] Citron, *supra* note 44 at 1813.

[48] Lipton, *supra* note 21 at 501.

[49] A property rule would avoid what privacy scholars perceive to be unjust enrichment; since information has value, privacy scholars view the collection of data to be a sort of

with real property, personal information property would allow some Americans to be data holdouts if it is important to them, even if that choice seems irrational.[50] A property system favors the autonomy and self-determination of information subjects over competing interests, such as information access and economic efficiency. It prioritizes privacy, so it is naturally attractive to anyone believing that privacy is not sufficiently guarded today.

Another attractive feature of a property right is its imposition of transaction costs. If an entity must provide notice and obtain consent before collecting or reusing personal data, it will incur non-negligible costs in the process. The data collected must meet some threshold amount of value to be worth the bother of collecting it. As long as transaction costs are non-zero, they will dampen the overall amount of data collected (even from willing consumers.)[51] Privacy scholars who are interested in harnessing the power of defaults, and in using transaction costs to curb overall collection efforts, are obviously interested in something other than consumer autonomy. Paul Schwartz argues that, since consumers cannot be expected to understand the full extent of the privacy consequences when they are asked to consent to data collection, they are likely to trade away their personal information for too little in return.[52] Transaction costs can indirectly counteract the information asymmetries that operate between companies and their customers.

The property model has gained traction. Virtually every lawsuit testing the legality of information collection, including legal challenges against Google, Netflix, DoubleClick, AOL, and Apple, has included claims based on trespass to chattels on the theory that information *about* a person is their personal property. The Federal Trade Commission (FTC) is influenced by current privacy scholarship, and has incorporated the dissemination and re-use limitations from the Fair Information Practice principles directly into its proposed framework for protecting consumer privacy.[53] The legal

theft. Eugene Volokh describes and responds to this argument. Volokh, *supra* note 22 at 1074. Empirical research suggests this value will be quite small for most Americans, anyway. Eric Goldman, *The Privacy Hoax*, FORBES (Oct. 14, 2002); IAN AYRES, SUPER CRUNCHERS 179 (2007) (citing studies that found most people were willing to disclose their social security numbers in exchange for fifty-cents-off coupons). But as with real property, a right to information property would allow some Americans to be data holdouts.

[50] Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEORGETOWN L. REV. 2381, 2397 (1996).

[51] Froomkin, *supra* note 149 at 1535. *But see* Litman, *supra* note 39 at 1299 (voicing skepticism that transaction costs will be significant, and noting that the real issues at stake are the allocations of the entitlements).

[52] Schwartz, *supra* note 10.

[53] FTC STAFF REPORT, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, 6 (2010), *available at* www.ftc.gov/os/2010/12/101201privacyreport.pdf. This is particularly odd since the Federal Trade Commission's consumer protection duties requires the FTC

settlements the FTC has negotiated with major data aggregators like DoubleClick include strict prohibitions on dissemination and repurposing of personal data, suggesting that dissemination and reuse are per se unfair consumer practices.[54] But even if this shift to a subject-control model has the support of the FTC at present, the control model is inherently unstable and unlikely to work long-term.

C. The Problems With Privacy Law Solutions

Americans and Europeans have historically had very different relationships to information.[55] Our enduring commitment to liberalism automatically places great value on unfettered access to facts.[56] In contrast, the Fair Information Practice principles ("FIPs") that form the bedrock of European privacy law grew out of a distrust of data.

FIPs were developed in the 1970s, in an era when computational power and data storage did not have great presence outside the federal government. Though the HEW Report's drafting committee had hoped Congress would apply its recommendations to all systems of personal data collection[57], the harms anticipated by the report were distinctly governmental.[58] While political processes are appropriate tools to constrain

---

and the plaintiffs bar to detect fraud and identify likely victims, both of which are improbable without the aid of data.

[54] Official Court Notice of Settlement in re DoubleClick Inc. Privacy Litigation, Master File No. 00-CIV-0641; FED. TRADE COMM., PRESS RELEASE: FTC ANNOUNCES SETTLEMENT WITH BANKRUPT WEBSITE, TOYSMART.COM, REGARDING ALLEGED PRIVACY POLICY VIOLATIONS, July 21, 2000, *at* http://www.ftc.gov/opa/2000/07/toysmart2.shtm.

[55] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L. J. 1151 (2004).

[56] The inherent value of information is expressed by the influential writings by John Stuart Mill:

> Wrong opinions and practices gradually yield to fact and argument: but facts and arguments, to produce any effect on the mind, must be brought before it. Very few facts are able to tell their own story, without comments to bring out their meaning. The whole strength and value, then, of human judgment, depending on the one property, that it can be set right when it is wrong, reliance can be placed on it only when the means of setting it right are kept constantly at hand.

JOHN STUART MILL, ON LIBERTY (1869).

[57] The HEW Report recommended the submission of legislative proposals to Congress to "establish a code of fair information practice for all automated personal data systems maintained by agencies of the Federal government or by *organizations within reach of the authority of the Federal government*."

[58] The examples in the section titled "Latent Effects of Computer Based Record Keeping," the chapter which describes privacy harms, includes fears of dragnet-style investigation processes, inaccurate welfare distributions, and the FB I's clearinghouse of criminal files.

how the state collects and uses data, those same processes, when directed at facts in private hands, are troubling. Consider, for example, the purpose limitations of FIPs, which constrain a holder of data from using it for any purpose other than that for which it was collected. This rule allows privacy interests to trump other important societal values. Imaginative repurposing of data is now common practice for public health[59] and security[60], sports and entertainment[61], and even core political activities, as demonstrated by the role of Digital Strategy Analysts in the 2012 Obama campaign, who will "analyze web traffic data, email results, social media, SMS data, and other digital information to provide insights" for the President's reelection team.[62] FIPs, though American in origin, are foreign to the regulatory environment that produced the hyper-efficiency of Walmart and the crowdsourced machine learning of Google.

This sub-part first examines constitutional limitations on treating personal information as property, and then demonstrates why a property model is unwise as a matter of public policy.

i. Constitutional Constraints

If a property model for privacy is incorporated into law, it will face a constitutional challenge. Restrictions on the flow of facts—even dry, unadorned facts about people—will receive heightened First Amendment

[59] Internet search terms can reveal epidemiological trends faster than the Center for Disease Control. Alexis Madrigal, *Google Could Have Caught Swine Flu Early*, WIRED, April 29, 2009; Melinda Wenner, *Google Flu TrendsDo Not Match CDC Data*, POPULAR MECHANICS, May 17, 2010 (explaining that the flu can infect an area without causing the fever and respiratory problems that are typically googled. What Google Flu Trends tracks is better understood as tracking flu-like symptoms rather than actual confirmed influenza outbreaks).

[60] Backlogs of crime victim reports and other data have allowed experimental law enforcement programs to use analytics to predict more accurately where larceny and other crimes are most likely to happen and when. The most cutting-edge programs can provide predictions as focused as a one square-block area. Erica Goode, *Sending the Police Before There's a Crime*, N.Y. TIMES, August 15, 2011.

[61] Baseball, which has rewarded fans and team owners who have the patience and aptitude for statistics, is about to undergo another data renaissance with the help of a new technology called Fieldf/x, which records every single motion of each player at every game. If it works as promised, the corrective statistics made popular by *Moneyball* may prove to be completely outmoded. Also, baseball's league awards and pay structure might become one of the most meritocratic systems known to exist. Ira Boudway, *Baseball Set for Data Deluge as Player Monitoring Goes Hi-Tech*, BLOOMBERG, March 31, 2011.

[62] Available at http://my.barackobama.com/Analytics-Jobs. The description of "Communications Analysts" shows the same repurposing of data. Communications Analysts "analyze political data, historical data, press data, and media data to inform our communications teams both nationally and in the states." *Id.*

scrutiny from the current Supreme Court.[63] A default rule that automatically assigns one person exclusive control over another's ability to spread accurate information is likely to be treated as a restriction on speech, and will have to be justified by, and narrowly tailored to, a compelling state interest.[64]

Defenders of a property rule for personal information might be able to avoid constitutional scrutiny by exploiting a loophole. Information is frequently propertized without running afoul of the First Amendment when it is cast as intellectual property. After all, copyright, trademark, the right to publicity, and trade secrets laws restrict the flow of accurate information. The field might have room for privacy rights, too. An extension of the right of publicity, traditionally a celebrity's claim, to a right to personal information property requires but one small hop in reasoning. [65] Consider the precedent set by Rosa Parks, icon of the American civil rights movement. Parks brought a right of publicity claim against Outkast's record label for the reference to her story in their song "Rosa Parks." [66] The chorus to the Outkast song repeats the words

> Ah ha, hush that fuss
> Everybody move to the back of the bus

---

[63] Sorrell v. IMS Health, Inc., 131 S.Ct. at 2667. ("Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs. There is thus a strong argument that prescriber-identifying information is speech for First Amendment purposes.") Lawrence Lessig and Neil Richards have argued that personal data is not "expression" and therefore should not be the basis for First Amendment protection. As a descriptive matter, *IMS Health* has put these arguments in doubt. As a normative matter, I agree with the broader views of the First Amendment, articulated by Derek Bambauer and Eugene Volokh, among others, that in deciding whether a First Amendment protection applies in the first place, we ought not allow the courts decide which types of information count as "speech" and which do not. Derek Bambauer, *Orwell's Armchair*, __ U. CHI. L. REV. __, 8-9 (forthcoming, 2012). Moreover, a test that assigns less protection to expressions that have a higher proportion of dry factual information puts undue emphasis on the proportion of an expression that is made from opinion and point-of-view.

[64] Bartnicki v. Vopper, 532 U.S. 514, 527-528 (2001).

[65] Diane Leenheer Zimmerman, *Information As Speech, Information As Goods: Some Thoughts On Marketplaces and the Bill of Rights*, 33 WM. & MARY L. REV. 665 (1992); Rochelle Cooper Dreyfuss, 1999 STAN. TECH. L. REV. 8 (1999). Right of publicity claims are often lumped under the banner of "misappropriation". I distinguish for the purposes of this article between the tort claim of misappropriation, which protects ordinary people from receiving unwanted and unconsented exposure when their images or names are used to sell commercial products, from intellectual property claims for the right of publicity, which are concerned with the commercial mining and exploitation of celebrity's fame without the celebrity's permission. For the contrast, *see, e.g.,* Carson v. Here's Johnny Portable Toilets, Inc., 698 F.2d 831 (6th Cir. 1983) (permitting recovery when Johnny Carson's celebrity was exploited to market port-a-potties).

[66] Parks v. LaFace Records, 329 F.3d 437 (2001)

> Do you want to bump and slump with us
> We the type of people make the club get crunk.[67]

Parks claimed that Outkast's song exploited the commercial value of her identity.[68] Surprisingly, the Sixth Circuit did not believe that the record label was entitled to summary judgment on their First Amendment defense. According to the court, Parks presented a genuine issue of material fact over the relevance of her name to the song's meaning.[69] The prima facie case for a right to publicity claim is quite easy to establish[70], so without a strong First Amendment limitation, a non-celebrity might be able to claim a property interest in the value of references to her, and facts about her experiences.[71]

But courts are unlikely to make the leap from celebrity rights of publicity to consumer rights of publicity, small as it may be. Intellectual property rights are justified as exceptions to First Amendment restrictions because they work in service of the First Amendment's goals—the production of information and ideas. In theory, intellectual property rights provide economic incentives for the labor required to produce new information goods.[72] The incentive theory doesn't work for privacy rights. Privacy-motivated information property rules attempt to *curb* the production of information, not to foster it.[73] Moreover, the *Parks* case notwithstanding, intellectual property rights propertize the form or expression of an idea, not the idea itself.[74] Raw facts generally cannot be propertized.[75] Intellectual property scholars are often reluctant to endorse a

---

[67] *Id.*
[68] *Id.* at 461.
[69] *Id.* at 442-43.
[70] *Id.* ("All that a plaintiff must prove in a right of publicity action is that she has a pecuniary interest in her identity, and that her identity has been commercially exploited by a defendant.")
[71] This extension of the right of publicity would correspond to Rochelle Dreyfuss's descriptive theory of intellectual property—that courts assign property rights wherever there is value. Dreyfuss, *supra* note 65.
[72] Zimmerman, *supra* note 65 at 667-668; Chakrabarty v. Diamond, 447 U.S. 303, 307 (1980); Eldred v. Ashcroft, 537 U.S. 186, 205, 213-215 (2003).
[73] Under a labor desert theory, it is very likely the data aggregator who will be seen to invest effort creating a usable and probative set of personal information since personal information is only as valuable as its data quality. To understand the effort required to create and maintain usable data, *see* THOMAS C. REDMAN, DATA DRIVEN (2008).
[74] Zimmerman, *supra* note 65 at 667.
[75] Volokh, *supra* note 22 at 1066; Jerry Kang, *Privacy in Atlantis*, 18 HARV. J. L. & TECH. 229, 233 (2004). Hot news misappropriation is an exception to the general proposition that facts cannot be property. *See* INS v. Associated Press, 248 U.S. 215 (1918). But again, this exception rests on a labor desert theory that aims to reward the production of information.

property entitlement over these last vestiges of free speech limitations, even in the pursuit of privacy.[76]

ii. Normative Constraints

Even putting aside First Amendment limitations, privacy scholars have not explained why a property right to control the dissemination and use of truthful personal information would improve social welfare instead of detracting from it. To illustrate, consider a map graphically illustrating the proportion of African-Americans by census tract. This map would fall short of the definition of "political discourse" that privacy scholars acknowledge must be immunized by the First Amendment.[77] Moreover, by reporting information on race, the map would violate the more aggressive privacy proposals requiring consent from data subjects even before aggregated, deidentified information may be disseminated.[78] But it takes just one small addition—the inclusion of voting district boundaries—to turn a dry collection of data into a message teeming with political meaning. It was, after all, a map that led to the coining of the term "gerrymandering." The bounds of Essex County, Massachusetts were molded into a shape that resembled a salamander and was politically convenient for the reelection of Governor Elbridge Gerry.[79] Why should we risk granting exclusive property rights in facts like those to the individuals described in the map?

Usually property entitlements and liability rules are assigned in a way that best ameliorates market information problems. In fact, scholars often attempt to design entitlement systems that have the effect of *forcing* information disclosures since information, by assumption, helps correct market inefficiencies.[80] To understand why property entitlements do not work very well with personal information, first consider why they do work

---

[76] Even Rochelle Dreyfuss, who enunciated the clearest jurisprudential path to propertization of personal information, advised against widening the scope of intellectual property since the recent expansions of intellectual property have been unprincipled. Dreyfuss, *supra* note 65 at 25. *See also* Zimmerman, *supra* note 65 (worrying that the expansion of intellectual property theories is "cannibalizing speech values at the margin"); LAWRENCE LESSIG, FREE CULTURE (2004).

[77] Richards, *supra* note 12 at 3.

[78] Lee Tien, the staff attorney for the Electronic Frontier Foundation, proposes a statute requiring consent to be obtained before de-identified data can be released. Natasha Singer, *Data Privacy, Put to the Test*, N.Y. TIMES, April 30, 2011.

[79] Mass. Hist. Soc., *The Birth of the Gerrymander,* available at http://www.masshist.org/objects/2008september.cfm.

[80] Ian Ayres & Eric Talley, *Solomonic Bargaining: Dividing a Legal Entitlement to Facilitate Coasean Trade*, 104 YALE L.J. 1027, 1031-32 (1995); LOUIS KAPLOW & STEVEN SHAVELL, FAIRNESS VERSUS WELFARE 411 (2002).

so well with tangible objects.[81] Lisa owns a coffee mug, and knows what it is worth to her better than a court, or the state, or some objective third party does. Likewise, Milhouse, a putative buyer, is in the best position to estimate what the coffee mug is worth to him. If Milhouse values the mug more than Lisa, then a transaction should occur, the buyer and seller will both experience an increase in utility, and overall social welfare will improve. A third party's judgment couldn't possibly be superior because Lisa and Milhouse have significant private information about how they would use the mug, and about their tastes and preferences.

A market for information, or more precisely, a market for rights to disseminate information, has a number of quirks and difficulties. First, information is a nonrivalrous good—everybody can have it at once. If Lisa could keep her mug *and* give it to Milhouse at the same time, it is no longer obvious that Lisa should have exclusive rights to it. Also, information problems are definitional. The value of a piece of personal information is very difficult for the information subject to determine, and it is impossible for the would-be purchaser, since the utility of new facts are hard to predict and are diffused across the entire population who may eventually come into contact with it. Two illustrations will help show why the property model is a poor fit.

First, consider the easy, Posnerian case against property rights.[82] Suppose a man desires to conceal his marriage to the women he meets on Match.com. A woman who uncovered his secret after several dates wishes to describe his behavior on TrueDater.com, a website that allows people to report complaints about members of online dating services.[83] The married man will demand a high price for a license to TrueDater to distribute this information. Under these facts, the holdout problem is obvious. The people who might value the information most—Match.com users who are looking for truthful partners—don't know what they are missing, and are unlikely to be organized enough to purchase his consent.[84] The social value of information dissemination—both to the specific Match.com users who have the misfortune of dating him and to the general public, which would prefer to deter adultery through disapproval—would easily outweigh the man's utility in secrecy. In fact, we might even think that a preference for secrecy in these circumstances is an "objectionable preference" that should not be

[81] Much of this example is borrowed from Richard Posner. RICHARD POSNER, ECONOMIC ANALYSIS OF LAW 37-38 (1998).

[82] This example is similar to Richard Posner's example of the sexually abusive school teacher. Richard Posner, *The Economics of Privacy*, 71 AM. ECON. REV. 405, 406 (1981).

[83] Lizette Alvarez, *(Name Here) Is a Liar and a Cheat*, N.Y. TIMES, February 16, 2006.

[84] Even if there were a business model for TrueDater, similar to the CarFax model, the married man will charge an exhorbitant price or hold out entirely. These problems do not plague businesses like CarFax that rely on records that are not under the control of the individuals selling the cars.

accorded any weight in the social welfare calculus (or put differently, that notions of justice and fairness ought to trump the adulterer's privacy interests.)[85] But under a property model, the information exchange would not happen, and the bulk of social costs would fall on a few "local losers" who end up dating him without knowing his true motivations.

The potential for fraud, deceit, and other perverse incentives is the most commonly deployed critique of privacy coming out of the law and economics literature.[86] But this critique is too facile: just because privacy *could* be abused does not, necessarily, mean that the model is deeply theoretically flawed. After all, opportunistic holdouts in real estate markets are a known and difficult problem, but they do not merit the abolishment of property rights.[87] The relevant question is whether even the ethical and reasonable personal information holdouts would tend to detract from overall social welfare. Indeed they would.

Consider the much more sympathetic facts of *Sipple v. Chronicle Publishing Co.*[88] In 1975, Oliver Sipple was living an openly gay life in San Francisco, but like so many men in the gay community at the time, his sexual preference was not known to his family. When President Gerald Ford visited San Francisco that year, Oliver Sipple saved his life by thwarting an assassination attempt. He struck the gun out of the hand of Sara Jane Moore, who was standing near Sipple during President Ford's public appearance. Sipple instantly became a national hero, but his story took a sad turn when several newspapers printed quotes from Harvey Milk suggesting that President Ford's hesitation to call or telegram Sipple with an expression of gratitude was caused by homophobia. The news reached Sipple's family in Detroit, and they subsequently disowned him. He passed away just five years after his unsuccessful lawsuit against the San Francisco Chronicle and other newspapers, a penniless and devoid of valuable

[85] KAPLOW & SHAVELL, *supra* note 80 at 427. Kaplow and Shavell would object to characterizing these valuation decisions as decisions driven by concerns for fairness, but the authors struggle, as others had before them, to find any pure economic rationale for dismissing and ignoring certain types of idiosyncratic preferences, such as preferences for sadism. *Id.* Richard Murphy preferred not to count the utility derived from deceit in his social utility calculus. Murphy, *supra* note 50 at 2386. I agree with this impulse, but note that it highlights a larger problem with utilitarian theories that command the analyst to make decisions, based on ethics, about what types of pleasure should and should not count as utility.

[86] Posner, *supra* note 82 at 406.

[87] Moreover, sometimes property rights *are* extinguished. Eminent domain provides relief when hold-outs are judged to be counter-productive. Monongahela Nav. Co. v. United States, 148 U.S. 312, 326 (1893). Sara Rimer, *Harvard's Anonymous Land Purchase Receives Criticism*, JOURNAL RECORD, June 20, 1997.

[88] Sipple v. Chronicle Publishing Co., 201 Cal. Rptr. 665 (Ct. App. 1984).

possessions save for the framed copy of his letter from President Ford (which was postmarked three days after the assassination attempt.)[89]

Given Sipple's accurate estimation that his family would react very badly to news about his homosexuality, Sipple would have valued a property right in his personal information highly. But the utility of the story to social welfare would likely be greater still. This was, after all, a culture-changing story. Sipple was one of America's first strong, gay, heroic figures. A wide range of people may have benefited from the Chronicle's story: those whose perception of homosexuality improved, those who valued knowing more about President Ford's potential prejudices, those in the gay community who experienced pride, or who faced a very slightly smaller amount of hostility because of Oliver Sipple's story. The San Francisco Chronicle, too, received reputational rewards for its newsgathering.[90] These benefits are unmeasurable and uncertain, but they receive considerable presumed weight. At least, that is the reasoning behind the core belief that "freedom of discussion, if it would fulfill its historic function in this nation, must embrace all issues about which information is needed or appropriate to enable the members of society to cope with the exigencies of their period."[91]

Under a property model, the San Francisco Chronicle would not have bought the rights to Sipple's personal information. The story would not have increased the prestige of the Chronicle enough to be worth the high price tag. Though the story was valuable to a wide range of other people, a sale of the information license would have required the coordination of an impossible network of transaction and valuation costs.[92] The fate of these facts was better off in the hands of the Chronicle and the other journalists, even though this rule sacrifices Sipple at the altar of social progress.

Sipple's losses were quite weighty since he was a member of a minority group that was heavily and irrationally stigmatized at the time. [93] Still, even under these very sympathetic circumstances, a right to hold out,

---

[89] Dean Morain, *Sorrow Trailed a Veteran Who Saved a President's Life and Then Was Cast in an Unwanted Spotlight*, L.A. TIMES (FEB. 13, 1989).

[90] If not, providing Sipple with an entitlement of any sort (let alone a property right) would not be economically efficient. Guido Calabresi and A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972). Speculation about the value of personal information also suffers from the problem of assessment costs.

[91] Thornhill v. Alabama, 310 U.S. 102 (1940).

[92] KAPLOW & SHAVELL, *supra* note 80 at 410.

[93] Guido Calabresi and Douglas Melamed warn against any analysis that favors economic efficiency and treats all costs with equal weight without regard for other considerations such as distributional effects and social justice. *Id.* Likewise, Kaplow and Shavell encourage models other than equal distribution when aggregating utility, including Rawlsian models that might weight the interests of the poor and underprivileged more heavily. KAPLOW & SHAVELL, *supra* note 92 at 28-29.

or scrape back, information will frustrate attempts to seize teachable moments and allow information to slowly winnow the misimpressions that caused so much grief in Sipple's day. *Sipple* illustrates the general point that privacy losses are the negative externalities from an otherwise productive and worthwhile activity—information flow.

Information flow should be deterred through liability rules when, and only when, the foreseeable privacy harms outweigh the benefits of free-flowing facts.[94] This is not to say that privacy must succumb to information absolutism.[95] Balances must be struck. Tort law is optimally suited to this task; property entitlements are not.

D. Personal Information Problems Are (Still) Tort Problems

The privacy law approach to information harms is misguided because it prioritizes the autonomy and self-determinism of an information subject over competing autonomy interests of the information-holders, and the societal interests in unencumbered information flow. Very few rights are absolute, and our rights to privacy and to information-access are not among them. A defensible system of privacy must analyze whether the social costs of free information flow outweigh the expected benefits.[96] Thus, an optimal

---

[94] Low stakes scenarios lead us to the same result. Suppose Hulu.com viewers were able to exercise a property right and withhold consent to use their viewing history information for directed advertising (or for any purpose other than serving the television shows they would like to watch.) In the best case scenario, the privacy-seekers would absorb the costs of forcing the site to supply a different business model—either in the form of having to watch more advertisements or by having to pay to watch the Hulu content. But since differentiating between viewers and creating different platforms imposes transaction costs on Hulu, it is more likely that Hulu will keep a single platform and force all viewers to absorb the additional costs—in the form of more advertisements, for example—that result from the privacy-seekers' withheld information. The property interest creates a free rider problem.

[95] Eugene Volokh makes the descriptive claim that a restriction on the flow of personal information would not survive constitutional scrutiny even if the restriction *did* maximize aggregate social utility. Volokh, *supra* note 22 at 1076. This may well be true, but this Article asks how information *should* be regulated. As a practical matter, since the utility of privacy and speech cannot be measured, one could argue that First Amendment strict scrutiny (requiring a compelling state need and tailoring) *is* a utilitarian test—one that assumes a high value in speech and looks searchingly for evidence of countervailing factors.

[96] This is the basic welfare economics model. Louis Kaplow & Steven Shavell, *Fairness Versus Welfare*, 114 HARV. L. REV. 961, 977 (2001). Paul Ohm, too, uses a utilitarian model and advises regulators to compare the risks of unfettered information flow to its likely costs in privacy. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1768 (2010). Note that this model is flexible as to what types of "harm" are accounted. Thus, it is not necessary to come up with one unifying theory of what constitutes a privacy harm. I tend to agree with

collection of privacy regulations will deter the sorts of information flows that tend to create more disutility than utility. This is exactly what common law tort rules aspire to do.[97]

A tort treatment of information harms has the virtue of assessing the new risks of personal data aggregation without committing to a certain predetermined end state. While privacy law scholars automatically code all increases in personal data accumulation as a threat, tort scholars are open-minded about the appropriate activity level, so long as the activity is not posing undue risk.[98] Thus, while privacy law scholars want a particular end state—less data shared with fewer people—tort law scholars are indifferent about the end state so long as the law deters harmful and objectionable acts.

Privacy scholars have given up on tort in part because they have become preoccupied with controlling the dissemination of data. The tort addressing personal information flows at this stage—the tort of public disclosure of private facts—has been chiseled away by case law.[99] But in their haste to find a new means of controlling dissemination, privacy scholars have overlooked a tort that operates at the stage of observation—the tort of intrusion.

By way of example, consider a hypothetical posed by Patricia Sanchez Abril:

> Fiona is gay but has not told her co-workers or professional acquaintances. George, one of Fiona's co-workers, secretly obtains her MySpace password so as to snoop around her profile. On her profile, he finds information that leads him to believe that she is leading a gay lifestyle. George instantly divulges this information to the rest of the office staff. As a result, Fiona suffers a great amount of stress and is ostracized by some of her colleagues. Her work and her career are subsequently jeopardized.[100]

Daniel Solove that this is a futile task. DANIEL SOLOVE, UNDERSTANDING PRIVACY ix (2008).

[97] Risk-utility models were originally anticipated by Samuel Warren and Louis Brandeis, whose groundbreaking article on privacy cautioned that privacy rights should not interfere with access to valuable information. Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890)

[98] KAPLOW & SHAVELL, *supra* note 80. Cf. Litman, *supra* note 39 at 1303; Richards, *supra* note 12.

[99] *See,* e.g., Neil Richards, *The Limits of Tort Privacy*, 9 J. TELECOMM. & HIGH TECH. L. 357 (2011). As Richards points out, much of this chiseling has been done for good reason in light of the speech interests implicated by the tort. For a full discussion *see infra* Part V.

[100] Abril, *supra* note 44 at 40-41.

Abril focuses on the fact that George *divulges* the information and causes suffering to Fiona—suffering that is not recoverable under the tort of public disclosure of private facts since Fiona's sexual preferences are neither private facts nor highly offensive to a reasonable person.[101] To fix this injustice, Abril recommends a major overhaul of the public disclosure tort despite that tort's inherent inconsistency with free expression and unobstructed information flow.[102]

Abril overlooks the more compelling fact that George broke into Fiona's MySpace account. This behavior fits quite comfortably within existing routes of recovery under the tort of intrusion and intrusion-style statutes.[103] By casting Fiona's cause of action as an uncontroversial, straightforward application of the intrusion tort, Fiona's recovery will avoid what Anita Bernstein calls the "novelty paradox"—the reluctance of courts to compensate new forms of injury precisely because they are new.[104] Moreover, the intrusion tort allows Fiona to recover from George based not only on the injuries *his* disclosures caused, but all the disclosures springing from it. Just as trespassers are liable for the full spectrum of damages they cause regardless of their intentions[105], George will be liable for the mental distress caused by hacking into Fiona's account, for the distress caused by his releasing the information to others, and for the distress caused by those others' spreading the information further.

The tort of intrusion and its potential for expansion are explored in the next two Parts.

III. OBSERVATION AND CAPTURE

We begin at the source of personal information flow by assessing the harms caused by observation and information capture, and the typical legal responses to them. Observation and capture are traditionally analyzed together, as "data collection,"[106] but observation and capture raise distinct and interesting problems that can be profitably explored by disentangling

---

[101] *Id.*
[102] *Id.*
[103] George's behavior is a criminal violation of the federal Computer Fraud and Abuse Act, 18 U.S.C. §1030. A Michigan resident is facing a possible five year sentence for using his wife's password to log into her Gmail account, in violation of Michigan state anti-hacking law. Sara Wilson, *Clara Walker: Leon Walker 'Violated My Privacy'*, HUFFINGTON POST, Jan. 5, 2011.
[104] Anita Bernstein, 75 TX. L. REV. 1539, 1544-47 (1997).
[105] *See*, e.g., Van Alstyne v. Rochester Telephone Corp., 296 N.Y.S. 726 (1937) (imposing liability for the poisoning of two dogs when telephone company trespassed by leaving small bits of cable insulation containing lead, which were then consumed by the dogs.)
[106] Richards, *supra* note 12 at 1182.

the two stages. The recent spate of state wiretap act prosecutions charging citizens who recorded their interactions with police officers on cell phones[107] shows the obvious tension between observation and capture: If somebody is allowed to observe something, why isn't he allowed to make a record of it? When do the acts of observation and capture raise sufficiently different privacy risks? This Part begins by analyzing observation alone, and then considers the nature of information harms caused by capture.

A. Observation

Suppose an obstetrician invites a friend to watch him perform a childbirth. The expectant mother mistakenly assumes that the friend, dressed in scrubs and introduced as a "helper," is a medical student or surgical assistant.[108] The friend's observation may have been quite valuable to him personally. Perhaps it indirectly improved the world by inspiring the friend to attend nursing school. Nevertheless, the observation was tortious.

The tort of intrusion imposes liability on anybody who intentionally intrudes on the seclusion of another if the intrusion would be "highly offensive to a reasonable person."[109] The intrusion tort protects an interest in respite from observation and judgment (when the expectation of seclusion is reasonable.) A right to seclusion is justified by a number of theories: Seclusion allows us to engage in "productive secrets"—surprises may be planned, plots may be concocted, and new aspects of our individuality can be tried out without censure.[110] Richard Posner promotes a right to seclusion on the theory that the effectiveness of communications will diminish if we worry that uninvited intruders are listening in.[111] Julie Cohen argues that zones of limited access promote individuality and noncomformity.[112] Seclusion is where we groom ourselves, both literally

---

[107] David Rittgers, *Maryland Wiretapping Law Needs an Update*, BALTIMORE SUN, June 1, 2010; Heidi Reamer Anderson*, The Mythical Right to Obscurity: A Pragmatic Defense of No Privacy in Public*, __ I/S __ (forthcoming 2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1759374.

[108] Based on the facts of De May v. Roberts, 46 Mich. 160 (1881). *See also* Sanchez-Scott v. Alza Pharmaceuticals, 86 Cal.App.4th 365 (2001) (A pharmaceutical sales representative intruded on a patient's seclusion when he observed a breast examination because the patient's consent to his presence was predicated on the false assurance that the sales representative was a doctor.).

[109] REST. (2D) TORTS §652B.

[110] Gavison, *supra* note 24 at 443; Solove, *supra* note 31 at 551; Joel R. Reidenberg & Francoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in the Network*, 30 WAKE FOREST L. REV. 105 (1995) (arguing that privacy on the internet is necessary in order to promote trust and exploration).

[111] Posner, *supra* note 82 at 408.

[112] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000).

and figuratively. It's where a person can practice and fail in peace. In the words of Ralph Waldo Emerson, "solitude, the safeguard of mediocrity, is to genius the stern friend."[113]

The intrusion tort avoids conflict with information flows because the psychic harms and chilling effects caused by intrusions are independent from the production of new knowledge. Though recognition of "seclusion" sometimes depend on the likelihood that sensitive information could be generated, such as behind the drawn curtain in a hospital emergency room or inside a hanging file marked "Private", strictly speaking an intrusion has nothing to do with the content of the information that was discovered. A voyeur who peers through the windows and observes a mundane family scene has intruded upon the family's seclusion even though he has not learned any secrets.

Observation is a natural and necessary part of the human experience, so liability must be reserved for behavior that incorporates a sufficient amount of intent and effort. Intrusion guards our affairs from the "prying eyes or ears of others."[114] It only offers a remedy when the eyes and ears are *prying*—that is, when an intruder has notice of a person's reasonable expectation of seclusion and intentionally makes an observation anyway. An intrusion requires a deliberate investigation. But by the same token, when a deliberate, obnoxious observation has taken place, liability is appropriate even in instances where the information learned ends up being highly valuable or newsworthy.[115]

Because the intrusion tort regulates behavior, its connection to speech, news, and the free flow of information is tenuous enough to avoid conflict with the First Amendment. Intrusion-style provisions in federal statutes like the U.S. Wiretap Act (prohibiting the interception of conversations)[116], the Stored Communications Act (prohibiting the unauthorized access of e-mail and other electronic communications)[117], and the Computer Fraud and Abuse Act (prohibiting hacking into another's computer accounts and personal files)[118] have avoided coming into conflict with the First Amendment jurisprudence.

Intrusions are in the class of activities that tort law attempts to deter completely.[119] It is in the public's interest to penalize intruders even if the

---

[113] RALPH WALDO EMERSON, CONDUCT OF LIFE 134 (1860).
[114] Nader v. General Motors Corp., 25 N.Y.2d at 566.
[115] *Barber v. Time Inc.*, 348 Mo. 1199 (1942) (liability and punitive damages imposed on Time Magazine for taking and publishing a photograph of a patient with a rare physical ailment after she explicitly denied consent).
[116] Wiretap Act (Title III), 18 U.S.C. §§ 2510-2522.
[117] Stored Communications Act, 18 U.S.C. §§ 2710-2712.
[118] Computer Fraud and Abuse Act, 18 U.S.C. §1030.
[119] Like other intentional torts, intrusion aims to penalize anyone who evades the information market and intentionally observes without permission. Since the optimal

subject is unaware that he is being observed. Indeed, many intrusion-based laws (like the Wiretap Act) assign criminal liability for intrusion irrespective of the observed's awareness that his seclusion had been violated. But given the heavy sanctions that can be applied to intrusive acts, courts are under significant pressure to craft a definition of "seclusion" that serves the best interests of the community. This is no easy task.

If seclusion is defined too narrowly, intrusion will be little more than an extension of trespass law, protecting places only. A narrow version of seclusion might prevent parabolic microphones, binoculars, and other sense-enhancing technologies that effectively transport the intruder into the home, but this is little more than a conceptual extension of a property line, and leaves out many contexts where the observed might expect and profit from respite.

On the other hand, an expansive version of "seclusion" could inappropriately constrain everyone else. It could hamper our own information-gathering practices that we instinctively rely on in order to learn from the experiences of others. Observation also plays an important role in the class structure of American society.[120] Unseemly tabloid stories, so reviled by Warren and Brandeis, tear down the barriers that separate elites from the rest.[121] These barriers are composed of etiquette and social norms. They are, in other words, made from the same things that forge expectations of privacy and seclusion. Courts face a dilemma when having to decide which of these norms of etiquette to enshrine into the right of seclusion, and which to leave unprotected by the rule of law.

The paparazzi scandals surrounding the death of Princess Diana, and the wiretapping scandals of Rupert Murdoch's News of the World tabloid are reminders that some acts of observation cross a line that even news-lovers find unethical and repugnant. On the other hand, the aggressive newsgathering that helped break stories about the sexual exploits of John Edwards and the investigative reporting tricks that helped expose abusive

---

activity level for intentional torts is zero, we should embrace any enforcement and deterrent that proves to be cost-effective. *See* POSNER, *supra* note 81 at 226-227.

[120] Whitman, *supra* note 55.

[121] Ryan Linkof elegantly makes this point in a recent op-ed in the *New York Times*.

> Watching the painfully choreographed, and highly policed, red-carpet arrival of Prince William and Kate Middleton at a recent Los Angeles polo match reminded me why intrusive journalistic tactics are often called upon. They exist to break down the barriers of access that keep social elites at a remove from ordinary people. The tabloids, throughout history, on both sides of the Atlantic, have been predicated on chipping away at that division. They play a fundamental role in democratic cultures, especially in societies characterized by the pull between the demands of a mass society and the persistence of social and economic inequality.

Ryan Linkof, *Why We Need the Tabloids*, N.Y.TIMES, July 19, 2011.

medical facilities are reminders that nosiness should be tolerated all the way up to that line.[122] Thus, the definition of seclusion must find a balance between the remoteness every human legitimately counts on, and the curiosity that every human legitimately explores.

Difficult as it may be to elucidate the definition, courts have not had too much trouble knowing seclusion when they see it. A strip search invades seclusion.[123] Cameras mounted in holding cells at a city jail do not.[124] A public restroom provides seclusion most of the time[125], but when a long masturbation session is interrupted by a janitor with a duty to oversee the safety of the restrooms, there is no violation of seclusion.[126] A wife does not have seclusion from her husband in their bedroom when her husband is there with her, but she *does* have seclusion, even from her husband, when she is alone in the same bedroom.[127] The site of a bad automobile accident does not offer seclusion to the accident victims, but the inside of the rescue helicopter does.[128]

Seclusion can be found in public spaces, as when a scorned lover conducts constant surveillance from exclusively public places. [129] But courts require public surveillance to be unusually dogged before assigning liability.[130] As described in the Introduction, intentionally leaning in to observe the money that Ralph Nader withdrew from his account is an intrusion. But if Nader kept his bills out and flaunted them as he walked through the bank, then the same intentional observation (even if performed for malicious purposes) would not be intrusive.[131] Seclusion cloaks our documents and affairs as well. If a person accesses a foe's bank records or medical records through fraud, he has intruded upon his foe's seclusion.[132]

---

[122] Emily Miller, Op-Ed, *John Edwards Indictment a Vindication for National Enquirer*, WASH. TIMES, June 3, 2011.
[123] Helton v. U.S., 191 F.Supp.2d 179 (D. D.C. 2002).
[124] DeBlasio v. Pignoli, 918 A.2d 822 (Penn. 2007).
[125] Kjerstad v. Ravellette Publications, Inc., 517 N.W.2d 419, 422 (S.D. 1994).
[126] Hougum v. Valley Memorial Homes, 574 N.W.2d 812 (ND 1998).
[127] *In re* Marriage of Tigges, 758 N.W.2d 824 (Iowa 2008).
[128] So is the quiet conversation between the accident victim and the doctor that came to the scene, because the conversation might have been heard only with the help of microphones. Shulman v. Group W Productions, Inc., 955 P.2d 469 (Cal. 1998).
[129] The *Nader* line of reasoning has been followed in other jurisdictions as well. Kramer v. Downey, 680 S.W.2d 524 (Tex. 1984) (holding incessant observation by a scorned ex-lover, even though she stayed on public property to do so, was an intrusion upon seclusion justifying a jury damages award).
[130] *Id*.
[131] Nader v. General Motors Corp., 25 N.Y.2d at 570-71.
[132] Brex v. Smith, 104 N.J.Eq. 386 (1929); Zimmerman v. Wilson, 81 F.2d 847 (3d Cir. 1939); Frey v. Dixon, 141 N.J.Eq. 481 (1948); State ex rel. Clemens v. Witthaus, 360 Mo. 274 (1950); Bednarik v. Bednarik, 18 N.J.Misc. 633 (1940).

The distinction between the rights enforced by the intrusion tort and the rights enforced by the broadsweeping data privacy regulations proposed by privacy scholars is not simply a difference between tort and property. Indeed, the line between property and intentional torts is blurred.[133] This is easiest to see with the tort of trespass, which enforces property rights to exclusively control access to land and tangible property. Likewise, exclusive control over our seclusion is in some sense a property-like entitlement that we are free to horde or share as we please. Countless facebook posts have proven that we are free to give away our seclusion if we do not value it highly. When we do maintain seclusion, our right to exclusively control over it is enforced through the intrusion tort. The main distinction between intrusion and the other privacy proposals is the object of the exclusive control. With the latter, the object of exclusive control is information; with the former, it isn't. This is why intrusion coexists so comfortably with other normative commitments.

The tort of intrusion reinforces norms by tracking social consensus, which means that most people will recognize what is and is not seclusion, even in new contexts. This makes the tort especially flexible and appropriate for application to new technologies. New applications of the tort will be discussed in Part IV. To make the discussion fruitful, we next consider regulations of information capture.

B. Capture

The capture stage of personal information flow presents a number of puzzles. Occasionally law forbids recording a person or event even if observation of the event is legal. These laws apply to mechanical capture—photographs, videos, audio recordings, and other means of capture that are sufficiently automated.

For example, some state wiretapping statutes contain an important deviation from the federal analog, the Wiretap Act. Federal law penalizes anyone who intercepts a private conversation, but if one party to the conversation chooses to record the conversation (or to have some third party listen in and record it for them), that capture is lawful.[134] The Wiretap Act is a "one-party consent" statute: if one party to the conversation consents to recording or interception, the penalties do not apply. Several states have enacted wiretap laws imposing civil or criminal penalties unless *all* parties to a conversation consent to the recording. These statutes have sparked public debate and criticism recently because citizens in Massachusetts, Illinois, Pennsylvania, and Maryland have been charged or prosecuted

[133] WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF TORT LAW, 30 (1987).
[134] 18 U.S.C. §2511(2)(c)

under the wiretap statues for recording their own interactions with state police officers.[135] However well-intentioned legislators may have been when the laws were adopted, the inexorable inference is that state police forces are exploiting the laws to evade public accountability.[136]

Courts have not created First Amendment safeguards for the use of recording devices. Photographs, video capture, and audio recordings are often found to lack the authorship or expressive character necessary to be considered speech[137], and recording equipment is not among the "indispensable tools of newsgathering" that receive derivative protection under the First Amendment.[138] The iPhone and the citizen-blogger might make one question whether the law accurately reflects today's news media landscape.[139] To take just one recent example, a bystander's photographs of Lt. John Pike pepper spraying Occupy movement protesters on the U.C. Davis campus catapulted the story into the national headlines and sparked a satirical Internet meme wherein the Lieutenant appears in famous works of art, casually pepper spraying the subjects.[140] Recent case law has begun to recognize a constitutional right to film public officials performing their official duties.[141] We may see this narrow right to capture expand in due time.

---

[135] Anderson, *supra* note 107.

[136] *Id.*

[137] Kelly v. Borough of Carlisle, 622 F.3d 248 (3d Cir. 2010); Pomykacz v. Borough of West Wildwood, 438 F.Supp.2d 504, 513 n.14 (D.N.J. 2006) (stating that an "argument can be made that the act of photographing, in the abstract, is not sufficiently expressive or communicative and therefore not within the scope of First Amendment protection—even when the subject of the photography is a public servant" (quoting Eruv Ass'n, Inc. v. Borough of Tenafly, 309 F.3d 144, 160 (3d Cir. 2002))); C. Thomas Dienes, *Protecting Investigative Journalism*, 67 GEO. WASH. L. REV. 1139 (1999). Perhaps in light of Justice Kennedy's reasoning in *Sorrell v. IMS*, the right to mechanical capture can be tested again. Sorrell v. IMS Health Inc., 131 S.Ct. 2653 (stating that "Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs. There is thus a strong argument that prescriber-identifying information is speech for First Amendment purposes.").

[138] Dietemann v. Time Inc., 449 F.2d 245 (9th Cir. 1971); Shulman v. Group W Productions, 18 Cal. 4th 200, 239 (1998); Shevin v. Sunbeam, 351 So.2d 723, 727 (Fla. 1977);

[139] Seth Kreimer makes a powerful case for First Amendment protection of image capture. Seth Kreimer, *Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right to Record*, 159 U. PENN. L. REV. 337 (2011).

[140] Robin Wilkey, *John Pike Memes Go Viral: Pepper-Spraying UC Davis Cop Becomes Internet Sensation*, THE HUFFINGTON POST, Nov. 21, 2011 (http://www.huffingtonpost.com/2011/11/21/john-pike-memes-go-viral_n_1106616.html).

[141] "Gathering information about government officials in a form that can readily be disseminated to others serves a cardinal First Amendment interest in protecting and promoting 'the free discussion of governmental affairs.'" Glik v. Cunniffe, Docket No. 10-1764 at 9 (1st Cir. 2011)(quoting Mills v. Alabama, 384 U.S. 214, 218 (1966).) The U.S. District Court for the Eastern District of Pennsylvania recognized a First Amendment right

Putting aside the First Amendment's application, when does mechanical capture alone, *without* observation, create serious risks? In the uncommon instances where a plaintiff has sued for intrusion based on capture alone, without alleging an offensive observation, the act of capture implied that the information would, eventually, be used for some lascivious or inappropriate purpose. For example, the plaintiffs in *Hamberger v. Eastman* were tenants who discovered that their landlord had installed hidden video cameras in the bedroom of their apartment.[142] The landlord attempted to evade liability for intrusion by arguing that the plaintiffs could not prove he actually viewed the video footage, but the court was not impressed with this argument.

Suppose, though, that the landlord had installed the video camera so that it monitored only the inside of the front door, and had a practice of not reviewing the footage unless a crime or emergency warranted it. The outcome of the case under those alternative facts is less certain. The recordings that were actually made, though, were so unlikely to be useful for any purpose other than the landlord's recreation that the court was compelled to impose liability even without evidence of an offensive *observation*.

Law addressing capture on its own, untethered from observation, is sparse, but two factors seem necessary. First, the subjects must have insufficient opportunity to prevent the intentional observation, and second, the record must have no redeeming social value. The facts of *Hamberger* satisfy both of these elements, as do video voyeurism laws, which prohibit surreptitious capture of other people's "private areas" irrespective of whether the images are ever observed.[143]

The Video Voyeurism Prevention Act imposes a penalty only if the individual has a reasonable expectation of privacy, and her body parts are captured surreptitiously, so the first element is met.[144] The second element is incorporated into the Act, too, because the Act prohibits only recordings that are made with the *intent* to capture an image of private areas. If a hidden surveillance camera, installed for the purposes of security, were to capture an image of a female breast when a gust of wind flips up a shirt, this

---

to videotape public officers performing their public duties, but the constitutional right was constrained to situations in which the recordings are made with an "expressive purpose." Robinson v. Fetterman, 378 F.Supp.2d 534 (E.D. PA 2005). The Third Circuit declined to follow *Robinson* when a recording was made during a traffic stop because these stops are inherently dangerous for police, and because the recording was not clearly made for a political or expressive purpose. Kelly v. Borough of Carlisle, 622 F.3d 248 (3rd Cir. 2010). *See also* Pomykacz v. Borough of West Wildwood, 438 F.Supp.2d 504.

[142] Hamberger v. Eastman, 206 A.2d 239 (N.H. 1965).

[143] *See*, *e.g.,* Video Voyeurism Prevention Act, 18 U.S.C. § 1801; ALA. CODE § 13A-11-32; FLA. STAT. ANN. § 810.145.

[144] Video Voyeurism Prevention Act, 18 U.S.C. §1801.

capture would not violate the Act. Footage created for the purpose of security provides significant utility, even if it also incidentally captures the occasional private part. Images intentionally capturing private areas do not tend to add significant social value.[145]

Before the era of rapid data growth, observation took place before, or concurrent with, capture. Sally Mann observed her family through the lens of her camera just before she captured them.[146] And Linda Tripp recorded her conversation with Monica Lewinsky as they were having it.[147] Today, information capture is a ubiquitous and unavoidable part of ordinary modern life. The geo-location data created and transmitted by our cell phones, the routing information logged by our Internet service providers, and even the data generated by our hotel doors[148], are part of the data exhaust we produce simply by going about our business. While it might seem convenient to consider all acts of capture to be acts of observation as well, doing so would severely shrink the scope of seclusion. The reason is a bit counterintuitive: if we consider all captures of data to be observations, then we would have to expect, and consent to, the observation of our data anytime we use a technology that must produce a data trail to function properly. This would eliminate any possible expectations we might have in seclusion to that data.

A critical insight for our purposes is that, except in the rare instances described above, it is *observation*, and not capture, that is at the heart of an intrusion. By recognizing that intrusion protects us from excessive and overzealous observations, we can distinguish between innocuous data capture and inappropriate, focused investigation. This permits courts to expand the intrusion tort amid the data exhaust.

---

[145] The tort of public disclosure of private facts has been used to effect a limitation at the point of capture when a momentary accidental nudity was captured without consent. Daily Times Democrat v. Graham, 162 So. 2d 474 (Ala. 1964). *But see* McNamara v. Freedom Newspapers, Inc., 802 S.W.2d 901 (Tex. 1991) (finding that the First Amendment provided immunity to a newspaper that published a photograph of a high school soccer player whose genitalia were accidentally exposed.) Apparently the exposure of nude body parts is the key to recovery. Other embarrassing moments outside the plaintiff's control tend to lose protection. *See* Borton v. Unisys Corp., 1991 WL 915 (E.D. Penn. 1991) (where a photograph taken while an employee cupped his hands over another employee's breast without consent was not depicting anything sufficiently "private" because none of the crucial body parts were exposed).

[146] Lyle Rexer, *Marriage Under Glass: Intimate Exposures*, N.Y. TIMES, November 19, 2000.

[147] Ian Ayres, *Why Prosecute Linda Tripp?*, N.Y. TIMES, August 10, 1999.

[148] Hotel door data was expected to play a role in the rape prosecution of Dominique Strauss-Kahn, the chief of the International Monetary Fund. Angelique Chrisafis & Ed Pilkington, *Consent Is Strauss-Kahn's Likely Defence, But the Battle Will Be Ugly*, GUARDIAN, May 18, 2011.

IV. THE NEW INTRUSION

In 2000, as privacy scholars began to convene, anticipate, and collectively fret over the mounting privacy troubles in the age of the Internet, Michael Froomkin suggested that the community might have to consider whether modern data collection practices "constitute an invasive tort of some type."[149] He recognized that, if privacy law can address invasive collection techniques, that will relieve the need for regulation to address problems downstream.[150] This Part takes up Froomkin's challenge. It will show how the intrusion tort can be clarified and modernized to tackle the most troubling data collection practices.[151]

A. Ubiquitous Data Exhaust

Recall the fictional General Motors spy from the Introduction who followed Ralph Nader down every aisle of a store, taking note of every product he examined or put, temporarily, into his cart, somehow managing to collect all this information without being detected.[152] This crudely describes the type of information collected by Web tracking technologies like cookies and Web bugs. Websites are not particularly unique in this regard; nearly all of machines and gadgets produce data about their users

[149] A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1536. Froomkin did not believe that existing tort laws including intrusion upon seclusion could be expanded to meet privacy demands such as closed circuit television monitoring because the tort traditionally excluded any surveillance or observations performed in public spaces. *Id*. He also believed expansion of the tort into public spaces would directly conflict with the First Amendment, but the tort is in fact in less tension with the right to free speech and access to information than the other reforms Froomkin considers. However, Froomkin and I are in agreement that the creation of records in the course of a business transaction is immune from tort liability, and therefore put limits on the aggressiveness with which the intrusion tort may defend and define privacy rights.

[150] *Id.* at 1543.

[151] For a more detailed description of the technology, *see In re* DoubleClick Privacy Litigation, 154 F.Supp.2d 497, 503 (S.D.N.Y. 2001).

[152] One military court opinion suggests that people cannot have a subjective expectation of privacy in data files that they do not know exist. "The military judge concluded the appellant had no expectation of privacy in the contents of the computer. We find no abuse of discretion in his ruling. There is no evidence the appellant was aware the Internet history files existed, and we are unconvinced the appellant could entertain a subjective expectation of privacy in them without such knowledge." U.S. v. Larson, 64 M.J. 559, 563 (A.F. Ct. Crim. App. 2006). This poor reasoning is probably an example of bad facts making bad law. Since the defendant was sanctioned for soliciting sex from somebody he believed to be a fourteen-year-old (but was in fact a law enforcement officer), the court was motivated to make every determination against him.

for some functional purpose. But since web tracking incorporates most of the issues that arise from other forms of data exhaust, an understanding of intrusion's application to website data provides an instructive template.

Suppose Arthur visits the website pandora.com for the first time. Pandora streams music based on bands that Arthur identifies as "seeds". Arthur is able to listen to the customized radio station and create an account for free; Pandora's business model relies on advertising, which is serviced by DoubleClick (now a subsidiary of Google.)[153]

When Arthur types pandora.com into his browser, his computer sends packets of data through the network of networks that constitutes the Internet until the packets reach their destination—Pandora's servers. Pandora's servers reconstruct the packets into the request message (essentially, "I want to see your home page.")

Pandora automatically sends a response to Arthur's computer containing three elements. First, the response includes the HTML or Javascript code and other files like JPEGs of pictures so that Arthur's computer can build and display the webpage. Now, Arthur's computer will have everything he needs to view the page except for the advertisements. Second, the response includes cookies and, perhaps, action tags or Web bugs, which are additional files stored on Arthur's computer that keep track of his online activities. Third, the response includes an IP address link that directs Arthur's computer to communicate with DoubleClick's server so DoubleClick can send the files needed to fill in the ad space. When that happens, DoubleClick places its own cookie on Arthur's computer, if he does not already have a DoubleClick cookie. (He probably does, in which case the IP address link would also contain his unique DoubleClick cookie ID and the existing profile information from his DoubleClick cookie.) DoubleClick will then send a targeted ad to Arthur.

The cookies—both Pandora's and DoubleClick's—record limited categories of information. They can record content that Arthur typed into his browser to transmit to Pandora—his name and password, and the names of the bands he typed in to seed his radio station. Cookies can store any content that is communicated between the user and the website, so if a user has provided their name, e-mail address, search terms, or credit card information to the website they are visiting, the website's cookie and the cookies of its third party intermediary advertisers may log the information. Cookies also store location information about the pages Arthur visited within the Pandora website. This may be of limited interest in the context of an online radio station website, but location information is more consequential when one considers a cookie for WebMD (and the cookies of its third party advertising affiliates.) WebMD might record that Arthur's

[153] Matthew Lasar, *The Perils of Being Pandora*, ARS TECHNICA, *available at* http://arstechnica.com/media/news/2011/02/the-perils-of-pandora.ars (Feb. 15, 2011).

computer visited the site's gonorrhea page. Action tags (also known as "Web bugs" or "clear gifs") work with cookies to record even more particularized information, such as the user's mouse movements across the website, and keystrokes that were entered into fields on the webpage but never actually sent (because the user deleted the content or decided not to submit the information.) The action tag is loaded directly onto the HTML page as the user views it, though it is not visible, and it writes the keystroke and mouse movement details onto the user's cookie.[154]

The creators of Web browsers (like Microsoft's Explorer, Mozilla's Firefox, and Google's Chrome) implement a number of industry standards developed by the Internet Engineering Task Force. The standards are referred to as Requests for Comments ("RFCs") to show the Task Force's commitment to consensus, adaptation, and non-stasis. The RFCs specify that information recorded on one party's cookie must be encrypted, cannot be observed by others, and must not contain malicious code (designed to inspect or tamper with the computer user's files.) Though the RFCs are technically industry self-regulation and, in theory, a new browser could ignore the standards, the RFCs have the force of network effects. If a browser does not implement one or more of the RFCs, it could have compatibility problems with other servers and users on the Internet and fail to function properly. Some of the RFCs are also supported by public law. If a third-party website or entity attempted to access a cookie without the authorization of the computer user or the website that placed the cookie, this act would presumably violate the Stored Communications Act.[155] And if a cookie was programmed with malicious code designed to vandalize the computer user's files, the cookie would violate the Computer Fraud and Abuse Act.[156]

While cookies are capable of capturing granular detail about computer users, the details are often accessed to improve visitors' experiences. These are benefits Web users have come to expect. For example, the cookie can store the Arthur's login information and password, and it can recall which pages on the site Arthur has viewed so that the hyperlinks appear in a different color. Even mouse and keylogging data can be aggregated across a sites' users and analyzed to assess whether the information architecture of the site is causing confusion or inefficiency.

---

[154] For a description of current cookie-setting practices, *see* Chris Jay Hoofnagle et al., *Can Advertisers Learn That "No Means No"?*, BNA Privacy & Security Law Report (2011).

[155] The computer user and the website (or its advertising intermediaries) are "users" under the Electronic Communications Privacy Act, and the communications recorded by the cookies are covered communications; thus, accessing the cookies without consent would be an offense under 18 U.S.C. § 2701(a). *In Re* DoubleClick Privacy Litigation, 154 F.Supp.2d at 507-509.

[156] The Computer Fraud and Abuse Act outlaws the intentional access of information and causing damage to an end user's computer. 18 U.S.C. §§ 130(a)(5)(B)&(C), 1030(a)(2)(C).

The cookies of third party intermediaries like DoubleClick cannot claim to have the same aim of helping the user's experience, and they record the same types of details. Moreover, they capture data during the interactions the user has with *all* of the intermediary's affiliated websites. Thus, DoubleClick's cookie has far more information about Arthur than Pandora's cookie. DoubleClick has all of the information on Pandora's cookie, as well as all the information on Toys R Us's cookie, as well as all the information on the New York Times' cookie, and so forth. A quick session of websurfing could increase the detail in the DoubleClick cookies significantly because of DoubleClick's aggregation of market power. Neil Richards has characterized these "uber-databases" as inherently problematic.[157] The vast scale differences between what was once known about people and what can be known about them today is also at the heart of Paul Ohm's critique of the accretion of information in our personal "databases of ruin."[158] But it is not analytically rigorous to say that a difference in scale is a difference in kind. Without a coherent theory of harm, accretion is merely a description of the information ecosystem we live in today and not, necessarily, a threat.

Offensive observations, on the other hand, are fully realized privacy harms as soon as they occur. A legal challenge that focuses on these harms has the most likelihood of success.

B. Failed Attempts

So far, every legal challenge to Web tracking has tried to force-fit the facts into federal statutory schemes that were designed to prevent something else.[159] Attempts to recover using the Computer Fraud and Abuse Act ("CFAA") falter on the $5000 damages and economic loss requirement—a threshold chosen by Congress to ensure that only the most malicious incidents of hacking are ensnared by federal criminal and civil liability.[160] Challenges based on the Wiretap Act fail because the website tracking the user is a party to the communication. Even the website's third party intermediaries, such as DoubleClick, fall outside the scope of the Wiretap Act because of the one-party consent rule; so long as one party to the conversation consents to a recording or interception, the statute's

[157] Richards, *supra* note 12.
[158] Ohm, *supra* note 96.
[159] Valdez v. Quantcast Corporation, CV10-05484 (Cal. 2010); Chance v. Avenue A, 165 F.Supp.2d 1153 (W.D. Wash. 2001); *In re* DoubleClick Privacy Litigation, 154 F.Supp.2d 497; *In Re* Pharmatrak, Inc. Privacy Litigation, 329 F.3d 9 (1st Cir. 2003).
[160] Chance v. Avenue A, 165 F.Supp.2d at 1160; *In re* DoubleClick Privacy Litigation, 154 F.Supp.2d at 522.

prohibitions do not apply.[161] Since Pandora authorizes DoubleClick to access its communications with Arthur, DoubleClick's data capture has the same legal consequences that Pandora's does.[162]

The plaintiffs' bar has not made a serious attempt to deter Web tracking through tort law. State causes of action were alleged in major Web tracking cases like *In re DoubleClick* and *Avenue A*, but after the federal courts dismissed the statutory claims and withdrew ancillary jurisdiction over the state claims, settlements were worked out quickly.[163] The state claims were never fully litigated—probably a reflection of the trial lawyers' confidence in the likelihood of winning based on a novel interpretation of privacy torts. Recent lawsuits against Google, Clearspring Technologies and Disney that challenge the use of flash cookies and respawning cookies attempt to use the same ill-fitting federal statutes rejected in DoubleClick and Pharmatrak, and will probably duplicate their fate.[164]

With a careful understanding of the intrusion tort, and the interests it is meant to protect, state courts are in the best position to address the perils of Web tracking. Courts can identify circumstances in which we should be able to expect seclusion while surfing the World Wide Web, even if the Web is considered to be public. Next, the Article describes how they should do so.

C. A New Intrusion

The intrusion tort is applicable to many contexts, but we will continue to use web tracking to explore its form and function, making only

---

[161] The Stored Communications Act exempts interceptions that are authorized "(1) by the person or entity providing a wire or electronic communications service; [or] (2) by a user of that service with respect to a communication of or intended for that user." 18 U.S.C. 2701(c). The Wiretap Act states "It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception." 18 U.S.C. 2511(2)(d); United States v. Caceres, 440 U.S. 741, 750 (1979) (confirming the statute adopts the one-party consent rule.) The Wiretap Act does outlaw interceptions that are made for a tortious purpose, regardless of whether a party has consented to the interception, but courts have distinguished between tortious *purposes* and tortious *means*. The interception cannot be the basis for relief under the "tortious purpose" clause. Sussman v. ABC, 186 F.3d 1200, 1202-03 (9th Cir. 1999).

[162] Chance v. Avenue A, 165 F.Supp.2d at 1161; *In re* DoubleClick Privacy Litigation, 154 F.Supp.2d at 510, 519.

[163] Chance v. Avenue A, 165 F.Supp.2d at 1163.

[164] Greg Sandoval, *Suit Alleges Disney, Other Top Sites Spied on Users*, CNET, August 14, 2010, *at* http://news.cnet.com/8301-31001_3-20013672-261.html; *Christopher Sheean on the Latest Google Class Action,* POINT OF LAW, December 8, 2010, *at* http://www.pointoflaw.com/archives/2010/12/chris-sheean-on.php

the occasional detour to consider how the tort could work with GPS data, security footage, and other personal data.

1. The Elements

Intrusion can benefit from some conceptual clarification before it is applied to new contexts. Even in real space, intrusion has only two aspects to its design: there must be an observation, and that observation must be highly offensive to a reasonable person.[165]

A new restatement of the tort might look something like this:

> *One who intentionally observes another is subject to liability to the other if the observation would be highly offensive to a reasonable person.*

As in real space, not every observation is offensive. Information that is voluntarily shared with an individual or the public can be observed without offense by that individual, in the case of the former, and by any individual in the case of the latter. The offensiveness element winds up turning on whether the observed could have and should have expected their information to be exposed to the observer. If a piece of information was not voluntarily exposed, liability will attach to any observation.

Identifying an "observation" is a surprisingly difficult and uncharted task. Recall that the creation and capture of data does not, on its own, mean that observation has taken place. In the classic intrusion cases, one human being observed another when they shouldn't have. Today many challenging privacy problems have little to no human involvement.

An observation requires personal information to be recognized in some meaningful way. If a human being reads a line of data about somebody and comprehends its context, knowing whom the data is describing, then the data is "observed." But we should not limit the definition of observation to events involving human cognition. Algorithmic

---

[165] This is a collapsed version of the Second Restatement definition of intrusion upon seclusion. The Restatement defines the tort as so:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

RESTATEMENT (2D) TORTS §652B. Here, the observation event incorporates the intentionality and the intrusion elements, and the requirement that the observation event be offensive incorporates both the "offensiveness" element as well as considering whether the plaintiff had "seclusion" in the first place.

and automated processes can violate a sense of seclusion, too. Suppose, for example, the website WebMD collects the IP addresses of Web users who visit its page on depression, and automatically submits them to a reverse-lookup service to obtain names and mailing addresses. Next, the WebMD program automatically transmits the names and mailing addresses to a business affiliate which, without allowing any employee to open the file, uses the data to fill out a form letter reading "Dear Mr. Smith, I understand you have been coping with depression. Our offices are here to help…" Business practices are increasingly automated. While human recognition is sufficient to create an observation, it is not necessary.[166] Thus, we must determine for the first time what constitutes machine observation. The results map quite neatly onto the Fair Information Practices concept of purpose limitation.

The "offensiveness" and "observation" elements are explored in more detail below. We start with "offensiveness" because, although it might seem ancillary to the observation element, it actually provides a helpful prerequisite sorting mechanism. We need not worry about what it means to observe data if the data has been voluntarily exposed. The function of the right to seclusion, as Part II has described, is to hash out a compromise between an individual's interests in privacy and others' interests in information. The contours of our right to seclusion are determined by the "offensiveness" element. Observations penetrate that seclusion.

a. Offensive Observations of Unexposed Data

During the consideration of an intrusion claim, juries and lawmakers will have to decide whether the defendant's observation is sufficiently offensive to trigger liability. Put another way, the fact-finder must decide whether a computer user was justified in expecting seclusion.

Some observations have long been treated as per se inoffensive, and there is no reason to believe the case law should be reversed. Transaction data created in the course of a purchase, for example, is precisely the sort of information the user has willingly exposed to the entity in order to purchase goods or services.[167] Likewise, most communications of content made by a computer user in order to interact with a company are willing exposures.[168]

---

[166] Ryan Calo has stressed the importance of defining privacy without reference to a human observation. Calo, *supra* note 21.

[167] In re Northwest Airlines Privacy Litigation, 2004 WL 1278459 (D. Minn. 2004)("finding that the plaintiffs' intrusion claim failed because "in this instance, Plaintiffs voluntarily provided their personal information to Northwest."); Dwyer v. American Express Co., 652 N.E.2d 1351 (Ill. App. 1995) ("By using the American Express card, a cardholder is voluntarily, and necessarily, giving information to defendants").

[168] Searches within a site, while technically communications between the computer user and the website, might be treated differently from other types of communications. These

If Arthur tells Pandora that he wants to hear Astrud Gilberto, it would not strike ordinary jurors as offensive that Pandora knows, and remembers, that he requested Pandora to serve up bossa nova music. The analogy to the brick and mortar world is instructive. A skilled waiter remembers the preferences and ordering habits of regular customers. Since organizations routinely maintain business records, it is not particularly disconcerting that a company can access information voluntarily submitted by the user in the course of obvious interaction. For these types of transaction data, restrictions on future dissemination and use would have to be justified on some other ground.[169]

This is not to say that transaction data is a total free-for-all. A third party can still intrude on the transaction data if he has accessed the data without permission from either the user or the transaction company; a hacker is no different from the snoop who peeks at a person's medical records without permission from the patient or the health provider.[170] But the website itself can observe with impunity the transaction records it maintains.

What about the detailed web tracking data? Has a visitor voluntarily exposed the precise HTML pages accessed within the domain, or the search terms used to find a page within the domain, or the items browsed in an online store, or the movements of a user's mouse? Ultimately, the answers will require juries or lawmakers to forge a rule based on expectations that are reasonable in context. The specific expectations of a particular plaintiff are not determinative; after all, hidden security cameras are designed to thwart expectations of surveillance, but they are not, categorically, offensive when the observed is in a so-called public space.[171] The "public" is a social construction, but it is one on which intrusion law has rested.

A number of factors could persuade a fact-finder or rule-maker that web tracking cookie data has been exposed to the websites. The public might have a sophisticated understanding about the revenue models for free web content, or Americans might genuinely prefer tailored advertising. But it's plausible if not probable that rule-makers charged with the task of delineating the boundary between private and public spheres would agree that, without explicit consent, observations of detailed web tracking are overzealous and exploitative.

---

searches might be distinguished from transactions with the website because they are a means of orientation only, and not part of the quid pro quo of a purchase.

[169] Dissemination and use restrictions are discussed in the next Part. Uses of legitimately observed information that seem obnoxious, such as price discrimination or employment screens, can be prohibited through tailored use restrictions.

[170] *See* note 132 for intrusion cases based on unauthorized access to records.

[171] Cameras installed in a restroom, or used to take up-skirt photographs, would be another matter. *See* e.g. Speer v. Ohio Dept. Rehab. & Corr., 624 N.E.2d 251; Video Voyeurism Prevention Act, 18 U.S.C. §1801.

> ***Illustration 1***. *Carol purchases a book on Amazon. Amazon records the date and time of Carol's transaction, the items Carol purchased, and Carol's method of payment.* ***Carol's purchase information has been exposed.*** *Amazon's observation of this data cannot be offensive.*
>
> ***Illustration 2***. *Ben browses a few books on Amazon but decides not to purchase anything. Amazon records the identities of the products that Ben has browsed.* ***Ben's browsing information has not been exposed.*** *Amazon's observation of this data will be offensive.*

The approach set forward here aligns the definition of seclusion with the larger goals of privacy. Sometimes this comes at the cost of abstraction. It requires us to draw distinctions between actions that are not very different technologically. The distinction between data transmitted in the course of a purchase with Amazon and data transmitted when the visitor loads a page for nose hair trimmers makes little difference in terms of the HTTP messages exchanged between the user's computer and Amazon's servers, but the conceptual distinction is great.

The New Intrusion's non-technical approach to defining seclusion is more of a strength than a limitation. The Internet has caused doctrinal quagmires in other areas of the law—is content stored in a computer's Random Access Memory (RAM) considered a "copy" for the purposes of copyright infringement? And do the contents of e-mails, which technically are revealed to Internet service providers, fall within the third party doctrine exception to the Fourth Amendment? In both cases, the most recent, better reasoned approaches have treated RAM copies as something other than a "copy,"[172] and the body of an e-mail as private, unexposed "inside the envelope" information, even though these treatments are divorced from the technical realities. The New Intrusion can be similarly pragmatic. Because we are more interested in how the Web *seems* to work than how it actually works, judges and juries are in a good position to decide what sorts of seclusion we instinctively expect to have while browsing the web or using our gadgets.

Seclusion is only half the story. Nothing prevents a website from collecting unexposed tracking data; indeed, http code must be transmitted to a website in order to load a particular page; although the data privacy literature often refers to "data collection," this collection is more accurately a failure to expunge data. The motive for separating the concepts of

[172] Aaron Perzanowski, *Fixing RAM Copies*, 104 NW. U. L. REV. 1067 (2010).

observation and capture was to allow websites and technology to use captured data to function more efficiently. High functionality often requires automated processing of historical data. But a device-user who has not voluntarily exposed her data should be able to expect that her data will not be *observed*.

b. Observation in the Digital Age

What is an observation? When do we feel we are being studied? Human recognition of a person's data is a sufficient condition, but as the Web MD auto-generated letter example shows, it is not necessary one.

A natural starting point is to designate all data access as observation. While conceptually clean, this definition quickly leads to a dead end. Data is generated in the first place to be accessed for *some* purpose. A Web user's request to a website's server to deliver an HTML page must be accessed in order to deliver it. Likewise, an HTML page might use code that instructs a computer user's Web browser to access data on his cookie in order to display the page properly—e.g. to load the user's previously customized display. If this sort of access is determined to be an observation, there is no material distinction between observation and capture. To have any meaning at all, observation must be distinct from the data processing that is intrinsic to the browsing experience or functioning of a device. The next illustration provides an example outside the webtracking context.

> ***Illustration 3***. *Vicki's GPS device, manufactured and serviced by TomTom, automatically stores and analyzes Vicki's location data, and is programmed to periodically recalculate her estimated time of arrival based on the location logs.* ***TomTom has not observed Vicki's location data.***

Websites also access personal data in order to aggregate and analyze it for general trends. Analytics are used to build predictive models about a generalized population and to analyze and refine the functionality of a website. When poor information architecture leads a sizeable percentage of a website's visitors to click on the wrong link, the backtracking leaves an impression in the aggregated data.

There are cogent reasons to treat the pooling and processing of data as a non-observation, so long as the data is processed without overt reference to the data subject.[173] First, since the data is used without

[173] That is, processed without direct identifying information such as name, address, or full IP address. If the aggregated data is going to be shared for research purposes it will need to

reference to the data subject, to the extent there is observation at all it is of a fact unleashed from its generator, like footprints in the snow. If the anonymized data are related back to the original device-user at some later point, the analytic exemption would expire. But so long as data is used without interaction with, or knowledge of, the particular data subjects, the subjects have not been observed.[174]

Second, the vast new accumulations of data can be extremely useful for research purposes. We are only just beginning to understand their value of these grand new sources of information. Researchers at MIT, the London School of Economics, and Harvard have used cell phone data to track mental illness, political discourse, obesity, happiness, and stock market fluctuations.[175] And GPS data can be used to improve traffic planning and to monitor congestion in real time, so that drivers can avoid delays.[176] For these purposes—whether they are as mundane as improving a website or as

undergo additional scrubbing to ensure that reidentification of a subject is not too easy to do. *See* Ohm, *supra* note 96; Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J. L. & TECH. 1 (2011).

[174] Privacy advocates, the advertising industry, and the Federal Trade Commission are locked in debate over whether an IP address, or the information contained in a cookie, is "personally identifiable information." FEDERAL TRADE COMM., PRIVACY REPORT (2012). The New Intrusion sidesteps this debate because, once a party accesses a cookie in order to communicate or interact with the end user for a purpose collateral or in tension with the original purpose for which it was generated, it is irrelevant that the advertiser does not know the name of the user, or does not know them in a meaningful way. This is consistent with the goals that underlie the intrusion tort; since intrusion protects a person's seclusion from observation, it makes no difference whether a peeping tom actually *knows* the person he observes. It is the act of observing that violates the rights of the observed.

[175] Robert Lee Hotz, *The Really Smart Phone*, WALL ST. J., April 23, 2011.

[176] Thus far, GPS studies have relied on vehicles carrying GPS logging devices with the intent that the data would be analyzed by the municipality or city conducting the studies. But the studies are enormously useful for studying travel time and delays, for assessing the effects (in traffic time) of construction or route alterations, and for evaluating whether traffic signals are timed correctly. These types of studies could become inexpensive and widespread standard practices for all jurisdictions if researchers are able to access the log data of commercial GPS providers. *See* GeoStats, *at* http://www.geostats.com/product_trav.htm. However, aggregated data is used for law enforcement purposes, such as to help determine where to establish speed traps. Such use is often perceived as violating the privacy of the GPS device-users. Tim Stevens, *TomTom User Data Sold to Dutch Police, Used to Determine Ideal Locations for Speed Traps*, ENGADGET, April 27, 2011, *at* http://www.engadget.com/2011/04/27/tomtom-user-data-sold-to-danish-police-used-to-determine-ideal/. It is possible that the issue underlying the privacy concerns is that law enforcement might have the wrong motivation in establishing speed traps. Data-assisted speed traps might do more to increase revenues and citation rates than they do to improve traffic safety. In that case, a person might feel tricked for his or her unwitting contribution to the dataset that enabled the police to create the speed trap. There are categories of government data uses that can be carefully cabined or prohibited altogether through use restrictions, but the capture of anonymized GPS data is not inherently harmful.

profound as understanding the determinants of happiness—researchers do not care who is in the database and who is not. Statistical analysis strikes a very safe balance, enriching the accumulation of knowledge and the proverbial marketplace of ideas without posing risk of repercussion or misuse to the individuals described in the data. But the data has to be processed in order to anonymize and prepare the data for research use.[177] The New Intrusion can be aligned with societal interests by exempting processing from the definition of observation, much like the European Union exempts processing for statistical research from the purpose limitations of the Data Protection Directive.[178]

> ***Illustration 4.*** *Verizon pools together its subscribers' cell tower data to analyze which geographic areas require the construction of additional towers.* ***Verizon has not observed the subscribers' tower data.***

> ***Illustration 5****. Alexander regularly views television shows on Hulu. Hulu gathers viewer usage data and anonymizes it in preparation for release to researchers.* ***Hulu has not observed Alexander's televiewing habits.***

Having carved out the more obvious exceptions, the harder question remains: what *does* count as an algorithmic observation? It is worth reflecting for a moment on the objectives of the right to seclusion. Seclusion gives people the breathing space to be and to act without having to worry about social or economic consequences. Data accessed for some purpose that is different and inconsistent with the product or service for which the data was generated will generate many of the same justified anxieties over the dissemination and potential implications as an intrusive observation. The user can no longer feel alone with his device.

For unexposed data—data for which a user maintains a right to seclusion—the goals and designs of the Fair Information Practices are quite

---

[177] If an entity with access to personal data exhaust wishes to analyze it in aggregated form (and without any future reference back to the data subjects), it is sufficient to strip direct identifiers such as names, IP addresses, contact information, and credit card numbers. If the entity wishes to share the data for research purposes to third parties, the data will need to go through additional anonymization procedures, or must be disseminated only through restricted licensing agreements. *See* Yakowitz, *supra* note 173.

[178] "Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards." EU Data Protection Directive Article 6(1)(b). Note, though, that the required "safeguards" demand that the data pose no risk of reidentification—a standard that is impossible to meet, and forces data holders to choose between risking sanction or halting standard practices. EU Data Protection Directive Article 13(2).

apt. When the personal data is used or disclosed for some purpose inconsistent with its original collection without advance notice and consent, an observation has occurred. This definition of automated observation is nearly identical to the "respect for context" incorporated into President Obama's proposed Consumer Privacy Bill of Rights.[179]

Context, or "purpose," is not self-defining. At the very least it would include uses collateral to the service the user had accessed that have the potential to significantly disadvantage the user. The next illustrations provide examples of such uses.

> ***Illustration 6***. *Anthony visits Amazon.com in order to purchase a book after reading a review on a blog. Research shows that customers who linked into Amazon from another website reviewing a product are less likely to perform price comparisons before making a purchase. Amazon uses a pricing algorithm that automatically offers Anthony a price $1.00 higher than the standard price based on his link-in data.* ***Amazon has observed Anthony's link-in data.***
>
> ***Illustration 7***. *(Based on the same facts as Illustration 6.) Amazon uses link-in and web-tracking data to construct a creditworthiness index.* ***Amazon has observed Anthony's link-in and web-tracking data.***
>
> ***Illustration 8***. *(Based on the same facts as Illustration 6.) Amazon discloses the link-in and web-tracking data to a third party data aggregator that uses the data to construct, among other things, interest profiles and employability indices.* ***Amazon has observed Anthony's link-in and web-tracking data.***

The New Intrusion framework intersects with Fourth Amendment law in at least one important way. The expansive third party doctrine, which allows law enforcement officers to access business records without obtaining a warrant, is premised on the assumption that business records contain information that the suspect "voluntarily turns over to third

[179] "Respect for Context" is defined as so: "Consumers have a right to expect that organizations will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data." OFFICE OF THE PRESS SECRETARY, ADMINISTRATION UNVEILS BLUEPRINT FOR THE 'PRIVACY BILL OF RIGHTS' TO PROTECT CONSUMERS ONLINE (February 23, 2012).

parties."[180] Personal data that has not been exposed, and which cannot be observed by a company without triggering intrusion liability, has no logical place in the third party doctrine exception to the search warrant requirement.[181]

Less obvious, however, is the New Intrusion's implication on behavioral advertising. Given the current, dominant business model for the most popular web services and online content providers, advertising is arguably intrinsic to the purposes for which web tracking data is created. If the raison d'etre for Facebook, Hulu, Google, and other popular websites is to attract visitors by creative (and expensive) content in exchange for the display of advertising, advertising is a key, obvious component of the web service. Along this line of reasoning, use of data to facilitate advertising would not be inconsistent with the purpose for which the data was created in the first place. This may be especially defensible in cases like gmail targeted advertising, where the scanning of the body of one's email, and the prominent display of all the free storage and service provision the user gets in exchange for the advertising program, provides clear visceral notice of Google's practice of scanning contents to deliver ads.[182]

On the other hand, tracking practices extend well outside a user's experience with each particular website because of the frequent use of third party cookies. A user's visit to website A on day one is arguably wholly unrelated to the advertisement he is served on website B on day 30. There is no definitive classification for behavioral marketing as an observation. Much will depend on whether one views advertising as the Internet's backbone or as its parasite. [183]

---

[180] Smith v. Maryland, 442 U.S. 735, 744 (1979).

[181] The more lenient warrant requirements adopted in the Stored Communications Act that apply to routing data do not require probable cause. 18 U.S.C. 2703(d). If web-tracking data is "unexposed" and deserving of full Fourth Amendment protection, the procedural protections of the SCA will not be constitutionally sufficient.

[182] For a description of visceral notice, *see* M. Ryan Calo, *Against Notice Skepticism,* 87 NOTRE DAME L. REV. __ (2012).

[183] I do not wish to speculate about social norms with respect to behavioral advertising since the empirical evidence is so mixed. Survey after survey confirms that, considered in isolation, Americans want to surf the Internet without creating a record of their transactions and activities. One study reports that 92% of Americans believe there should be a law requiring "websites and advertising companies to delete all stored information about an individual, if requested to do so." Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities that Enable It* (2009) (available at http://ssrn.com/abstract=1478214). *See also* A. M. McDonald and L. F. Cranor, *Americans' Attitudes About Internet Behavioral Advertising Practices*, WORKSHOP ON PRIVACY IN THE ELECTRONIC SOCIETY 63 (2010) (E. Al-Shaer & K. B. Frikken, eds.); Karl W. Lendenmann, *Consumer Perspectives on Online Advertising- 2010*, PreferenceCentral Benchmark Research Study (2010). However, these studies repeat a flaw that undermines the credibility of the findings: they do not ask respondents whether they would prefer an alternative reality where the same online content contains about twice the amount of (non-

2. Consent

Intrusion rules can always be modified through private agreements. Today private industry places considerable faith in their privacy policies and End User Licensing Agreements ("EULAs") to define the scope of their duties. Boilerplate formalities of this sort might suffice to limit the scope of contract liability, but they are not sufficient to constitute consent to conduct that would otherwise be tortious. Consent is not assent. Consent requires acts that manifest an objective expectation that the would-be tort victim is willing for the tortious conduct to occur.[184] Qualitative research conducted by Chris Hoofnagle and Jennifer King indicates that web users rarely have actual notice of a website's policies; in fact, the mere existence of a privacy policy prompts web users to assume, inaccurately, that the website promises not to re-use or share its transaction data.[185] Notices and agreements that expand the scope of observation beyond what courts would otherwise consider to be appropriate leave open a number of important questions. Are there circumstances in which the courts should demand heightened forms of notice for intrusive observations?[186] Are there circumstances in which, for public policy reasons, courts should not recognize consent at all?[187] This

---

targeted) advertising, or where they pay for content. The handful of studies that do force survey respondents to state their preferences in the context of privacy tradeoffs find that a majority of Internet-users prefer free content with targeted ads over other types of privacy-protecting options like pay walls or increased quantity of advertising, though some of these studies too have methodological flaws. Pew Internet Project, Lendenmann, *supra* note__ at 11 (note that the phrasing of the question, and the ordering of the answer options, are objectionable. The survey does not offer respondents the option to view the same content with *more* advertising; the closest is an option for "somewhat limited online information or less functional services.") *See also* D. Hallerman, *Behavioral Targeting Attitudes,* EMARKETER (2008) (finding that 55% of respondents are "very" or "somewhat" comfortable with behavioral advertising); Jacqui Cheng, *53% of Mobile Users Happy to Hand Over Location Data For Discounts*, ARS TECHNICA, August 17, 2011.

[184] Mansfield, *Informed Choice in the Law of Torts*, 22 LA. L. REV. 17, 31 (1961) ("Consent is the right term to use when the plaintiff was willing that a certain event occur, probably some conduct on the part of the defendant, because he desired an invasion of a normally protected interest."); Litman, *supra* note at 1311. However, in light of the recent Supreme Court holding in *Concepcion*, websites might enjoy de facto immunity from intrusion claims by requiring all visitors to arbitrate their claims individually. AT&T Mobility LLC v. Concepcion, 131 S.Ct. 1740 (2011).

[185] Chris Hoofnagle & Jennifer King, *What Californians Understand About Privacy Online*, at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1262130.

[186] Groundwork for these questions has already been laid by Andrea Matwyshyn. Andrea Matwyshyn, *Technoconsen(t)sus*, 85 WASH. U. L. REV. 529 (2008).

[187] For example, should job applicants be able to consent to observed urinalysis drug testing when applying for jobs for which drug use is not particularly predictive of incompetent or unsafe performance?

Article reserves for future research consideration of what form of notice is sufficient to convert an intentional tort into a consented activity.[188]

However, standard privacy policies and user agreements may interact with New Intrusion liability. When an entity makes promises that data will not be tracked or maintained, these promises can define the contours of a user's objectively reasonable expectations of seclusion. Thus, if a website observes data that it claims is not even being captured, the observation will violate an expectation of seclusion created by the website itself.[189]

In the past, lawsuits alleging that a website violates its own privacy policies have proceeded under contract theory. Because the resulting contract damages are speculative the lawsuits have been unsuccessful.[190] A claim for intentional intrusion upon seclusion could better deter privacy policy gaming because plaintiffs would have access to tort damages based on emotional distress and punitive damages, or even nominal damages multiplied by large numbers of class members.[191]

3. The Gap Between Tort Theory and Application

A primary goal of tort law—and especially the law of intentional torts—is to deter socially repugnant behavior. Since privacy claims are based on psychic harms and emotional distress, compensatory damages and even exemplary damages rely on evidence that distress has, indeed, occurred.[192] In theory, courts should allow juries to compensate plaintiffs generously based on any credible evidence of distress in order to supply the basis for punitive damages, and in order to effect deterrence. Far from being an amorphous approach to the law, compensation for emotional distress in

---

[188] Christine Jolls has begun this very inquiry. Christine Jolls, *Rationality and Consent in Privacy Law*, available at http://www.law.yale.edu/faculty/CJolls.htm.

[189] For example, the privacy policy for AudienceScience claims that the site will replace any cookie of a user who opts out of information-collection with a new cookie instructing the website to stop collecting information. What *actually* happens, according to Stanford researchers, is that AudienceScience keeps a highly unique cookie in place that tracks the user's interests, and continues to add information to this interest cookie. Jonathan Mayer, *Tracking the Trackers: Early Results,* STAN. CENTER FOR INTERNET & SOC., at http://cyberlaw.stanford.edu/node/6694.

[190] *In re* JetBlue Airways Corp. Privacy Litigation, 379 F.Supp.2d 299 (E.D.N.Y. 2005); Dyer v. Northwest Airlines Corps., 334 F.Supp.2d 1196 (D. N.D. 2004).

[191] In the context of trespass, which has a number of theoretical similarities to intrusion, courts have allowed plaintiffs to recover punitive damages even though the plaintiff suffered only nominal damage from the trespassing act. *See* Feld v. Feld, Civ. No. 08-1557, 2011 WL 1792783 (D.D.C. May 8, 2011).

[192] Alternatively, even nominal damage spread over a large enough class—such as the class of Californians with DoubleClick cookies on their computers—would expose web trackers to significant liability.

instances of intentional offensive behavior is soundly within the canonical law and economics vision of tort law. The harms, though they are noneconomic and difficult to count, easily outweigh the negligible benefits of the intentional offensive conduct. But many scholars have noted judges' skepticism when overseeing cases based on psychic injuries.[193] This Article does not attempt to explore or resolve the gap between tort theory and its application in the courtroom, but the hesitancy of the plaintiffs' bar to bring novel privacy cases, and the jurists to allow them to proceed to the jury, must be acknowledged.

However, there are reasons to be guardedly optimistic that courts might embrace the New Intrusion as a conservative response to a mounting problem. Intrusion liability rules will create much-needed clarity of law and policy, allowing businesses to use cookies without risk so long as they stay within the bounds of per se objectively reasonable observation. Companies would not have to provide opt-out procedures or a "do not track" cookie, though they might choose to do so to respond to market pressures.[194] Intrusion law would put an end to many problematic practices without forcing online businesses to significantly alter their websites, and without undermining the revenue model that currently supports much of the free online content. The intrusion approach is also readily enforceable because, by definition, the tort applies only to offensive behavior. Thus intrusion avoids the problems facing European privacy enforcement agencies, which are forced to choose between ignoring blatant violations of the EU cookies laws by nearly every website (including those of most EU governments) or cracking down arbitrarily.[195] Finally, if the common law can deter offensive observation of personal data, lawmakers will not have to consider restricting downstream dissemination and use of data which, for reasons articulated in the next Part, will be more difficult.

---

[193] Citron, *supra* note 44 at 1809; Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373, 393 (2009).

[194] A new firm called Evidon is offering the behavioral marketing industry's first "assurance platform." It organizes industry best practices that would, if followed, receive Evidon's trusted seal of approval. *Turn Names Evidon Preferred Provider of Compliance Services*, PRWEB, May 4, 2011, *at* http://www.prweb.com/releases/prweb2011/5/prweb8377655.htm.

[195] Mike Butcher, *Stupid EU Cookie Law Will Hand the Advantage to the US, Kill Our Startups Stone Dead*, TECHCRUNCH EUROPE, March 9, 2011, *at* http://eu.techcrunch.com/2011/03/09/stupid-eu-cookie-law-will-hand-the-advantage-to-the-us-kill-our-startups-stone-dead/. The European cookie law would require any website that uses Google Analytics to keep track of the number of visitors to a website, who would also have to comply with the opt-in consent requirements. *See also* the discussion in note 18.

V. PRIVACY AFTER OBSERVATION: DISSEMINATION AND USE

Once information is collected through legitimate means, policymakers face an uphill climb to justify the regulation of its dissemination. Laws restricting the disclosure or reuse of truthful, legitimately observed information proceed on the counterintuitive theory that having more facts is bad for society. However, there are times when the spread of information does cause great, avoidable harm, and laws deterring the spread of truthful facts can be the best course in these instances. Again, tort law has already laid much of the foundation for sensible restrictions on dissemination.

This Part begins by considering the nature of harms that flow from the dissemination of information that was lawfully observed and collected. The subsections that follow describe workable dissemination restrictions on two categories of information: information revealed in the context of a special relationship, and information that is "predictably explosive." These categories roughly map onto the common law torts of breach of confidentiality and public disclosure of private facts. These categories are not meant to be exhaustive; there may very well be other types of dissemination restrictions that tend to promote social welfare. But by analyzing confidentiality and public disclosure laws, it will become apparent that restricting the dissemination of truthful information is sound public policy only in a limited number of contexts. This part ends with a case study on dissemination and use regulations from the credit reporting context.

A. Conceptions of Harm

Some of the losses routinely identified as "harm" do not look like redressable injuries after sober reflection. This is particularly true for reputation-related injuries. Since harm, and risk of harm, are necessary prerequisites for tort liability, these infirmities are important and merit explication.

1. Reputation Damage

Reputational harm and shame are among the most commonly cited privacy harms.[196] The information age has undeniably increased the availability of reputation-damaging content. In his book *Delete*, Viktor Mayer-Schoenberger argues that the vast collections of digital information

[196] JEFFREY ROSEN, THE UNWANTED GAZE (2000); DANIEL SOLOVE, THE FUTURE OF REPUTATION (2007); Murphy, *supra* note 50 at 2385; Jacqueline D. Lipton, *Mapping Online Privacy*, 104 NW. U. L. REV. 477, 503 (2010).

keep us from forgetting the embarrassing things we've done.[197] Websites that catalog mug shots[198] or highlight moments of embarrassment[199] deny us the comfort we once had that our mistakes and failings would evaporate from collective memory. This new state of affairs has motivated the European Union to define a right to be forgotten, requiring websites to destroy any personal information at the request of the subject.[200]

Privacy scholars are puzzled that shame and reputational harms are only reluctantly, if ever, vindicated by U.S. courts.[201] Jacqueline Lipton speculates that lawmakers may fear chilling truthful speech, and that individuals who have suffered shame and humiliation are unlikely to demand legal redress, since the process would put their facts in the spotlight once again.[202] Danielle Citron argues that courts should be more likely than ever to recognize reputational injuries since the Internet creates a permanent, searchable record of embarrassing personal facts.[203] But shame, while undoubtedly unpleasant to the person feeling it, is not always socially undesirable.[204]

2. Harm Versus Consequence

Reputational damage is usually either a collateral consequence of past behavior (as when a bad credit history prevents a person from obtaining a loan[205]) or the accidental loss produced by an otherwise

---

[197] VIKTOR MAYER-SCHOENBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE (2009).

[198] David Kravets, *Mug-Shot Industry Will Dig Up Your Past, Charge You to Bury It Again*, WIRED, August 2, 2011, *at* http://www.wired.com/threatlevel/2011/08/mugshots/.

[199] *Sex List Rating Female University Student's Lovers Becomes Internet Sensation*, DAILY MAIL, October 8, 2010.

[200] Matt Warman, *Online Right "To Be Forgotten" Confirmed by EU*, THE TELEGRAPH, March 17, 2011, at http://www.telegraph.co.uk/technology/internet/8388033/Online-right-to-be-forgotten-confirmed-by-EU.html.

[201] Lipton, *supra* note 54 at 504; Citron, *supra* note 44 at 1808.

[202] Lipton, *supra* note 37 at 504.

[203] Citron, *supra* note 44 at 1808, 1810. Citron's argument makes real sense if the Internet allows a large number of micro-invasions to add up to real, actionable psychic costs. The question, though, is whether each revelation of embarrassing information is a small harm, too trivial to be redressable on its own but adding up to a real psychic harm due to repetition over the Internet (a summation of epsilons), or whether instead each revelation is not a legal harm at all (a summation of zeroes).

[204] *But see* Laura A. Heymann, *The Law of Reputation and the Interest of the Audience*, 52 BOSTON COL. L. REV. 1341 (2011) (arguing that legal frameworks for reputational interests must account for the public's interest in access to the information).

[205] Bad credit histories are a surprising mainstay among privacy scholars' examples of privacy harm. *See* Citron, *supra* note 44 at 1814 (coding a client's decision not to work with somebody in debt as a "privacy invasion"); Lori Andrews, *Facebook Is Using You*, N.Y. TIMES, February 4, 2012.

functioning system (as when a person's story is used as a cautionary tale.) Take, for example, the woman who is known worldwide as Dog Poop Girl after she rebuffed the pleas of her fellow subway-riders to pick up after her dog, which had just made a deposit in the subway car.[206] If her fellow passengers had called her selfish and entitled, the insults, while stinging, could not possibly require redress. The insults would not be "harm" at all, at least not in the sense that we use that term colloquially.[207] They burden her, but they are the natural social consequence of her actions.

What happened instead was slightly different. Dog Poop Girl became the target of a shaming campaign. Koreans pored over the pictures of the incident posted on the Internet via cell phone camera. Soon her identity, place of employment, and family members' names were attached to the story. She left her job in humiliation, and for the rest of her life, searching Google for her real name will reveal her epithet.

Dog Poop Girl's story is a sad one. Despite her transgression, she did not deserve to bear the full brunt of the world's contempt for litterers. This, however, does not make her loss a compensable one.[208] Stories like hers feed the engine of cultural norm-making, and as unfortunate as the damage might be for her, the deterrent effect on incivility and inconsiderate behavior will outweigh that damage. Dog Poop Girl was the unlucky victim in a properly functioning system. Though her penalty was out of proportion to her fault, she could have avoided it by picking up after her dog. She was the cheapest cost avoider, and so her aberrational penalty is equivalent to the tort defendant who is liable for the full costs of an eggshell plaintiff's injury.[209]

This system, callous as it is, is superior to the alternatives. A generic right to be forgotten allows an information subject to insist that existing, truthful information about her must be destroyed. Such a right imposes

---

[206] Jonathan Krim, *Subway Fracas Escalates Into Test of the Internet's Power to Shame*, WASH. POST, July 7, 2005, *at* http://www.washingtonpost.com/wp-dyn/content/article/2005/07/06/AR2005070601953.html. *See also* DANIEL SOLOVE, THE FUTURE OF REPUTATION 1-2 (2007).

[207] For strict utilitarians, the disapprobation would be harm. It would count against Dog Poop Girl's utility in the overall calculation of social welfare. But her decrease in utility is easily overcome by the deterrent effect that shaming and social norms have on litterers and dog-owners, by the avoidance of the sizable cost that would be imposed on the subway passengers if they were constrained from expressing their opinions, and by the justice and satisfaction the subway passengers would get from retribution. KAPLOW & SHAVELL, *supra* note 80 at 12, 18-19.

[208] Privacy scholars have argued that Dog Poop Girl deserves legal recourse. *See* Lipton, *supra* note 21 at 511.

[209] Vosburg v. Putney, 80 Wis. 523 (1891). Or, perhaps she is more similar to the accident victim whose loss of life or limb was caused by non-negligence. Either way, we traditionally let the chips fall where they may.

serious costs on the public.[210] It plucks out of the public domain information that people have determined to be pertinent to the evaluation of a person, supplanting instead that person's own (self-interested) judgment about what facts should inform public perception.[211] Descriptions and empirical claims would have to give way to opinion and conjecture. Credible proof and certainty of knowledge would be replaced with rumor, speculation, and deniability. Social class would be less dynamic; any information that would tend to blemish a person's reputation and relative social standing will be erased, thereby hardening the status quo.[212] (Upward social mobility is, after all, dependent on social downward mobility.) Also, the risk of moral hazard is not negligible. A decision to exercise the right to be forgotten can be driven by perverse incentives, as when an abusive spouse seeks to have his domestic violence record shielded from public disclosure.[213]

This is not to say that concrete privacy harm cannot arise from the dissemination of information. In circumstances where the ex ante expected losses to an information subject are greater than the expected societal gains, disclosure of personal information can and should lead to redress. Reasonable minds are bound to differ when deciding whether the likely psychic harms outweigh the social gains. The values on both sides of the scale are inordinately difficult to measure. But privacy legal scholars tend to demand avenues of redress in every instance where a person has suffered a psychic loss. Conceived of this way, a right to privacy would be stronger even than a right to bodily integrity.

The overarching concern motivating reputational harm arguments is that, with rapidly changing technologies and capabilities to store and process personal data, negative consequences to individuals' wellbeing are overlooked by courts and lawmakers. Implicit in this concern, though, is a strong assumption that losses in the era of big data automatically count as privacy *harm*. Many are simply collateral consequences.

Nevertheless, just as intrusion constitutes an injury with coherent theoretical underpinnings, certain types of disclosures also can cause predictable direct and indirect injury. In the next two sections, we explore restrictions on dissemination that successfully target appreciable harm.

---

[210] Heymann, *supra* note 204.

[211] Robert Post raises a similar objection to Jeffrey Rosen's claim that Bill Clinton's sexual exploits ought to have been kept private. Robert Post, *Three Concepts of Privacy*, 89 GEO. L. J. 2087, 2089-90 (2001) (Reviewing JEFFREY ROSEN, THE UNWANTED GAZE).

[212] Whitman, *supra* note at 1169-70 (though Whitman heralds the expressive value of dignity-based privacy protections).

[213] *See* Sheetz v. The Morning Call, Inc., 946 F.2d 202 (3d Cir. 1991). Another example, discussed in Part III, is a police officer's use of a state wiretap statute to prevent a citizen from recording an interaction the citizen believes to be corrupt or unethical ACLU v. Alvarez, Civil Action No. 10 C 5235 (N.D. IL, 2011).

B. Confidences

When personal information is revealed to a professional in a special, fiduciary relationship with the subject, as when a client tells a lawyer an unflattering fact about himself, disclosure restrictions function like an extension of the zone of seclusion. When the lawyer learns the secrets of his client, the client has not abandoned his seclusion. Instead, he has let the lawyer into it. The private facts, at least as disclosed to the lawyer, are still in the client's control, as if he had never exposed them in the first place. The client's conversation with his lawyer is different from other private conversations because the client has reserved, through express agreement or by implication, a right to confidentiality.

Arguably, dissemination restrictions could be left to private law, since express agreements of confidentiality can be worked out between private parties. However, individuals and society at large benefit so routinely from candor in certain types of relationships that law has stepped in to create default duty of confidentiality rules.[214] Placing stringent restrictions on doctors to keep their patients' confidences will on balance serve the public interest by encouraging candor and minimizing gawking. But the duty is qualified: in circumstances when disclosure *would* be better, as when others are in foreseeable danger, the common law either permits disclosure or requires it.[215]

Relationships were historically regulated through tort duties and professional codes of ethics[216], but now a host of federal and state statutes

---

[214] McCormick v. England, 494 S.E.2d 431 (S.C. 1997) (stating that "Being a fiduciary relationship, mutual trust and confidence are essential"). Courts look for a degree of kinship between the parties, or disparities in age, health, or mental conditions, or disparities in training and experience in order to determine whether two people are in a fiduciary relationship. Pottinger v. Pottinger, 605 N.E.2d 1130 (Ill. App. 1992).

[215] Tarasoff v. Regents of University of California, 551 P.2d 334 (Cal. 1976) (duty to warn likely victim of psychotherapy patient); Pate v. Threlkel, 661 So. 2d 278 (Fla. 1995) (duty to warn patients' children about genetic conditions). This description does not

[216] The tort of confidentiality does not enjoy the recognition that Prosser's privacy torts do, and it does not appear in the Second Restatement. But many jurisdictions recognize and enforce the duty of confidentiality in contexts ranging from doctors to bankers to accountants. Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L. J. 123 (2007). I am in agreement with Richards and Solove, and with Susan Gilles and Danielle Citron as well, that a clearer and more robust tort of breach of confidentiality could allow the common law to react to harmful disseminations of personal information. *Id.*; Susan Gilles, *Promises Betrayed: Breach of Confidence as a Remedy for Invasion of Privacy*, 43 BUFF. L. REV. 1 (1995); Citron, *supra* note 44 at 1848-50. The tort of public disclosure of private facts occasionally provides recourse for confidentiality-style harms. The disclosure tort has imposed responsibility on the police force to hold information about accident and crime victims in confidence, as well as the information from cooperative witnesses. *See* Catsouras v. Dept. Cal. Hwy. Patrol, 181 Cal.App.4th 856 (2010) (providing recovery to a decedent's family when a paramedic

impose some confidentiality rules. They usually regulate relationships where the information-receiver has an express or implied fiduciary responsibility to the information-provider. The major sector-specific federal privacy regimes are examples of confidentiality-style statutes, covering medical providers[217], creditors[218], educators[219], communications service providers[220], banks[221], and entertainment geared toward children[222].

The harm caused by the dissemination of information held in confidence is three-fold: first, the dissemination constitutes an invasion of seclusion. If a doctor provided his patient's medical file to a curious snoop, the revelation would cause at least as much distress as if the snoop had stolen a glance without the doctor's permission (a traditional intrusion upon seclusion[223]). Second, the professional's breach of trust may be an independent source of distress. And third, because confidentiality duties are imposed in contexts to promote the candid transfer of inherently sensitive information, dissemination of confidential information is likely to be used against the subject in some way.

Scholars focus on the third form of privacy harm as a means of understanding the goals of laws like HIPAA. On that basis, they advocate for a recognition of dissemination harms for more, or even all, categories of information.[224] But this second form contains an inherent tension between society's interest in having probative information and a person's desire to

---

took pictures at the scene of a deadly accident and sent the pictures to friends and acquaintances on Halloween). On the other hand, police are not expected to keep the confidences of suspects. *Wilson v. Freitas*, 214 P.3d 1110 (HI, 2009).

[217] Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, regulations at 45 C.F.R. § 164.

[218] Fair Credit Reporting Act, 15 U.S.C. § 1681.

[219] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.

[220] Telecommunications Act, 47 U.S.C. §222; Stored Communications Act, 18 U.S.C. § 2702 (business records may be disclosed to non-government third parties, but the contents of electronic communications may not).

[221] Gramm-Leach-Bliley Act, 15 U.S.C. § 6801.

[222] Children's Online Privacy Protection Act, 15 U.S.C. § 6502.

[223] *See* records-based intrusion cases, *supra* note 132.

[224] Richards, *supra* note 12. Neil Richards and Daniel Solove suggest that, if the tort of confidentiality were adopted in the U.S. to the same extent it is embraced in the United Kingdom, nearly every relationship could be considered the basis for a duty of confidentiality—ordinary citizens could be expected to refrain from divulging information about their friends, and airlines could be expected to maintain the confidences of their customers. Neil Richards & Daniel Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 176-177 (2007). *But See* Litman, *supra* note 39 at 1308-09 (proposing the expansion of the breach of confidence tort on the basis of the first source of harm—distrust.) Litman predicted that without robust confidentiality-style protection for all consumer transactions, we would "think twice before making embarrassing purchases or watching certain pay-per-view movies." *Id.* Consumer behavior in the twelve years that have elapsed since her writing this has proven otherwise.

keep information secret precisely because it is probative. The first form of harm, by contrast, allows confidentiality-style regulations to fit comfortably with our commitments to the free flow of information because, like intrusion, injury from a breach of confidentiality is independent from the utility of the divulged information. If a doctor talked about a particular patient's routine appendectomy at a party, he would violate his patient's privacy even if the facts were not particularly embarrassing.

American privacy law is criticized for being fragmented[225], but the existing statutory schemes typically apply to sectors in which an imbalance in training or experience justify the imposition of fiduciary responsibilities. For sectors that do not have a quasi-fiduciary responsibility with the consumer, assigning a duty of confidentiality unduly encumbers relationships that are not ones of unusual trust.[226] In addition to lost information, the public would bear the costs of administering a strong privacy system. These costs are considerable. A small hospital with only 400 beds can spend upwards of $500,000 on HIPAA compliance each year, and for large hospitals the direct administrative costs are in the millions of dollars.[227] Arguably, it is appropriate to impose these costs on doctors and spread them across the base of health care consumers because the confidentiality duty promotes truthful medical consultations and leads to optimal care, but the same reasoning does not hold for our merchants.[228]

Some existing privacy laws unwisely create confidentiality duties for relationships with only marginal amounts of trust. California's carpooling privacy statute, for example, imposes criminal liability for divulging carpool or ridesharing information. [229] The Video Privacy Protection Act ("VPPA") imposes criminal and civil liability upon video rental stores and their employees who disclose customer rental information.[230] These statutes are often the products of legislation by anecdote, as when the release of Judge Robert Bork's video rental records during his Supreme Court confirmation hearings prompted the passage of

---

[225] Lior Strahilevitz, *Reunifying Privacy Law*, 98 CAL. L. REV. 2007 (2010); Lipton, *supra* note 21 at 510.

[226] I disagree with scholars who explain the current collection of statutes as imposing privacy restrictions when information is "regarded as more sensitive than others." Lipton, *supra* note 21 at 510. Bartenders, personal trainers, and friends end up with a lot of special information about the most sensitive aspects of their customers' and colleagues' lives. It is the nature of the relationship, and not the nature of the information, that justifies a different treatment for the information held by doctors and financial advisors.

[227] P. Kilbridge, *The Cost of HIPAA Compliance*, 348 N. ENGL. J. MED. 1423 (2003).

[228] Confidentiality duties might be expanded to cover relationships of trust in the online space. An online support group, or a website offering customized medical or legal advice, arguably should have the same responsibilities that apply in real space.

[229] CAL. PEN. CODE §637.6.

[230] Video Privacy Protection Act, 18 U.S.C. § 2710.

the VPPA.[231] The VPPA now demonstrates how overreaching confidentiality-style statutes can frustrate a regulated industry's attempts to expand services or use data in innocuous ways. Netflix has expended considerable energy, and billable hours, to find a lawful way for its members to report that they "like" a movie on Facebook. The VPPA's written consent requirements for re-disclosure of video rental information are so onerous that Netflix has resorted to lobbying for a change in the law.[232] Duties of confidentiality should be imposed only in the instances where the benefits are known to outweigh the considerable costs.

C. Disclosure of Highly Volatile Information

The tort of public disclosure of private facts has an uncertain future. Liability for public disclosure is triggered when somebody gives "publicity" to a private fact, if the matter is highly offensive, and if the fact is not of legitimate concern to the public.[233] Scholars have struggled to make sense of the public disclosure tort's interaction with the First Amendment for decades. The tort is constructed with a number of safety valves to ease the inherent tension between the right to speech and the right to not have one's story told. It avoids roping in gossip and ordinary conversation by requiring the plaintiff to show that the defendant disclosed the private fact to a broad audience.[234] And it also immunizes disclosures of newsworthy information, an exemption much bemoaned by privacy scholars as the exception that swallows the rule.[235] These exceptions may be helpful for avoiding constitutional challenges, but they only make it more difficult to understand what the tort is attempting to accomplish. If a person is not at liberty to communicate a piece of information he has, why do we not constrain this person through confidentiality laws? And if this person is too distant from the tort victim to formalize their relationship through confidentiality laws, then what is it that makes the fact "private"?

Notwithstanding these puzzles, the public disclosure tort serves important and unique functions. Consider this hypothetical, based loosely

---

[231] Michael Dolan, *The Bork Tapes Saga*, THE AM. PORCH, http://www.theamericanporch.com/bork2.htm.

[232] Adam Clark Estes, *Why Robert Bork (Indirectly) Kept Netflix Off Facebook*, ATLANTIC WIRE, July 26, 2011, *at* http://www.theatlanticwire.com/technology/2011/07/why-robert-bork-indirectly-kept-netflix-facebook/40408/.

[233] REST. (2D) TORTS §652D.

[234] In most jurisdictions the "publicity" element requires disclosure to the general public, but in some states disclosure to an especially important audience will suffice. Miller v. Motorola, Inc., 560 N.E.2d 900 (Ill. 1990) (finding that disclosure to the plaintiff's work colleagues was sufficient to fulfill the "publicity" element).

[235] Citron, *supra* note 44.

on the facts of *Doe v. Borough of Barrington*[236]. A heated argument at a bar in 1987 led to a physical confrontation between Arthur and Billy. Arthur said, "Careful! I'm HIV positive." At this time, the AIDS epidemic was not well understood by the general public. Later that night, Billy told Arthur's neighbors about Arthur's serostatus. One of Arthur's neighbors had young children who attended public school with Arthur's children. She phoned the parents of all of the other students in the class and spread the news that Arthur has HIV. Panicked, the other parents decided to keep their children home from school, fearing they might somehow contract the disease. Arthur's children arrived at school to find empty classrooms and social stigmatization.

These facts demonstrate that the public disclosure tort can target harm outside the ambit of confidentiality laws. The disclosure cases that tend to overcome the default assumptions favoring information flow usually share two characteristics: first, there is some modicum of implied use restriction[237], and second, the public will have a predictably irrational reaction to the disclosed facts. These types of highly volatile facts lead to consistent overreaction and discrimination.[238] Disclosure liability under these conditions avoids conflict with net public knowledge because highly volatile facts degrade public knowledge instead of improving it.[239]

Courts face a difficult task in identifying which types of personal facts are highly volatile. The lawmakers must have confidence that the public's response is not only overwhelmingly negative, but irrationally so. Sexually transmitted disease (especially HIV and AIDS) marks one example where the public's perception of the risks of transmission and fault

---

[236] Doe v. Bor. of Barrington, 729 F. Supp. 376 (D.N.J. 1990). In the case, the HIV status is initially disclosed to a police officer, who then told other people in his department for no health- or public safety-related reason.

[237] Lior Strahilevitz has shown that courts' determinations in disclosure cases tend to track theories of social networks. If a personal fact is shared with a support group made up of 20 members, the fact is treated as more private than if it is shared with 20 unconnected friends. Strahilevitz's social network theory is quite useful in explaining which contexts might have a modicum of implied use restriction. *See* Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005).

[238] Richard Murphy makes the sound argument that overreactions to AIDS and other phenomena are not necessarily irrational. Over-reaction can occur when the population remains rationally ignorant about a disease that is difficult to understand and relatively rare. Murphy, *supra* note 50 at 2401

[239] And, because of the first factor, disclosure torts would avoid imposing liability when the plaintiff puts no effort into keeping the information private. This reasoning lines up with Judge Frank Easterbrook's argument that reasonable restrictions on information will limit certain types of information that have the effect of diminishing the overall quality and quantity of publicly available information. Frank H. Easterbrook, *Insider Trading, Secret Agents, Evidentiary Privileges, and the Production of Information*, 1981 SUP. CT. REV. 309 (1981).

of the carriers are not in line with reality.[240] Homosexuality might be another.[241]

The trouble is that classifications are unlikely to stay static over time, and are sometimes defused in a single generation. A strong regulation that makes sense at one point of time can cause unexpected problems later. As an example, California's HIV privacy law prohibits the disclosure of HIV test information for *any* reason, including through compelled discovery with protective orders.[242] At the time of the law's passage this seemed like a wise way to protect HIV-positive patients and their supportive communities. However, as the stigma of positive serostatus diminished, the law began to produce unintended consequences. For example, the plaintiff in *Children's Hospital v. Workers' Compensation Appeals Board* mysteriously contracted HIV during her time working at a hospital.[243] She presented convincing evidence to the Workers' Compensation Board that she did not contract HIV from her husband, her only sexual partner, but the Board demanded evidence that affirmatively supported her claim she contracted the disease at work.[244] The plaintiff subpoenaed her former employer hospital for a statistical record reporting the number of patients that passed through her particular hospital ward each year during her employ.

California's HIV privacy statute prevented the hospital from complying with her demand.[245] Because a record of this sort didn't yet exist, the hospital would have to order a member of its staff to go through patients' charts to count the number of HIV cases, and even a staff member could not do so without first securing explicit consent from every hospital patient. At the time of the law's passage, even hospital employees may have had a morbid curiosity in the serostatus of patients, but today it is difficult to believe that a hospital administrator would be unable to maintain professionalism while compiling a statistical record of this sort. Since the plaintiff's claim for worker's compensation depended on her access to this evidence, the privacy statute quashed her chances of receiving pay and, as a

---

[240] Doe v. Bor. of Barrington, 729 F. Supp. 376 (D.N.J. 1990); Doe v. Southeastern Penna. Transportation Auth., 72 F.3d 1133 (3d Cir. 1995); CAL. HEALTH & SAFETY C. §120975; Margo Kaplan, *Rethinking HIV-Exposure Crimes*, 87 IND. L. J. __ (forthcoming, 2012).

[241] Sipple v. Chronicle Publishing Co., 201 Cal. Rptr. 665 (Ca. 1984) (finding the disclosure of Sipple's sexual orientation was a matter of public concern because the newspaper story was exploring the possible homophobia of President Ford. Sipple's parents disowned him after the national news coverage broke, showing the high stakes when this sort of information is released.).

[242] CAL. HEALTH & SAFETY C. §120975.

[243] Children's Hosp. & Research Center Oakland v. Workers' Comp. Appeals Bd., 2010 WL 3936050 (Cal. 2010).

[244] *Id.* at *2.

[245] *Id.* at *7.

result, harmed a member of the very HIV-positive community it had intended to help. State laws regarding homosexuality as a category of libel per se exhibit a similar problem.[246] The common law might be better suited than legislatures to recognize highly volatile facts without letting that status ossify and outlast its usefulness.

Privacy advocates and scholars champion dissemination restrictions, but when the regulations do not follow the confidentiality model or the highly volatile fact model, they are usually ill-advised. The next subsections discuss the problems that can result from overzealous dissemination bans using credit markets as a case study.

D. Dissemination Restriction Case Study: Credit Markets

Many Americans have difficulty accessing credit for the first time. Banks and credit card issuers use debt payment histories to determine credit-worthiness, so without debt histories, college students and low socio-economic status ("SES") individuals are frequently shut out of mainstream credit markets.[247] This is not in the best interests of reliable low-SES applicants who might benefit from a line of credit, nor is it in the credit issuers' interests. But creditors have a difficult time distinguishing low-risk applicants who lack credit history from those who pose a high risk of default. The credit market suffers from an information problem. By leaving a significant portion of the American population un-assessable and unscorable, the information problem does a disservice to creditors and would-be debtors alike.

A recent study by the Political & Economic Research Council found a new source for measuring creditworthiness: utility bills.[248] Utility bill payment histories correlate well with loan repayment, so adding data on utility payment histories to the calculation of credit scores improves the scores' predictive power. More importantly, utility bills provide a means of *creating* credit scores for 10% of the previously unscorable population.

Privacy advocates have objected to the disclosure of utility bill data for this purpose because some applicants' credit scores might decrease on account of payment histories they did not know were being tracked.[249] It is an odd argument: because consumers are not given the opportunity to game the credit markets through strategic behavior, a creditor's use of a fuller,

---

[246] Klepetko v. Reisman, 41 AD3d 551 (N.Y. 2007) (reluctantly followed recently in Yonaty v. Mincolla, 2011 NY Slip Op 51037-2011 (N.Y. 2011)).
[247] Ylan Q. Mui, *Little-Known Firms Tracking Data Used in Credit Scores*, WASH. POST, July 16, 2011.
[248] Michael Turner, et al., *You Score, You Win: The Consequences of Giving Credit Where Credit is Due*, POLITICAL & ECONOMIC RESEARCH COUNCIL (2008), *available at* http://perc.net/files/downloads/web_layout-you-score.pdf.
[249] Mui, *supra* note 247.

more accurate set of information constitutes a privacy violation. This is another example where collateral consequences of past behavior are mistaken for privacy harm. Moreover, privacy regulations outlawing the transfer of utility bills in this context would hinder class mobility.

Better measures of creditworthiness *help* the poor. They allow traditionally overlooked credit applicants to access credit lines, and just as importantly, they weed out higher-SES credit applicants who score well on traditional measures but are actually more likely to default.[250] Without the utility credit scores, lower-SES applicants would cross-subsidize higher income applicants.[251]

Utility payment history reporting for credit scoring is a novel repurposing of data. If all business records operated under the same dissemination restrictions that our medical records do, this new use would have been overlooked.[252] Dissemination restrictions are rarely the best means of balancing privacy and information interests. Restrictions that prohibit all uses other than the ones for which the information was collected are equally problematic.[253] On the other hand, regulations targeting specific misuse can work quite well.

E. Use Restriction Case Study: Credit Reports

[250] Perhaps this point is best illustrated if we imagine an alternative universe where credit lenders were not allowed to access *any* credit or consumer data on their applicants. In this case the creditor would use existing assets and income in order to determine who got a loan and who didn't. In other words, lower-income applicants would systematically be denied credit due to lack of collateral. This would not serve creditors well, either. Because of the noise in their algorithm, default rates would rise, and interest rates would have to increase.

[251] This phenomenon is completely overlooked by the National Consumer Law Center, which concluded that utility credit reporting would adversely affect low-income credit applicants. NATIONAL CONSUMER LAW CENTER, FULL UTILITY CREDIT REPORTING: RISKS TO LAW INCOME CONSUMERS (2009), *at* http://www.nclc.org/images/pdf/credit_reports/credit_reports_full_utility_dec2009.pdf. The report argues that, because 14% of households in the lowest income quintile missed a payment on their utility bill (compared to just over 2% for the highest income quintile), a credit measure that takes utility bills into account will disproportionately harm the poor. It is true that utility data, like *all* measures of creditworthiness, does not fall uniformly across income classes. But the consumer organization overlooks the fact that credit scores will rise for the 86% of the lowest quintile who did not miss a payment. The report also concludes that incorporating utility bills into credit scores will have the effect of pushing utility bills to the top of the priority list for low-income households, and as a result these households would reduce their purchases of necessities like food and medical care. This claim is not supported by data in the report, but is an interesting empirical question.

[252] Utility credit reports, like all reports used to make credit and hiring decisions, ought to be paired with regulation allowing for consumers to check for the accuracy of their records, and to challenge any report believed to contain inaccurate information. The Fair Credit Reporting Act serves as a model for such a scheme. 15 U.S.C. §§ 1681e(b), 1681i(a)(1).

[253] EU Data Protection Directive, *supra* note 30.

Laws prohibiting specific uses of personal information can achieve the goals of privacy law without significantly curtailing the flow of truthful information. If we have reason to believe that a particular use diminishes social welfare, we can and should craft prohibitions on those specific uses. Antidiscrimination laws are prime examples of narrow use restrictions. Anti-discrimination laws restrict the use of race, age, sex, or medical information for hiring, housing, and lending decisions because the biases that result from use of this information, whether statistically rational or not, run against the public interest.[254] These laws work well on the risk-utility calculator because they allow information to be exploited for all purposes except the ones that have been determined to be harmful or risky.[255] The large, rich scholarship on discrimination law explores and debates the soundness of anti-discrimination measures.[256] Curiously, the privacy and discrimination fields often work in isolation, without overt awareness that regulations called "privacy laws" and those called "antidiscrimination laws" often aim to prevent the same harms.[257]

To observe how privacy goals can be achieved through antidiscrimination policies, consider the utility credit reports described in the last subsection. We might wonder whether employers should be proscribed from using these new utility credit scores. As a general matter, we would like employers to differentiate between job applicants on the basis of characteristics that have a relationship to job performance. If employers are enjoined from making hiring considerations based on likely performance ability, the redistribution of jobs and wealth will take place within a pool of applicants such that the it will be slightly harder for higher-performers to obtain the job, and slightly easier for lower-performers.[258] However, employers, like all humans, are susceptible to biases or

[254] Title VII of the Civil Rights Act of 1964, 42 U.S.C. 2000e et seq.

[255] Occasionally these laws will override pragmatism, as when the Americans with Disabilities Act requires employers to incur additional costs by hiring disabled applicants who require an accommodation, and whose inclusion in the employer's health plan may drive up fees. We do so for expressive and equitable reasons, but such laws require some forethought and caution, since use regulations of this sort will localize large costs that might be better spread across society. 42 U.S.C. §§ 12111-12117.

[256] I include just a smattering of the scholarship here. Kimberle Williams Crenshaw, *Race, Reform, and Retrenchment: Transformation and Legitimation in Antidiscrimination Law*, 101 HARV. L. REV. 1331 (1988); RICHARD EPSTEIN, FORBIDDEN GROUNDS: THE CASE AGAINST EMPLOYMENT DISCRIMINATION LAWS (1991); John J. Donohue, *Anti-Discrimination Law*, THE NEW PALGRAVE DICTIONARY OF ECONOMICS (Steven N. Durlauf & Lawrence E. Blume, eds., 2008).

[257] The one exception seems to be the topic of genetic privacy, which inspires privacy and discrimination scholars to synchronize their efforts. *See*, *e.g.,* Michael S. Yesley, *Protecting Genetic Difference*, 13 BERKELEY TECH. L. J. 653 (1998).

[258] George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623, 630 (1980)

unexamined assumptions leading them to adopt a hiring criterion that does not actually predict future job performance. When this happens, wealth and employment are distributed within the within the class of job applicants in a way that is capricious at best, discriminatory at worst, and in any case unmoored from merit and desert. Under which of these models do credit reports fall? Do credit reports make the labor market more meritocratic or less so?

The federal Fair Credit Reporting Act permits employers to access credit reports during hiring processes.[259] Considering that federal law prohibits just about everyone else to access credit reports[260], one would think there is abundant evidence that credit scores correlate strongly with worker competency and job performance. While there is evidence that present financial stress correlates with absenteeism[261], there is little evidence that credit reports predict the likelihood of success among job applicants.

Even if credit reports were somewhat predictive of job performance, if the effect is small, social welfare could benefit from limiting an employer's access to credit information. A person who is already struggling to pay bills and regain control over their finances is vulnerable to sliding into bankruptcy or poverty if he cannot obtain employment. If he does, he will impose negative externalities on others including unemployment insurance, the cost of uninsured health care, and at the extreme, welfare programs. We also might be concerned about disparate impacts on the disabled and working mothers since financial crises are often caused by medical or family emergencies. We might classify the financially insecure as a protected class, and prevent discrimination on the basis of financial security. However, this puts employers in a difficult spot. They are under pressure to avoid hiring risky employees not only for financial reasons, but to avoid liability under Title VII or for the tort of negligent hiring.[262]

An information-forcing law might provide a reasonable middle ground, obligating employers to disclose to their job applicants all personal

---

[259] 15 U.S.C. 1681b(a)(3)(B)

[260] 15 U.S.C. 1681b(a) ("any consumer reporting agency may furnish a consumer report under the following circumstances and *no other*") (emphasis added).

[261] So-hyun Joo and E. Thomas Garman, *The Potential Effects of Workplace Financial Education Based on the Relationship Between Personal Financial Wellness and Worker Job Productivity*, 2 PERSONAL FINANCES & WORKER PRODUCTIVITY 163 (1998).

[262] Cathie A. Shattuck, *The Tort of Negligent Hiring and the Use of Selection Devices: The Employee's Right of Privacy and the Employer's Need to Know*, 11 INDUS. REL. L. J. 2 (1989); Meredith J. Fried, *Note, Helping Employers Help Themselves: Resolving the Conflict Between the Fair Credit Reporting Act and Title VII*, 69 FORDHAM L. REV. 209 (2000); John E. Matejkovic & Margaret E. Matejkovic, *Whom to Hire: Rampant Misrepresentations of Credentials Mandate the Prudent Employer Make Informed Hiring Decisions*, 39 CREIGHTON L. REV. 827 (2005).

information accessed in the course of making a hiring decision. Accurate information, and the influence it has on the choices of both employers and job applicants, is one of the three means of transferring power identified in Mary Graham's *Democracy by Disclosure*. Transparency laws are in direct tension with personal privacy, but they can be unexpectedly consonant with the aim of respectful and dignified treatment.

The credit report case study shows that, with careful consideration for competing public policy concerns, information harms can be reduced using carefully tailored use restrictions. But these restrictions have little in common with the blunt and comprehensive restrictions proposed by privacy scholars.[263]

VI. CONCLUSIONS

Tort law holds the solution to vexing problems in privacy law. Yet it has been neglected by privacy law scholars, who are on a misguided quest to constrain the quantity, spread, and re-purposing of personal data. The extensive regulations they propose come into direct conflict with traditional American normative commitments to the free flow of information. Rather than questioning the wisdom of their proposals, privacy scholars pursue the dubious goal of changing America's normative commitments.

We do not yet understand the benefits and consequences of living in a world of unlimited quantities of accurate data—bad portraits, precise records of e-mails, Web search histories, recordings of our own voices, and nearly every other interaction we have with a computer. Undoubtedly we know more about each other and ourselves because of these new information troves. It is natural, even if it isn't rational, to regard change as a presumptive threat. Privacy scholars, like all humans, are wired to believe that the existing state of affairs has struck a good balance between remembering and forgetting, and that technologies tipping the scale in one direction or the other are more likely to damage the information ecosystem than to improve it.[264] Behavioral psychologists and economists refer to this

[263] Richards, *supra* note 12; LESSIG, *supra* note **Error! Bookmark not defined.**; Kang, *supra* note **Error! Bookmark not defined.**.

[264] Jessica Litman argues that the mere fact that most Americans deplore the collection and selling of personal data is reason enough to regulate or prohibit the practices, though she does not attempt to define what, exactly, is so deplorable. Litman, *supra* note 39 at 1303. Orin Kerr posits that an unconscious quest to maintain the existing equilibrium in relative information power explains the outcomes of Fourth Amendment cases. Orin Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. __ (forthcoming 2011).

as status quo bias[265], and Lawrence Lessig more vibrantly refers to it as Is-Ism: what Is is what must be. [266] Technology shocks significantly alter the world, and predictions about the future state will be more pessimistic than the valuation of the current state, of what we have to lose.

To this point, American lawmakers have been wisely reluctant to condemn the accumulation of personal information until we fully understand its consequences. It is tempting to think that controlling the production of records so that we have not-too-many-more than we used to will keep intact the best balance between the virtues of information and secrecy, but this is emotion-driven rationalization of the status quo. Consider the similarities to the fable of King Thamus, originally told by Plato and retold in Neil Postman's *Technopoly*.[267] Theuth, an inventor, approached Thamus with a new invention he hoped to introduce to the Egyptian people: the written word. Claiming that the use of letters could make Egyptians wiser by improving their memories, King Thamus responded:

> [Y]ou, who are the father of letters, have been led by your affection to ascribe to them a power the opposite of that which they really possess. For this invention will produce forgetfulness in the minds of those who learn to use it, because they will not practice their memory. Their trust in writing, produced by external characters which are no part of themselves, will discourage the use of their own memory within them. You have invented an elixir not of memory, but of reminding; and you offer your pupils the appearance of wisdom, not true wisdom, for they will read many things without instruction and will therefore seem to know many things, when they are for the most part ignorant and hard to get along with, since they are not wise, but only appear wise.[268]

The comparison between distrust of personal data and Plato's distrust of the written word is all the more chill-inducing when we consider the history of personal data collection. The progenitor of Big Data was the early accounting records scratched into clay tablets six thousand years ago by traders in Uruk, an ancient Mesopotamian city.[269] These clay accounting

---

[265] Daniel Kahneman et al., *Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias*, 5 J. ECON. PERSPECTIVES 193, 197-199 (1991).
[266] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 24 (1999)
[267] NEIL POSTMAN, TECHNOPOLY 73-74 (1992).
[268] PLATO IN TWELVE VOLUMES, Vol. 9 (1925) (Harold N. Fowler, trans.).
[269] MATT RIDLEY, THE RATIONAL OPTIMIST: HOW PROSPERITY EVOLVES 160 (2010).

tablets are also the first form of writing.[270] Records really are the building blocks of ideas and expression.

Though the United States stands alone among developed countries without omnibus data protection laws, our preference for tort principles over property rights is eminently sensible. The sweeping restrictions of Europe's Data Protection Directive allow individuals to control the flow of information regardless of the impact on the rest of the public. Tort doctrines find rules that favor the well-being of society over the preferences of any one individual. They begin with a presumption that private actors may gather and distribute information freely. This presumption is overcome in circumstances where privacy rights improve social welfare.[271] Courts and lawmakers are desperate to find a privacy response suited to the ambiguity and risks of new technologies without imposing too many restrictions on information flow. Even Justice Kennedy, who is not by any stretch of the imagination a privacy advocate, acknowledges that technology "presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure." [272] Fortunately, tort has already developed an attractive, pragmatic option.

Privacy scholars have overlooked the potential of the old common law intrusion tort to meet new privacy challenges in the information age. Because the interests protected by the intrusion tort are independent from the public's interest in probative information, the tort is more stable than other types of privacy laws. By clarifying that the intrusion tort imposes liability for obnoxious observations, as opposed to the creation of data, this Article has demonstrated that the intrusion tort is apt to deter offensive, targeted observations, and to protect the sense of seclusion that people have come to expect even in a world brimming with data. Intrusion offers a principled way to penalize space invaders without unduly taxing the benefits society enjoys from open information exchange.

* * *

[270] *Id.*

[271] Tort and Privacy scholars alike have doubted the viability of tort law to make a significant impact in the information frontier, especially since tort is regarded as the disfavored branch of common law, inviting accusations of litigiousness and uncertainty that do not seem to attach to the doctrines of property and contract. This is what Anita Bernstein calls the "tort paradox." Bernstein, *supra* note 104 at 1547-52.

[272] Sorrell v. IMS Health Inc., 131 S.Ct. at 2672.