2016

Taking Trust Seriously in Privacy Law

Neil M. Richards
Washington University in St. Louis School of Law, nrichards@wustl.edu

Woodrow Hartzog
Boston University School of Law

TAKING TRUST SERIOUSLY IN PRIVACY LAW

Neil Richards* & Woodrow Hartzog**

CITE AS: 19 STAN. TECH. L. REV. 431 (2016)

ABSTRACT

Trust—the willingness to accept vulnerability to the actions of others—is the essential ingredient for friendship, commerce, transportation, and virtually every other activity that involves other people. It allows us to build things, and it allows us to grow. Trust is everywhere, but particularly at the core of the information relationships that have come to characterize our modern, digital lives. Relationships between people and their ISPs, social networks, and hired professionals are typically understood in terms of privacy. But the way we have talked about privacy has a pessimism problem—privacy is conceptualized in negative terms, which leads us to mistakenly look for "creepy" new practices, focus excessively on harms from invasions of privacy, and place too much weight on the ability of individuals to opt out of harmful or offensive data practices.

But there is another way to think about privacy and shape our laws. Instead of trying to protect us against bad things, privacy rules can be used to create good things, like trust. In this paper, we argue that privacy can and should be thought of as enabling trust in our essential information relationships. This vision of privacy creates value for all parties to an information transaction and enables the kind of sustainable information relationships on which our digital economy must depend.

Privacy laws and practices centered on trust would enrich our understanding of the existing FIP principles of confidentiality, transparency, and data protection, moving them from procedural means of compliance for data extraction towards substantive principles

---

* Thomas and Karole Green Professor of Law, Washington University School of Law, Affiliate Scholar, The Center for Internet and Society at Stanford Law School.

** Starnes Professor of Law, Samford University's Cumberland School of Law, Affiliate Scholar, The Center for Internet and Society at Stanford Law School. We thank Lisa Austin, Ryan Calo, Julie Cohen, Nico van Eijk, Sue Glueck, Mike Hintze, Margot Kaminski, Bill McGeveran, Caroline Nguyen, Jules Polonetsky, Jason Schultz, Jeffrey Vagle, Christopher Yoo, and the participants at workshops at the Center for Technology, Innovation & Competition at Penn Law, the Privacy Law Scholars Conferences at Berkeley Law and the IViR at the University of Amsterdam, the Privacy and Security Forum at George Washington University, Saint Louis University, Dartmouth College, Berkeley Law, Notre Dame Law School, the Future of Privacy Forum, and Microsoft, Inc. for their helpful comments and suggestions. We also thank Ujjayini Bose, Kevin Jacobsen, Lydia Wimberly, and Megan Fitzpatrick for their excellent research assistance.

to build trusted, sustainable information relationships. Thinking about privacy in terms of trust also reveals a principle that should become a new bedrock tenet of privacy law: Loyalty. Rejuvenating privacy law by getting past Privacy Pessimism is essential if we are to build the kind of digital society that is sustainable and ultimately beneficial to all—users, governments, and companies. There is a better way forward for privacy. Trust us.

TABLE OF CONTENTS

I. INTRODUCTION

Trust is beautiful. The willingness to accept vulnerability to the actions of others is the essential ingredient for friendships, commerce, transportation, and virtually every other activity that involves other people. It allows us to build things, and it allows us to grow.

Trust is everywhere, even if it is not obvious. We trust that architects and builders have created bridges that will support us when we cross them. We trust that merchants will accept the small, green pieces of paper (or digital code) we've earned in exchange for goods and services. We trust that airplanes will arrive safely and to the correct airport. We trust that professionals in our service will act in our best interest, and we trust that our friends will support us and look out for us. Without trust, our modern systems of government, commerce, and society itself would crumble.

Trust is also the essential ingredient for our digital lives. So much of modern networked life is mediated by information relationships, in which professionals, private institutions, or the government hold information about us as part of providing a service. Such relationships are everywhere we look. We see them when we share sensitive personal information with Internet service providers (ISPs), doctors, banks, search engines, credit card companies, and countless other information recipients and intermediaries. We also see them as we get information via large and small computers to access apps, social media, and the Internet at large.

Even relationships that used to have no significant informational component—grocery stores, airlines, political party affiliations, and the like—are now part of the data game. Merchants use data to predict what shoppers will do. Companies give away products and services "for free" just to get the information that

comes with it. Data brokers amass vast troves of data to enable their clients to profile, segment, and influence people as consumers or as voters. The stampede for big data and the development of the "Internet of Things" are only accelerating these developments. If we want a sustainable digital society, we need strong, trusted information relationships.

When we talk about personal information changing hands, policymakers, lawyers, and citizens throughout the world use the word "privacy." In this context, privacy means the rules governing the collection, use, and disclosure of information. Ostensibly, privacy rules should encourage and fortify information relationships. They should build trust in these relationships. But they don't. Rather than encouraging trust, modern American privacy law encourages companies to profit in short-sighted ways by extracting as much value as possible from personal data in the short term. As long as companies don't cause a narrow set of legally recognized, largely financial harms, they are essentially free to set up the terms of information relationships any way they wish. Companies have this power because of a second hallmark of modern American privacy law, its reliance on a control-based regime of "notice and choice." Under this arrangement, terms are hidden in the fine print of legal notices virtually no one reads, and there is as little meaningful choice as in old-fashioned consumer adhesion contracts. Consumers are left exposed and bewildered, lamenting what they see as the "death of privacy."[1]

Privacy—the legal regime governing the use of personal information—is not dead, nor is it going away. In a society in which the exploitation of personal data is an enormous source of value, national and international rules governing that data are inevitable. But how we talk about privacy matters, as it structures the terms of a debate in which little is inevitable and so much is up for grabs.

Critically, the way we talk about privacy as lawyers is increasingly inadequate because it is too often framed in negative terms. Privacy is seen a tax on profits, a drain on innovation, a dangerous and naive assumption, and a burden on the individual to fend for herself in the digital thicket. Hot information age topics like "permissionless innovation," "creepiness," "privacy harm," and "the privacy paradox" highlight what is to be lost rather than gained in the privacy debate. In short, privacy has a pessimism problem.

Such negative ways of thinking about privacy are incomplete and often inaccurate. What's missing is a positive understanding of privacy in terms of the good it can potentially do. And what's missing is the essential relationship between privacy and trust. Privacy Pessimists often ignore trust, even though trust is essential. Yet thinking about information relationships and privacy rules in terms of trust reveals how privacy protections can be a positive force, generating deeper and more sustainable information relationships and corporate profits.

We need information relationships to function in our modern networked society. But as users we're bewildered. Our information is collected, used, and ana-

1. Neil M. Richards, *Four Privacy Myths*, *in* A WORLD WITHOUT PRIVACY? 33 (Austin Sarat ed., 2015) (critiquing the rhetoric of the "death of privacy").

lyzed in ways we cannot understand and can rarely control. Given this fact, it should be no surprise that people feel confused and disempowered when it comes to their data. Instead of feeling confident that we'll be protected when we share information with others, we increasingly feel helpless and resigned to our fate, whatever that might be.

This is a problem not just for consumers but also for the companies and governments on the other side of these relationships. Without trust, people share less information, bad information, or no information at all. They become anxious, bewildered, and suspicious. They lie or self-censor otherwise beneficial information. If people don't trust a company, they are more likely to switch to a competitor or resist or fail to become fully invested in the commercial relationship. Our piecemeal laws of personal data create incentives for a quick buck through a kind of data strip mining. We have a legal regime that encourages a short-term and short-sighted "monetization" of data that leaves consumers confused and frustrated. This is an inefficient and unsustainable state of affairs, yet both our laws and the ways we talk about privacy enable it.

Our basic claim in this paper is quite simple: modern privacy law is incomplete because from its inception it has failed to account for the importance of trust. This gap has biased privacy law and norms toward a pessimistic proceduralism in which harm avoidance is the only substantive value. Trust in information relationships is necessary for the digital economy not just to function, but to flourish. Acting together, privacy and trust can do more than avoid harm, but can create value. We can do better, and should use privacy law promote trust across the board.

Our argument proceeds in three steps. First, we highlight the problem of Privacy Pessimism. We survey the world of privacy law and describe how and why it has led us to be pessimistic. Framing the privacy debate over what is being lost has frustrated the true potential of information rules to benefit everyone. This frame, which affects both our policies and the ways we talk about them, results in casting privacy in opposition to other interests like innovation and security. It leads us to obsess over locating "privacy harms" and scratch our heads over mysteries like "creepiness," "the privacy paradox" and "notice and choice." This pessimism is then enshrined in law, which perpetuates the fatalistic cycle.

Second, we propose an alternate vision for privacy by conceptualizing it in terms of trust. Privacy rules—regulation of information in relationships—have enormous potential to build the trust necessary for our digital society to flourish. Our theory of privacy and trust seeks to encourage the creation of long-term, sustainable information relationships to unlock the full potential of data and modern technology. Thinking about privacy in terms of its potential to build trust focuses on creating strong social bonds and sustainable, profitable relationships. It serves the interests of commerce, social relationships, and promotion of free expression and political engagement. It also shows thinking of privacy exclusively in negative terms is just plain wrong.

Finally, we suggest how our law and social practices can better promote trust in government and corporate information relationships. We propose two paths

forward. First, the Fair Information Practices (FIPs) and their progeny should be rejuvenated by incorporating trust as a guiding principle. Doing so will add nuance, rigor, and direction to many of the exiting obligations under the many legal regimes that incorporate the FIPs. Confidentiality becomes more useful and contextual as a duty of *Discretion*. Transparency becomes more effective and inclusive if re-conceptualized as an obligation of *Honesty*. And, security becomes more complete when framed as a duty of *Protection*.

We also introduce the new concept of *Loyalty* as a foundational value for privacy law. Borrowing from the law of fiduciaries, we argue that there should be limits on the amount of self-dealing one can engage in after being entrusted with personal information. Consent via the fine print of a legal agreement no one reads is disloyal and illegitimate. One of the biggest fears in the modern information economy is that personal information obtained from users will be used against their interests. The obligation of Loyalty aims to prevent that from happening, and should be enshrined in statutes as well as the common law torts and consumer protection law.

There is a better way forward for privacy. Trust us.

II. PRIVACY'S PESSIMISM PROBLEM

Modern privacy law has painted us into a corner. We have designed elaborate, nuanced, and even powerful frameworks to respond to the wrongful collection, use, and dissemination of personal information. For a while, it worked reasonably well. But new problems have come to thwart the best intentions of privacy law.

Modern privacy law is the offspring of two separate bodies of law. The privacy torts were developed in response to new surveillance technologies and a perceived media aggressiveness,[2] while the Fair Information Practices or "FIPs" were developed in response to electronic databases.[3] Tort privacy offers a substantive principle: Do No Harm when processing personal data. By contrast, the FIPs offer a procedural framework for managing the collection and flow of personal data rooted in some opportunity for individuals to have *notice* of when their data is being collected or used and some *choice* to control objectionable practices.[4] Together, the *Harm Principle* that comes from tort law and the *Control Principle* that comes from the FIPs are the bedrock of modern privacy law, animating everything from statutes like the federal Privacy Act and HIPAA to the substance of FTC enforcement actions and foreign privacy regimes.

As we discuss below, while the FIPs haven proven to be quite useful as an or-

---

2. Neil M. Richards, *The Limits of Tort Privacy*, 9 J. TELECOMM. & HIGH TECH. L. 357, 361-62 (2011).

3. *See* NEIL RICHARDS, INTELLECTUAL PRIVACY (2015).

4. *See* Robert Gellman, Fair Information Practices: A Basic History, Version 2.16, Feb. 11, 2015, http://bobgellman.com/rg-docs/rg-FIPShistory.pdf [http://perma.cc/54DD-WPAT]; HELEN NISSENBAUM, PRIVACY IN CONTEXT 129 (2010).

ganizing principle, they are weakening. Not only are the FIPs non-responsive to some new privacy problems, but they are also centered on the autonomous ideal of control. As long as users have control to decide when they relinquish certain privacy rights, then companies are abiding by the FIPs. In the current system of FIPs-based regulation of personal data, the user is seen as a completely rational, autonomous actor capable of controlling her down privacy destiny. If she loses any privacy, it is because she chooses to do so.

This model of choice and control is well established in the privacy literature at all levels. Some of the most popular theories of privacy cast the concept in terms of control.[5] So too does the dominant system of informal regulation in the corporate world.[6] But both the *Harm Principle* and the *Control Principle* are oriented in negative terms—Do No Harm in using data, or at least get some kind of consent before you do. From this perspective, privacy is almost always a negative and costly concept, a harm to be avoided, or a consent to be obtained before something positive can happen. This is the pathology of Privacy Pessimism, and in this Part, we describe how Privacy Pessimism has caused us to think about privacy in a way that is unnecessary, incomplete, and focused on fixing harm rather than creating value. Three dimensions of this pessimism problem are most important. We call them *the Creepy Trap, the Harm Fixation*, and *the Control Illusion.*

A. *The Creepy Trap*

Most discussions of privacy and new technologies run into accusations of creepiness at some point. Surveillance-based advertising? Creepy.[7] Facebook tweaking your news feed to make you sad? Creepy.[8] The NSA, black box data recorders in cars, eavesdropping Barbie dolls, the Internet of Things, drones, or Google scanning your Gmail? Each of these practices have been labeled as "creepy" at one time or another.[9]

---

5. Alan Westin defined privacy as an individual's right "to control, edit, manage, and delete information about them[selves] and decide when, how, and to what extent information is communicated to others." ALAN WESTIN, PRIVACY AND FREEDOM (1967).

6. Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 260 (2011); Michael Zimmer, *Mark Zuckerberg's Theory of Privacy*, WASH. POST, Feb. 3, 2014, http://www.washingtonpost.com/lifestyle/style/mark-zuckerbergs-theory-of-privacy/2014/02/03/2c1d780a-8cea-11e3-95dd-36ff657a4dae_story.html [http://perma.cc/26KZ-9MLR].

7. *See generally* JULIA ANGWIN, DRAGNET NATION (2014).

8. Caitlin Dewey, *9 Answers About Facebook's Creepy Emotional-Manipulation Experiment*, WASH. POST (July 1, 2014), http://www.washingtonpost.com/news/the-intersect/wp/2014/07/01/9-answers-about-facebooks-creepy-emotional-manipulation-experiment [http://perma.cc/FZT9-BJ45].

9. Douglas Rushkoff, *NSA's Phone Snooping a Different Kind of Creepy*, CNN (June 6, 2013, 2:34 PM), http://www.cnn.com/2013/06/06/opinion/rushkoff-nsa-verizon [http://perma.cc/9VY3-YVAQ]; Chris Ward, *In Car Black Box Data Recorder Sounds Creepy*, DAILYCARBLOG (Jan. 15, 2015), http://www.dailycarblog.com/2015/01/car-black-box-data-recorder-sounds-creepy [http://perma.cc/Z86A-DUGR]; Tony Bradley, *The Creepy Factor of the 'Internet of Things'*, RSA BLOG (June 17, 2014), http://blogs.rsa.com/creepy-factor-internet-

This should be no surprise. Creepiness is our first impulse when we encounter changing norms or technologies that leave us exposed or vulnerable. It's a visceral sensation of discomfort and revulsion, a trigger that tells us when privacy might be threatened. If we feel that a practice is creepy, goes the intuition, maybe we should think about regulating it. But the flip side also seems to be true: if something isn't creepy, then it probably isn't a problem.

Creepiness has been explored as a privacy concept. In advice to technology companies about how to avoid the creepiness reaction from their users, Omer Tene and Jules Polonetsky suggest that there are "several categories of corporate behavior that customers and commentators have begun to label 'creepy' for lack of a better word," activities that don't violate any established law, but which give their customers the creeps.[10] Tene and Polonetsky advise companies to avoid deploying new technologies (or old technologies in new ways) in ways that seem creepy. Such limits are necessary, they assert, because "social values are far more nuanced and fickle that any existing (and most likely future) laws and regulations. In order to avoid creep, companies should resist the temptation to act with chutzpah, even though brazen and audacious behavior constitutes a hallmark of Silicon Valley entrepreneurship culture. The challenge is for companies to set the right tone when seeking intimate relationships with consumers."[11]

Creepiness is also embedded in more formal kinds of privacy law. The old privacy tort of "intrusion into seclusion" protects private places and relationships from menacing (or creepy) intrusions.[12] The Fourth Amendment's venerable *Katz* test requires not only a famous "reasonable expectation of privacy," but a subjective expectation of privacy as well.[13] This subjective element means that for the Fourth Amendment to apply, a citizen has to feel violated by a government intrusion or monitoring. Though rarely phrased in terms of creepiness, Fourth Amendment law is based upon a similar idea that privacy is only invaded when there is a felt sense of intrusion of violation.

Helen Nissenbaum's much-praised theory of privacy as "contextual integrity"

---

things [http://perma.cc/EQJ2-CB3M]; Cyrus Farivar, *Vancouver Man Creeped Out by Drone Buzzing Near His 36th-Story Condo*, ARS TECHNICA (Aug. 20, 2014, 12:27 PM), http://arstechnica.com/tech-policy/2014/08/vancouver-man-creeped-out-by-drone-buzzing-near-his-36th-story-condo [http://perma.cc/5LS3-AXYS]; Benjamin Herold, *Lawsuit Alleges That Google Has Crossed a 'Creepy Line' With Student Data*, HUFFINGTON POST (Mar. 17, 2014, 2:49 PM), http://www.huffingtonpost.com/2014/03/17/google-data-mining-students_n_4980422.html [http://perma.cc/89LP-8QJX]; Sarah Halzack, *Privacy Advocates Try to Keep 'Creepy' 'Eavesdropping' Hello Barbie from Hitting Shelves*, WASH. POST (Mar. 11 2015), http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/11/privacy-advocates-try-to-keep-creepy-eavesdropping-hello-barbie-from-hitting-shelves [http://perma.cc/VB9R-NJBX].

10. Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J. L. & TECH. 59, 61 (2013-14).

11. *Id.* at 101.

12. RICHARDS, *supra* note 3, at 64-72.

13. *See* Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1521-22 (2010).

also contains overtones of creepiness. Nissenbaum suggests that privacy violations occur when "context-relative informational norms" are not respected when sharing information.[14] Her framework of contextual integrity suggests that "finely calibrated systems of social norms, or rules, govern the flow of personal information in distinct social contexts (e.g., education, health care, and politics)."[15] Individuals experience privacy violations when those social norms about information are violated in inappropriate ways.[16] Nissenbaum's theory has been highly influential among academics, and is starting to influence policy, with her work built into the Federal Trade Commission's updated approach to regulating privacy.[17] At the core of Nissenbaum's theory is her claim that we should consider privacy issues in the first instance when people react to new information practices by expressing "alarm."[18] In other words, although she does not use the term, something like creepiness in a particular context is the trigger for a potential privacy violation.

But there is a problem with creepiness, regardless of how carefully it is defined. It might be a very human and natural way to respond to new social or technological circumstances, but it ultimately tells us little about whether a legally cognizable privacy issue exists. At the outset, creepiness is over-inclusive as a proxy for information privacy threats. Lots of new technologies that might at first appear viscerally creepy will turn out to be either unproblematic or beneficial. Evan Selinger reminds us that early train passengers were not merely creeped out but terrified, fainting, and complaining of serious maladies from traveling at speeds that by today's standard would not constitute speeding in a school zone.[19] In the early days of the Internet, many users refused to buy products online, fearing security lapses from digital technologies they didn't understand.[20] Facebook's

---

14. NISSENBAUM, *supra* note 4, at 129; Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 155 (2004).

15. NISSENBAUM, *supra* note 4, at 3.

16. Nissenbaum, *supra* note 14, at 155.

17. Alexis C. Madrigal, *The Philosopher Whose Fingerprints Are All Over the FTCs New Approach to Privacy,* THE ATLANTIC (Mar. 29, 2012), http://www.theatlantic.com/technology/archive/2012/03/the-philosopher-whose-fingerprints-are-all-over-the-ftcs-new-approach-to-privacy/254365/ [http://perma.cc/FMH6-SKLK].

18. NISSENBAUM, *supra* note 4, at 3, 11. Nissenbaum's theory offers more than creepiness, but we note it here because it is (a) prominent and influential, and (b) its violation of "context-relative information norms" bears a close similarity to the what is colloquially deemed as "creepiness." As Nissenbaum's work on context becomes adopted by third-parties into regulation, and thus loses academic nuance, we predict that her nuanced philosophical treatment is likely to be folded in with colloquial "creepiness."

19. Evan Selinger, *Why Do We Love to Call New Technologies "Creepy"?*, SLATE (Aug. 22, 2012, 3:30 AM), http://www.slate.com/articles/technology/future_tense/2012/08/facial_recognition_software_targeted_advertising_we_love_to_call_new_technologies_creepy_.html [http://perma.cc/UZ9W-DZCH].

20. Ye Diana Wang & Henry H. Emurian, *An Overview of Online Trust: Concept, Elements, and Implications*, 21 COMPUTERS IN HUMAN BEHAVIOR 105 (2005), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.2184&rep=rep1&type=pdf [http://perma.cc/8TW9-AY5Y].

News Feed feature "creeped out" many users when it was first introduced because users were not accustomed to having all their information aggregated in one place for easy consumption.[21] Now the feature is considered to be fundamental both to the company's success and to the social awareness of many users of its network.[22]

But creepiness is also under-inclusive. New information practices that we don't understand fully, or highly invasive practices of which we are unaware, may never seem creepy, yet still present serious threats to values we care about. Take, for example, surveillance of which we are unaware,[23] or the use of secret algorithms to score our lives.[24] Such practices may unconstitutionally subject us to criminal or civil punishment (from jail time to designation on "no-fly" or "watch" lists), or they may deny us access to health, insurance, or economic opportunities (in the case of scoring by credit or university admissions algorithms). Such practices may be illegal, inaccurate, or both, but if they operate behind layers of secrecy, we may never learn about them. And things we are unaware of are unlikely to trigger the creepiness reaction.

Finally, because it rests on psychological reactions to perceived practices, creepiness is not only socially contingent, but malleable. A pervasive threat to privacy or our civil liberties can be made less creepy as we become conditioned to it. Such a threat may remain equally serious, but become normalized as we fit it into our understanding of the world in which we have to operate, like police corruption, sexism, or drunk drivers. Arguably, the Internet advertising industry, which relies on detailed surveillance of individual web-surfing to target ads, has fallen into this category.[25] Becoming "normal" in this way hardly removes the problem, even if we become accustomed or resigned to it. In the context of privacy, consider the ever-expanding reach of data collection, always pushing up against (and seeking to roll back or desensitize) the creepiness reaction. As Google's Eric Schmidt put it honestly in 2010, "Google policy is to get right up to the creepy line and not cross it."[26]

While it may be a natural psychological response to novelty, in the context of privacy law, creepiness is ultimately a trap. It locks us into a false binary of things that are *creepy* and thus potentially problematic, and things that are *not creepy* and thus presumably okay. Under the standard story, a finding of creepiness is only

---

21. danah boyd, *Facebook's Privacy Train Wreck*, 14 CONVERGENCE 13 http://www.danah.org/papers/FacebookPrivacyTrainwreck.pdf; Tiffany A. Pempek, Yevdokiya A. Yermolayeva, & Sandra L. Calvert. *College students' social networking experiences on Facebook,* 30 J. APPLIED DEV. PSYCH. 227 (2009).

22. Sam Biddle, *Facebook's New News Feed: The Biggest Change in Years*, GIZMODO (Mar. 7, 2013, 1:12 PM) http://gizmodo.com/5989228/facebooks-new-news-feed-the-biggest-change-in-years-updating-live [http://perma.cc/CAC8-2G95].

23. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013).

24. *See generally* FRANK PASQUALE, BLACK BOX SOCIETY (2015).

25. ANGWIN, *supra* note 7, at 4-5.

26. Shane Richmond, *Eric Schmidt: Google Gets Close to the "Creepy Line,"* TELEGRAPH (October 5, 2010), http://blogs.telegraph.co.uk/technology/shanerichmond/100005766/eric-schmidt-getting-close-to-the-creepy-line [http://perma.cc/5VZ4-BULW].

the start of the inquiry. Since some things that are creepy actually turn out to be desirable (recall the screaming Victorian train passengers and Facebook's News Feed), a creepy new technology begs a second question of whether something experienced as creepy is actually harmful. This fixation on harm is another major symptom of Privacy Pessimism, which we'll turn to now.

B. *The Harm Fixation*

A second pathology of Privacy Pessimism is that it is too focused on privacy's costs, often to the exclusion of any benefits. From this perspective, privacy is an injury to be remedied, a cost to be balanced in the ledger book, a harm rather than an opportunity. After all, goes the logic, we have to find out whether our sense of creepiness is actually a harmful one or just a false positive.

The Harm Fixation began with Warren and Brandeis, who were concerned about coverage of elite social functions by newspapers and by the new technology of "instantaneous photography." Worried that press coverage of intimate affairs and the circulation of unauthorized photos were causing psychological harm, they argued that the common law should recognize a tort to remedy these emotional injuries.[27]

Today's privacy law has expanded far beyond Warren and Brandeis's tort claims against the press. Modern privacy law is regulatory in scope, structuring data relationships in personal data and covering types of information and advanced technologies that nineteenth century lawyers might find indistinguishable from magic.[28] "Instantaneous photography" has nothing on Snapchat or GPS, and the Fair Credit Reporting Act and FTC investigations are much more complex and nuanced than a common law tort claim. But even though privacy law has evolved far from its origins in tort law, tort law's fixation on compensable individual harm has stubbornly remained with it, even when other elements of the law of torts have fallen by the wayside.

The Harm Fixation also manifests in the form of balancing tests used to decide whether certain information practices should be permissible or not. For example, Section 5 of the FTC Act, which outlaws unfair and deceptive trade practices, has become the most important piece of legislation for protecting consumer privacy in the United States.[29] But in order for a practice to be deemed unfair, it must be "likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[30]

---

27. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); RICHARDS, *supra* note 3, at 17.

28. This is of course Arthur C. Clarke's Third Law of Technology, first posited in Leigh Brackett, *The Sorcerer of Rhiannon*, ASTOUNDING, Feb. 1942, at 39.

29. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 588 (2014).

30. 15 U.S.C. § 45(n) (2013).

In privacy-related disputes, companies, agencies, and courts are asked to articulate whether the cost of acting fairly, in this instance to preserve privacy, is outweighed by the potential benefit to the consumer, which is often articulated as "cost savings passed on to the consumer."[31] The Obama White House's proposed "Consumer Privacy Bill of Rights" wholly embraces balancing privacy risks with other considerations.[32] It provides for a rulemaking procedure that considers "among other factors, the privacy risks posed by personal data processing by categories of persons of various sizes, experiences, resources, and types of commercial activity, including nonprofit activity; the importance of mitigating privacy risks; and the costs and benefits of including those categories of persons as covered entities."[33] This balancing requirement pits privacy and affordability against each other as values in conflict.

Companies, agencies, and courts are not the only privacy pessimists fixated on the cost of privacy. Critics of privacy regulation bemoan its toll on "innovation" and "progress."[34] Very few companies want to cause problems to people or hurt them, but focusing on the expense of privacy inevitably frames privacy as "the cost of doing business" instead of an opportunity to help form long-term, sustainable relationships.[35] Even advocates for privacy frequently consider privacy as a negative value that must be balanced against innovation, efficiency, or security. Responding to the framing of Privacy Pessimism, there is a large academic literature on "privacy harm" seeking to articulate exactly what the nature of the injury caused by threats to privacy.[36]

The Harm Fixation is thus problematic because it frames the privacy inquiry in negative, costly terms. But there is a second problem. The Harm Fixation also demands proof that is increasingly elusive.[37] In order to be actionable, all of the privacy torts demand a demonstration of harm that is "highly offensive to a reasonable person."[38] Those arguing against regulation of behavioral advertising assert that regulation is unnecessary because no harm from the practice can be

---

31. *See* Solove & Hartzog, *supra* note 29.

32. White House, ADMINISTRATION DISCUSSION DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT OF 2015 (Feb. 27, 2015), http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf [http://perma.cc/8SJ6-ND47] ("If a covered entity processes personal data in a manner that is not reasonable in light of context, the covered entity shall conduct a privacy risk analysis . . . to examine the potential for privacy risk. Covered entities shall take reasonable steps to mitigate any identified privacy risks, which shall include, but are not limited to, providing heightened transparency and individual control.").

33. *Id.*

34. *See, e.g.,* ADAM THIERER, PERMISSIONLESS INNOVATION (2014).

35. See Richards, *supra* note 1 (collecting examples).

36. *See, e.g.*, Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011); *see also,* Nathan Newman, *The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google*, 40 WM. MITCHELL L. REV. 849 (2014).

37. Calo, *supra* note 36.

38. RESTATEMENT (SECOND) OF TORTS §§ 652B-D (1977).

demonstrated.[39] Claims against companies for providing poor data security usually fail unless the plaintiff can demonstrate actual individualized harm, such as financial loss, instead of harms like uncertainty or increased risk shared across large numbers of people that are large in the aggregate but small for each affected individual.[40] The Supreme Court has taken a number of cases in recent years assessing whether allegations of harm are sufficient under the Federal Privacy Act,[41] and a pending case asks whether a private cause of action under the Fair Credit Reporting Act can ever satisfy Article III standing.[42] In these and other cases, the Supreme Court is increasingly interpreting privacy harm very narrowly.[43] State courts also routinely reject notions of privacy that are not immediately ascertainable or are speculative in nature.[44] Given the arc of decisions limiting notions of what constitutes privacy harm, an alternative focus would be useful.

Harm is, of course, an important concept in our law. It will remain a critical component in regulatory regimes that punish companies and provide redress through private causes of action for individuals, whether for identity theft, data breach, or revenge porn. It is an effective way of determining compensation amounts and separating important claims from trivial or meritless ones. But the goal of privacy law shouldn't *solely* be to avoid harm. Such a fixation is too rigid and focuses our attention away from important areas where privacy regulation can create value, rather than merely remedying injury.

While many laws are designed to deter harm, that is not the only function of law. Other laws, like tax regulations that provide incentives for charitable giving and consumer spending, are designed to encourage behavior that is seen as desirable within society.

The Harm Fixation forces us to come up with ill-fitting theories of harm

---

39. *See, e.g.*, Joel Rosenblatt, *Facebook Seeks Dismissal of $15 Billion Privacy Suit*, BLOOMBERG BUSINESS (Oct. 5, 2012, 11:06 AM), http://www.bloomberg.com/news/articles/2012-10-05/facebook-seeks-dismissal-of-15-billion-privacy-suit [http://perma.cc/67KN-GASC].

40. *See, e.g.*, Katz v. Pershing, LLC, 672 F.3d 64 (1st Cir. 2012) (finding no harm from increased risk of identity theft); Anderson v. Hannaford Bros. Co., 659 F.3d 151 (1st Cir. 2011); Holmes v. Countrywide Fin. Corp., No. 5:08–CV–00205–R, 2012 WL 2873892 (W.D. Ky. July 12, 2012) (rejecting theory of harm for time and efforts expended to deal with breach); Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046 (E.D. Mo. Nov. 23, 2009) (rejecting standing for increased risk of identity theft); Key v. DSW, Inc., 454 F. Supp. 2d 684 (S.D. Ohio 2006) (rejecting standing for increased risk of identity theft); Bell v. Acxiom Corp., No. 4:06CV00485-WRW, 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006) (rejecting theory of harm for increased risk of junk mail).

41. E.g., Doe v. Chao, 540 U.S. 614 (2004); Fed. Aviation Admin. v. Cooper, 132 S.Ct. 1441 (2012).

42. *See Spokeo v. Robins, Inc.*, SCOTUSBLOG, http://www.scotusblog.com/case-files/cases/spokeo-inc-v-robins/ [http://perma.cc/9YKM-HEJ3].

43. *See, e.g.*, Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1151 (2013) ("[R]espondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.").

44. *See, e.g.*, *Holmes*, 2012 WL 2873892; *Amburgy*, 671 F. Supp. 2d 1046; Key, 454 F. Supp. 2d 684; *McLoughlin*, 2009 WL 2843269; *Bell*, 2006 WL 2850042.

when we inevitably sense that there is a problem but cannot easily articulate a clear, cognizable, and individualized injury. Like an itch that can't be scratched or a problem that we just can't seem to put our finger on, this dimension of Privacy Pessimism paints us into a corner of narratives like "creepy" that sound compelling at first, but crumble in practice or under scrutiny.[45]

C. *The Control Illusion*

A third problem of Privacy Pessimism is its assumption that people can adequately make choices to protect their information. In the United States, privacy policy is largely centered on the idea that the best way to protect your privacy is to be careful about what and how much information you disclose and to whom. We have called this the *Control Principle,* though it is also called a "notice and choice regime" or "privacy self-management."[46]

When the FTC first started to regulate privacy in the late 1990s, it adopted a basic notice and choice regime for businesses that was congruous with many of the FIPs. As long as companies notified people about their information collection, use, and disclosure practices and gave them a choice to opt out (usually by not using the service), then companies were free to act in any way consistent with the notice given to consumers. The most salient example of this notice and choice regime is the ubiquitous privacy policy, that dense, unreadable, boilerplate text tucked away in some corner of virtually every website and application on the Internet.

In most cases that matter, the assumption that users have actual notice or meaningful choice is an illusion. Privacy self-management is increasingly recognized to be unworkable and possibly even a farce. There are many jokes about whether anyone reads privacy policies or Apple's infamously turgid Terms of Service agreement, but these jokes rest on the undeniable truth that privacy self-management is impossible. For example, one study by computer scientists found that if an ordinary Internet user were to quickly read every privacy policy they encountered over the course of a year, it would take them seventy-six working days to do so.[47] Another study by leading privacy journalist Julia Angwin revealed that it was practically impossible to opt-out of pervasive surveillance by governments and companies without practically opting out of society and human contact

---

45. *See, e.g.,* Tene & Polonetsky, *supra* note 10.

46. Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879 (2013); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

47. Alex C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, ATLANTIC (Mar. 1, 2012, 2:25 PM), http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851 [http://perma.cc/2ZJN-BYLA]; Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. POL'Y INFO. SOC'Y 543 (2009).

itself.[48] The Control Principle is the key element of American data regulation, but it is false.

When pressed on this point, federal regulators concede the futility of notice and the absence of real choice about the pervasive collection of personal data. The White House Privacy and Civil Liberties Oversight Board recognized as much in its long-awaited report on privacy and surveillance.[49] In its report on Big Data, the White House also repudiated the Control Principle, stating, "[t]he framework of notice and consent is also becoming unworkable as a useful foundation for policy."[50] Even the FTC has realized the limits of notice and choice.[51] The agency's report on protecting consumer privacy in the digital age acknowledged that "the emphasis on notice and choice alone has not sufficiently accounted for other widely recognized fair information practices, such as access, collection limitation, purpose specification, and assuring data quality and integrity."[52] Yet despite the acknowledgment that choice cannot do the work we ask of it, new proposals remain rooted in the Control Illusion. For example, the White House "Privacy Bill of Rights" released in February 2015 surprisingly remains rooted in a notice and choice view of the world.[53]

Such fixation on choice is especially problematic because the illusion of the Control Principle benefits the rich at the expense of the poor. AT&T's Internet service, for example, will let users opt out of a "supercookie" that monitors its users' habits for $29 a month.[54] Privacy then becomes merely a luxury good that

---

48. ANGWIN, *supra* note 7.

49. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (Jan. 23, 2014).

50. EXECUTIVE OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 46 (May 2014).

51. Julie Brill, Comm'r, Fed. Trade Comm'n, Keynote Address at Proskauer on Privacy 2 (Oct. 19, 2010), http://www.ftc.gov/sites/default/files/documents/public_statements/remarks-commissioner-julie-brill/101019proskauerspeech.pdf [http://perma.cc/CQH4-TA8R] ("[T]he Notice and Choice model, as it is often deployed today, places too great a burden on consumers."); Jon Leibowitz, Chairman, Fed. Trade Comm'n, Introductory Remarks at the FTC Privacy Roundtable 3 (Dec. 7, 2009), http://www.ftc.gov/sites/default/files/documents/public_statements/introductory-remarks-ftc-privacy-roundtable/091207privacyremarks.pdf [http://perma.cc/XCQ5-PXLW] ("We do feel that the approaches we've tried so far—both the notice and choice regime, and later the harm-based approach—haven't worked quite as well as we would like.").

52. Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 2 (2012), http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (also acknowledging the limits of privacy harm, stating "[t]he FTC's harm-based approach also has limitations. In general, it focuses on a narrow set of privacy-related harms—those that cause physical or economic injury or unwarranted intrusion into consumers' daily lives. But, for some consumers, the actual range of privacy related harms is much wider and includes reputational harm, as well as the fear of being monitored or simply having private information 'out there.'").

53. White House, *supra* note 32.

54. Sophia Cope & Jeremy Gillula, *AT&T is putting a price on privacy. That is outrageous,*

most people cannot afford. Thus, under the Control Illusion, users simply "choose" surveillance and the loss of privacy either because they cannot afford anything else, or because (as noted earlier) privacy harm is notoriously hard to calculate. Other times surveillance of everyday life just gets built into modern technologies, whether it is Samsung's "smart" TVs that record conversations in your living room, or Lenovo's laptops that shipped with insecure software that surveilled user web surfing in order to serve ads.[55]

The reality that the Control Principle is an illusion also provides an answer to one of the by-products of Privacy Pessimism, the so-called "privacy paradox." This is the idea that surveys consistently measure both consumer anxiety about privacy and behavior that is seemingly at odds with such concerns. Some commentators use the paradox to suggest that individuals are either hypocritical or ignorant.[56] But the privacy paradox is fallacious because it only considers one party in an information relationship: the user. Users given a blunt choice between protecting their data and participating in modern society really have no choice at all, especially when the terms of any such choice are clouded by confusing technology and legal mumbo-jumbo, where long-term interests in privacy are hard to value, or where meaningful choice is an illusion. In fact, given the limited notice and choice that most of us encounter, the privacy paradox suggests that users care about their personal data *in spite* of the limited legal and technological choices they face in protecting it.[57] If our revealed preferences show that we don't care about privacy, why do so many of us remain anxious about our personal data?

Ultimately, the Control Illusion reveals the limits of the procedural approach taken by the FIPs. For years, there was no privacy problem the FIPs purportedly could not fix. But doing so has worn out the concept amid the explosion of new data applications. Big Data has challenged the wisdom and practicality of data retention.[58] Profiling, discrimination, and other inferential harms happen so re-

---

GUARDIAN (Feb. 20, 2015, 12:09 PM), http://www.theguardian.com/commentisfree/2015/feb/20/att-price-on-privacy?CMP=fb_us [http://perma.cc/ZB2X-MZN6].

55. Parker Higgins, *Big Brother Is Listening: Users Need the Ability to Teach Smart TVs New Lessons*, ELEC. FRONTIER FOUND. (Feb. 11, 2015), http://www.eff.org/deeplinks/2015/02/big-brother-listening-users-need-ability-teach-smart-tvs-new-lessons [http://perma.cc/9YA9-EZPN]; Seth Rosenblatt, *Lenovo's Superfish Security Snafu Blows Up in its Face*, CNET (Feb. 20, 2015, 5:00 AM), http://www.cnet.com/news/superfish-torments-lenovo-owners-with-more-than-adware [http://perma.cc/WW29-PBVC].

56. Stuart N. Brotman, *Grappling with the Privacy Paradox*, BROOKINGS INST. (July 8, 2014, 7:30 AM), http://www.brookings.edu/blogs/techtank/posts/2014/07/8-brotman-privacy-paradox#.U7xJMEM6Z4M.twitter [http://perma.cc/A6ZC-MDKS]; Steve Lohr, *The Privacy Paradox, a Challenge for Business*, N.Y. TIMES (June 12, 2014, 2:12 PM), http://bits.blogs.nytimes.com/2014/06/12/the-privacy-paradox-a-challenge-for-business/?_php=true&_type=blogs&_r=0 [http://perma.cc/VGC2-LU4P]; Diane Brady, *Privacy Paradox: Americans Happy to Share Personal Data With Big Business*, BLOOMBERG BUSINESSWEEK (June 25, 2013), http://www.bloomberg.com/bw/articles/2013-06-25/privacy-paradox-americans-happy-to-share-personal-data-with-big-business [http://perma.cc/Z3LH-892E].

57. Richards, *supra* note 1 (suggesting the existence of such a "reverse privacy paradox.").

58. Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of*

motely from the source as to remove any doubt that the "choice" offered to users who disclose personal in the modern world is usually an illusion. After all, what choice can users have to opt out of profiling by ad networks and data brokers of whose existence they are unaware?

The FIPs have been whittled away to an empty shell in many areas of privacy law, especially the law protecting consumers in their Internet usage in the United States. In many areas, the FIPs have become little more than a set of procedural protections lacking a substantive theory of what privacy is and why it matters. From this perspective, it should be no wonder why so many people are pessimistic about privacy.[59]

***

Behold, then, the traditional story we tell ourselves about privacy, a story we have called "Privacy Pessimism." Privacy is under threat from new technologies and business practices that we perceive as "creepy." When we encounter a creepy privacy practice, tort law has trained us to see if there is any harm. Yet in many instances, regardless of the harm, we feel like our consent is being wrongly manufactured using fine print and malicious design. The Harm Fixation limits our ability to think about what privacy can do for us, while the fiction of the Control Illusion manufactures consent through the operation of the FIPs.

Privacy Pessimism is reactive, negative, and largely ineffective at protecting individuals in information relationships. It is worn out. If privacy law is to survive, if ordinary people are to have any meaningful participation in when, whether, and how their data is being used, some positive articulation of what good privacy can do is necessary. We offer such a theory in the next Part.

III. A THEORY OF PRIVACY AND TRUST

Getting past privacy's pessimism problem requires companies and confidants to recognize that protecting the privacy of others is mutually beneficial. Businesses, intermediaries, carriers, and intimates must *want* privacy for articulable reasons beyond moral or ethical concerns. Without articulable benefits to recipients of personal information, we will never escape Privacy Pessimism.

Our current set of ground rules about what kinds of data uses are permissible will not create a sustainable digital society. To remedy this problem, we offer a new theory of privacy and trust. Put simply, privacy matters because it enables trust. Privacy rules can govern the uses of information in relationships, and these rules can build trust. Trust-promoting privacy rules allow people to safely disclose personal information in ways that benefit not just individuals, but the entities they share their data with as well. Understanding how privacy rules can promote trust goes beyond the Harm Principle. Instead of remedying speculative harm,

---

Analytics, 11 NW. J. TECH. & INTELL. PROP. 239 (2013).

59. *See* Richards, *supra* note 1, at 59 ("[T]he available evidence suggests that people do in fact care about privacy, but they are bewildered by the difficulty of protecting their personal information in a time of rapid technological change and limited options.").

privacy can promote trust and promise a way forward for the safe and equitable collection, use, and disclosure of information in long-term, sustainable relationships. Similarly, trust mitigates the problems and distrust that stem from the Control Illusion. From this perspective, privacy isn't a paradox, it is essential to our digital future. It's not a drain on progress, but rather a signpost to the way forward.

D. *Conceptualizing Trust*

Trust is an essential component of healthy relationships and healthy societies.[60] Although various disciplines define trust in various ways, at bottom, "trust is a state of mind that enables its possessor to be willing to make herself vulnerable to another—that is, to rely on another despite a positive risk that the other will act in a way that can harm the truster."[61] Trust allows cooperation with other people in spite of the fact that exposing ourselves enables them to harm us.

There is a vast literature on trust across a variety of academic disciplines, from social sciences like political science and psychology to fields as wide-ranging as medicine, management, and neuroscience.[62] There is also substantial legal

60. *See, e.g.,* FRANCIS FUKUYAMA, TRUST: THE SOCIAL VIRTUES AND THE CREATION OF PROSPERITY 26 (1995); Diego Gambetta, *Can We Trust Trust?*, *in* TRUST: MAKING AND BREAKING COOPERATIVE RELATIONS 217 (Diego Gambetta ed., 1988); PIOTR SZTOMPKA, TRUST: A SOCIOLOGICAL THEORY 25 (1999); THE WESTMINSTER DICTIONARY OF CHRISTIAN ETHICS 632 (James F. Childress & John Macquarrie eds., 1986); Margaret M. Blair & Lynn A. Stout, *Trust, Trustworthiness, and the Behavioral Foundations of Corporate Law*, 149 U. PA. L. REV. 1735, 1745-46 (2001); Eli Bukspan, *Trust and the Triangle Expectation Model in Twenty-First Century Contract Law*, 11 DEPAUL BUS. & COM. L.J. 379, 415 (2013).

61. Claire A. Hill & Erin Ann O'Hara, *A Cognitive Theory of Trust*, 84 WASH. U. L. REV. 1717, 1723-24 (2006) (citing Denise M. Rousseau et al., *Not So Different After All: A Cross-Discipline View of Trust*, 23(3) ACAD. MGMT. REV. 393, 394-395 (1998)). *See also* FUKUYAMA, *supra* note 60; Gambetta, *supra* note 60; Frank B. Cross, *Law and Trust*, 93 GEO. L.J. 1457, 1461 (2005); Sirkka L. Jarvenpaa & Emerson H. Tiller, *Customer Trust in Virtual Environments: A Managerial Perspective*, 81 B.U. L. REV. 665, 677-78 (2001).

62. KENNETH J. ARROW, THE LIMITS OF ORGANIZATION (1974); BERNARD BARBER, THE LOGIC AND LIMITS OF TRUST (1983); Morton Deutsch, *Cooperation and Trust: Some Theoretical Notes*, *in* 10 NEBRASKA SYMPOSIUM ON MOTIVATION 275 (1962); Gambetta, *supra* note 60; RUSSELL HARDIN, TRUST AND TRUSTWORTHINESS (2002); Jack Knight, *Social Norms and the Rule of Law: Fostering Trust in a Socially Diverse Society*, *in* TRUST IN SOCIETY 354 (Karen S. Cook ed., 2001); PAUL SEABRIGHT, THE COMPANY OF STRANGERS: A NATURAL HISTORY OF ECONOMIC LIFE (2004); TRUST IN ORGANIZATIONS: FRONTIERS OF THEORY AND RESEARCH (Roderick M. Kramer & Tom R. Tyler, eds., 1996); Philip Worchel, *Trust and Distrust*, *in* THE SOCIAL PSYCHOLOGY OF INTERGROUP RELATIONS 174 (William G. Austin & Stephen Worchel eds., 1979); Mark A. Hall et al., *Measuring Patients' Trust in Their Primary Care Providers*, 59 MED. CARE RES. & REV. 293 (2002); Hill & O'Hara, *supra* note 61, at 1796; Brooks King-Casas et al., *Getting to Know You: Reputation and Trust in a Two-Person Economic Exchange*, 308 SCI. 78 (2005); Michael Kosfeld et al., *Oxytocin Increases Trust in Humans*, 435 NATURE 673 (June 2, 2005); Kevin A. McCabe & Vernon L. Smith, *A Comparison of Naïve and Sophisticated Subject with Game Theoretic Predictions*, 97(7) PROC. NAT'L ACAD. SCI. 3777 (2000); *Special Topic Forum on Trust In and Between Organizations*, 23 ACAD. MGMT. REV. 393 (Denise M. Rousseau et al. eds., 1998); *See also* Julian B. Rotter, *Interpersonal Trust, Trustworthiness, and Gullibility*, 35 AM. PSYCHOL. 1, 1 (1980) ("Common sense tells us that interpersonal trust is an important variable affecting human relationships at all lev-

scholarship on the role of the law in general in generating or discouraging trust,[63] as well as in such sub-disciplines as contracts, corporations, and the law of fiduciary duties.[64] Our purpose in this paper is not to advance a theory of trust for all purposes or even all purposes in the law. Our goal is more modest. While we recognize and draw from the vast scholarly literature on trust, we have no wish to enter academic debates other than how we should think about privacy rules in a digital society, for that problem is large enough.

We offer instead a theory of trust in the context of information relationships that allows us to better understand why legal, technological, and social rules regulating the collection, uses, and flows of information in those relationships can make us all better off.[65] Put simply, privacy rules are necessary to build the trust our digital society needs not merely to function sustainably over the long term, but also to flourish. There have been occasional references to trust in the scholarship on law, technology, and privacy, but trust has failed to develop as a core justification for why privacy matters.[66] In this paper, we make exactly that case: that thinking of privacy in terms of trust is essential, and that trust must become an essential part of the legal conversations about data, innovation, technology, and privacy.

In the context of information relationships, trust means the willingness to become vulnerable to a person or organization by disclosing personal infor-

---

els . . . ."); Tom R. Tyler, *Trust and Law Abidingness: A Proactive Model of Social Regulation*, 81 B.U. L. REV. 361, 362 (2001); Russell Hardin, *Distrust*, 81 B.U. L. REV. 495, 496 (2001); Justin (Gus) Hurwitz, *Trust and Online Interaction*, 161 U. PA. L. REV. 1579 (2013).

63. Hill & O'Hara, *supra* note 61, at 1720; Tamar Frankel and Wendy J. Gordon, *Symposium: Trust Relationships*, 81 B.U. L. REV. 321 (2001); Tyler, *supra* note 62.

64. *See, e.g.* CHARLES FRIED, CONTRACT AS PROMISE: A THEORY OF CONTRACTUAL OBLIGATION (1981); Blair & Stout, *supra* note 60 at 1738 ("We contend that people often trust, and often behave trustworthily, to a far greater degree than can possibly be explained by legal or market incentives."); John J. Chung, *Promissory Estoppel and the Protection of Interpersonal Trust*, 56 CLEV. ST. L. REV. 37, 38-39 (2008).

65. A very small number of legal scholars have suggested that trust might be important in privacy disputes. Indeed, this is a claim that each of us has made in prior work. *See* Richards, *supra* note 1; RICHARDS, *supra* note 3. In a forthcoming article, Ari Waldman draws on the work of sociologists to argue that sociological notions of trust are broader than the "everyday trust" we have in our friends and family members. Waldman concludes from this analysis that privacy and trust are the same thing. Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in the Twenty-First Century*, 69 U. MIAMI L. REV. 559, 629. While we agree with Waldman that modern understandings of privacy fail to account for trust, we disagree with him to the extent that he thinks trust and privacy are just synonyms for each other. In our view, privacy and trust are distinct concepts, and trust is an important end that privacy law can serve. Privacy rules—rules governing the treatment of personal information—can serve many purposes, not just remedying the harms of Privacy Pessimism, but protecting our civil liberties, *see* RICHARDS, *supra* note 1, and a whole host of other goals. *See, e.g.*, DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2009). Rather than bind all of privacy law to the mast of trust, for the reasons we give in this article, we think it is sufficient (and more nuanced) to argue that rules governing personal data in information relationships are trust-promoting, and that this function is essential for the kind of sustainable digital society we should want to build.

66. *See, e.g.* Hurwitz, *Trust and Online Interaction*, *supra* note 62; Helen Nissenbaum, *Securing Trust Online: Wisdom or Oxymoron*, 81 B.U. L. REV. 635 (2001); Waldman, *supra* note 65.

mation. Some terminology is necessary to aid in precision. We will refer to disclosers of this personal information as *trusters*, the act of sharing sensitive personal information as *entrusting*, and the recipient of such information as *entrustees*. While the natural term for one entrusted with personal information is a "trustee," we are mindful of the specific meaning of this term within, for example, fiduciary and estate law. We will use the term "entrustee" for greater precision, but we are also mindful that the power of an information recipient to harm another is part of the historical basis for the imposition of a trustee relationship in the law of fiduciaries.[67] The difference between an "entrustee" and a "trustee" may be negligible in practice. We nevertheless want to separate them because an "entrustee" is a factual description ("someone has entrusted their data with me . . ."), while becoming a "trustee" means the imposition of legal obligations (". . . and the law requires me as her Trustee to treat it a certain way").

Let us illustrate how these terms work in practice. We are all trusters at various times. As trusters, we share data by entrusting it with entrustees. A truster can be a bank customer, the user of a search engine, or a customer at Target. In these cases, the entrustee is the bank, the search engine, or the big box retailer, and the information being entrusted can be financial data, search queries, or information about the consumer's purchases.

When trusters entrust information about themselves, they make themselves vulnerable. Their vulnerability might include increased risk of information misuse, unauthorized disclosure, manipulation, or loss of autonomy. A bank could leave their account numbers on a laptop in an airport.[68] A search engine could turn their queries over to the government[69] or the general public.[70] Target could guess that they are pregnant and market to them at their time of vulnerability,[71] or Target could itself be the victim of a data breach.[72] The possibilities for disclosure, injury, or manipulation in such cases are limited only by the human potential for innovation. Once a truster's information is disclosed, she no longer has sole control over its use and dissemination.[73] She is exposed and at the mercy of

67. *See* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 135 (2007).

68. *See, e.g.*, Resnick v. AvMed, Inc., 693 F.3d 1317 (11th Cir. 2012); *see also* Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018 (D. Minn. 2006).

69. *See, e.g.*, Gonzales v. Google, Inc., 234 F.R.D. 674 (N.D. Cal. 2006).

70. *See, e.g.*, Michael Barbaro & Tom Zeller Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES (Aug. 9, 2006), http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all [http://perma.cc/Y2YL-DJQQ].

71. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all [http://perma.cc/TPV6-WNGY].

72. *A Message from CEO Gregg Steinhafel about Target's Payment Card Issues*, TARGET (Dec. 20, 2013), http://corporate.target.com/discover/article/Important-Notice-Unauthorized-access-to-payment-ca [http://perma.cc/9S7W-J8ZG].

73. Woodrow Hartzog, *Chain-Link Confidentiality*, 46 GA. L. REV. 657, 658 (2012) ("[I]ndividuals lose control of their personal information once they disclose it on the Internet.").

the entrustee.

When people disclose personal details within information relationships, two distinct kinds of vulnerabilities occur. The first is vulnerability to actions by the trustee. One of us has written regarding surveillance that "information gives the watcher increased power over the watched that can be used to persuade, influence, or otherwise control them."[74] The same is true within information relationships. Employees can be immediately fired, insurance can be denied, friends can be embarrassed, lovers can be devastated by the disclosure of secrets or sexy photos. Increasingly, Internet users can be manipulated by technological design guided by companies with an intimate knowledge of their background and preferences. If you know your customers well, it is much easier to nudge them into doing what you want them to do, even when it is a choice they might not otherwise have made freely.[75]

A second kind of vulnerability faced by trusters is to third parties who receive the personal information from the entrustee. This can happen when the entrustee sells or rents the data "downstream," or it can happen when the entruster's security is breached by a true third party. An ISP might sell web-surfing habits to an advertising company or data broker.[76] Any retailer, data broker, or other entity might get hacked by online criminals.[77] When trusters intentionally or unintentionally disclose entrusted information to others, entrustees can be manipulated, user profiles can be impersonated, reputations can be destroyed, and bank accounts can be cleaned out.

Virtually every disclosure of personal information in the modern age leaves the discloser vulnerable in some way, if even only incrementally. As a result, every information relationship involves some degree of trust, or willingness to become vulnerable. This is true even if that trust is not a conscious one on the part of the truster.[78] The phenomenon of trust exists in all information relationships, though of course to different degrees. The key, then, is determining which information relationships require extra scrutiny from the law.

E. *Why Trust Matters in Information Relationships*

Because disclosure of personal data leaves people vulnerable, trust is the glue that holds together virtually every information relationship. An information relationship is any relationship that requires personal information to develop or

---

74. Richards, *supra* note 23, at 1956.

75. Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014); Duhigg, *supra* note 71.

76. Natasha Singer, *Your Online Attention, Bought in an Instant*, N.Y. TIMES (Nov. 17, 2012), http://www.nytimes.com/2012/11/18/technology/your-online-attention-bought-in-an-instant-by-advertisers.html?pagewanted [http://perma.cc/D6DA-C3C6].

77. Michael Riley et al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG BUS. (Mar. 13, 2014), http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data [http://perma.cc/6C67-758Y].

78. Cross, *supra* note 61, at 1459; Hill & O'Hara, *supra* note 61, at 1721-22.

achieve a particular goal. This includes a person's relationship with merchants, doctors, employers, common carriers, intermediaries, friends, and intimate partners.[79] And in practice, privacy rules—rules governing the uses of personal information—are essential requirements for the existence of these trust-dependent relationships in the first place.

Trust in these relationships produces numerous benefits, but three are particularly worth highlighting. These three values—commerce, social interaction, and free expression—cannot exist without a willingness to become vulnerable to the actions of others.

Commerce. Commercial relationships, the engine of any economy, are entirely a product of trust. Without this trust, our modern way of life simply would not exist. When privacy is conceptualized as trust, it becomes clear how privacy can be essential for business.[80] If consumers cannot trust businesses with information, they will be hesitant to buy goods and services that require information relationships. Online commerce is particularly reliant upon trust.

Trust is essential to nearly every component of commerce, not just aspects involving privacy and personal information. Trust in commerce begins with the most common initiator of a commercial exchange—a promise which leads to a contract.[81] As first-year law students learn, the most important tool in commerce, the contract, is essentially a mechanism for encouraging and protecting trust.[82]

---

79. *See, e.g.*, Avner Ben-Ner & Louis Putterman, *Trusting and Trustworthiness*, 81 B.U. L. REV. 523, 523 (2001); Cross, *supra* note 61, at 1459; *see also* G. Richard Shell, *Opportunism and Trust in the Negotiation of Commercial Contracts: Toward a New Cause of Action*, 44 VAND. L. REV. 221, 265 (1991); *cf.* Hurwitz, *supra* note 62 (discussing the vital role of trust between Internet users, Internet intermediaries, and the architecture of the Internet itself); Andrew J. McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality*, 74 U. CIN. L. REV. 887, 913 (2006); Joel Reidenberg & Francoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in the Network*, 30 WAKE FOREST L. REV. 105 (1995); Larry E. Ribstein, *Law v. Trust*, 81 B.U. L. REV. 553, 554-55 (2001); Ethan J. Leib, *Friends As Fiduciaries*, 86 WASH. U. L. REV. 665, 673 (2009).

80. Nicole Ozer, *Privacy and Free Speech: It's Good for Business*, ACLU CAL. (2d ed. 2012), http://www.americanbar.org/content/dam/aba/events/labor_law/2013/04/aba_national_symposiumontechnologyinlaboremploymentlaw/2_conley.authcheckdam.pdf [http://perma.cc/L45X-5DQK].

81. Bukspan, *supra* note 60, at 382-83. Bukspan notes how "[t]he idea of interpersonal trust has personal, social, moral, psychological, and utilitarian advantages that are consistent with common sense and easily relatable. Thus, it comes as no surprise that interpersonal trust has been adopted into many fields, particularly social and economic fields. From a social perspective, trust is understood as a vital element in the relationship between people." *Id.* Buskpan argued that trust is an essential ingredient for commerce, stating: "Mutual trust is a tool that is used to avoid economic pitfalls . . . . [I]nterpersonal trust promotes cooperation and contributes to economic performance in large organizations." *Id.*; *see also* Cross, *supra* note 61, at 1460 ("There is evidence that legal regulation strengthens securities markets around the world. Because investment in corporate equity requires at least a modicum (and sometimes a great deal) of trust, this evidence suggests the positive effect of the law. Other international evidence shows the benefit of the law and contracts on overall economic growth, providing more evidence that law is associated with greater trust.").

82. Anthony J. Bellia Jr., *Promises, Trust, and Contract Law*, 47 AM. J. JURIS. 25, 25-26 (2002) ("By making a promise, a person invites another to trust, and to break a promise is to

While trust has not been fully embraced in regulatory conversations about privacy, it has played a critical role in commerce and consumer protection. Kenneth A. Bamberger and Deirdre K. Mulligan's research into the practices of corporate privacy officers revealed that "promoting consumer trust, rather than protecting individual privacy, motivates many recent privacy interventions."[83]

Intimacy. People simply cannot be close to each other without trusting others with personal information, which is often deeply sensitive. We trust those we love by revealing ourselves (sometimes quite literally). We expose our hopes and fears, our wishes and secrets, our body parts, and our desires to intimates, trusting that they will not reveal what we have shown and told them to others. Most especially, we trust that they will be loyal with our confidences and will not use what they have learned against us.

Trust is an essential component for friendship as well. Friends share basic kinds of information such as hobbies, opinions, and jokes. But true friendship is based upon much more personal disclosures and experiences. Psychologists Irwin Altman and Dalmas Taylor have shown that the strength of relationships is based upon the frequency of reciprocal personal disclosure and degree of vulnerability that reciprocal disclosure creates.[84] In other words, the quality of friendships is defined by the extent to which we trust each other with personal disclosures.[85] Altman's theory of privacy as a boundary regulation process works with his social penetration theory to establish that privacy is "selective control of access to the

---

abuse that trust."). Bellia noted that many theorists have argued that "in order to maximize aggregate preferences, one must have some incentive to rely on certain promises. The incentive to rely on a promise exists only to the degree that a promise is trustworthy." *Id.* Bellia summarizes the theorists who claim that the role of contract is essentially "to protect the ability of individuals to trust promises in circumstances in which that trust is socially beneficial." *Id.* at 28 ("In many contexts, it is the enforceability of promises that creates possibilities for relationships of lesser trust to ripen into relationships of greater trust."); *see also* Bukspan, *supra* note 60, at 379 ("The concept of trust best explains the true nature of contract law and is found in key contract-law doctrines, such as good faith and public policy.").

83. Bamberger & Mulligan, *supra* note 6, at 260. According to Bamberger and Mulligan, "[t]he language of 'trust,' and the connection between privacy and consumer protection, first arose on the global stage during the early days of the commercial Internet." *Id.* at 279. Bamberger and Mulligan found that trust was truly the impetus for companies who sought to protect privacy. The privacy leaders they interviewed as part of their research equated privacy to trust and respect for people, even if they had difficulty articulating what trust rules should look like. *Id.* at 283 ("The link between privacy, trust, and commerce was underscored by repeated consumer pushback after corporate privacy blunders. Companies announced information-sharing deals only to cancel them once masses of consumers made their objections known.")

84. IRWIN ALTMAN & DALMAS A. TAYLOR, SOCIAL PENETRATION: THE DEVELOPMENT OF INTERPERSONAL RELATIONSHIPS (1973); Irwin Altman, *Reciprocity of Interpersonal Exchange*, 3 J. THEORY SOC. BEHAVIOUR 249 (1973); Dalmas A. Taylor, *The Development of Interpersonal Relationships: Social Penetration Processes*, 75 J. SOC. PSYCH. 79 (1968); *see also* STEPHEN LITTLEJOHN, THEORIES OF HUMAN COMMUNICATION 250 (2002) (describing social penetration theory as "[t]he idea that relationships become more intimate over time when partners disclose more and more information about themselves").

85. Altman, *Reciprocity of Interpersonal Exchange*, *supra* note 84; Taylor, *The Development of Interpersonal Relationships: Social Penetration Processes*, *supra* note 84.

self."[86] This insight might seem intuitive, but it has yet to be fully incorporated into a policy that promotes trust in the interests of establishing and maintaining friendship and intimacy.[87]

This theory helps us understand why we disclose even more information on social media when we have privacy settings.[88] At first, the research around privacy settings confused us. Why would those that are contentious enough about privacy to employ privacy settings actually share more information? The reason is that people disclose more when they trust. When they believe that the other party is trustworthy, they are more likely to share, just as they do with their doctors, lawyers, and spiritual advisors. When control is not an illusion, trusted sharing can occur. Privacy is thus not merely an interest for selfish users. Contrary to the mantra of Dave Eggers' fictitious social network "The Circle" in his novel of the same name, privacy is not theft.[89] Instead, it is good for businesses like social media that need users to share with friends in order to be considered successful. Trust enables the strong relationships that make sustainable digital business possible.

Expression. Finally, trust within information relationships is critical for free expression and a precursor to many kinds of political engagement. We have become used to talking about the Internet purely in the economic language of the

---

86. IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR: PRIVACY, PERSONAL SPACE, TERRITORY, CROWDING (1975); Stephen T. Margulis, *On the Status and Contribution of Westin's and Altman's Theories of Privacy*, 59 J. SOC. ISSUES 411, 412 (2003). Other scholars have built upon Altman's concept to theorize that disclosure happens only when we trust that the information is safe within an outer boundary. SANDRA PETRONIO, BOUNDARIES OF PRIVACY (2002); Valerian J. Derlega & Alan L. Chaikin, *Privacy and Self-Disclosure in Social Relationships*, 33 J. SOC. ISSUES 102 (1977); Leysia Palen & Paul Dourish, *Unpacking "Privacy" for a Networked World*, CHI '03 PROC. ACM SIGCHI CONF. ON HUM. FACTORS COMPUTING SYS., Apr. 5-10, 2013, at 129, 130; Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 919-20 (2005).

87. *See generally* ETHAN LEIB, FRIEND V. FRIEND: THE TRANSFORMATION OF FRIENDSHIP AND WHAT THE LAW HAS TO DO WITH IT (2011); Leib, *supra* note 79, at 670 ("We should accept close friendship as triggering certain fiduciary duties. Courts have already started to treat friends as fiduciaries—and there is much that can be appreciated about friendship itself when friends begin to see their relationships through the lens of the fiduciary concept."); *see also* Ethan J. Leib, *Contracts and Friendships*, 59 EMORY L.J. 649, 652 (2010).

88. Laura Brandimarte, Alessandro Acquisti & George Loewenstein, *Misplaced Confidences: Privacy and the Control Paradox*, http://www.futureofprivacy.org/wp-content/uploads/2010/09/Misplaced-Confidences-acquisti-FPF.pdf [http://www.futureofprivacy.org/wp-content/uploads/2010/09/Misplaced-Confidences-acquisti-FPF.pdf]; *see also* Fred Stutzman, Ralph Gross & Alessandro Acquisti, *Silent Listeners: The Evolution of Privacy and Disclosure on Facebook*, 4 J. PRIVACY & CONFIDENTIALITY 7 (2012); Maritza Johnson, Serge Egelman & Steve Bellovin, *Facebook and Privacy: It's Complicated*, SYMP. ON USABLE PRIVACY AND SECURITY, July 11-13, 2012, http://www.guanotronic.com/~serge/papers/soups12-facebook.pdf [http://perma.cc/37EQ-MC2T]; Somini Sengupta, *Study: Facebook Users More Protective Even as They Reveal More About Themselves*, N.Y. TIMES (Mar. 5, 2013), http://bits.blogs.nytimes.com/2013/03/05/study-facebook-users-more-protective-even-as-they-reveal-more-about-themselves [http://perma.cc/98QB-ZKRU].

89. DAVE EGGERS, THE CIRCLE (2013).

market. From this perspective, Internet users are consumers rationally maximizing their preferences. But the Internet has long been a forum for political engagement and free speech, and it was such well before the "dot-com" era and the rise of the surveillance economy turned the Internet into a shopping mall as well. It remains a source of political fundraising,[90] political information,[91] and political activism.[92] The Internet's consumers are also citizens, and the way their access to information is structured has enormous effect on political debate and the political process more generally.

The architecture of the Internet relies upon our ability to trust each other in routing communications.[93] People must also be able to trust recipients with possibly controversial ideas that are not yet fully formed. Thus, as a practical matter, people need to be able to rely upon intermediaries and recipients to engage politically and further the free speech ideals of self-development, self-governance, government accountability, and the search for truth. Trust is not only necessary to protect our economic interests; it is an essential component of our political rights and civil liberties. Without privacy rules promoting trust in digital systems, even freedom of speech is imperiled.

In our lifetimes, communication technologies based upon paper have increasingly been supplemented or even replaced by digital forms; emails have replaced letters, websites have replaced newspapers, and electronic books (and books ordered over the Internet) have begun to rival those sold in bookstores for market share. These digital technologies have been a force for good, expanding both our access to knowledge and our practical ability to engage in free expression. But while our digital technologies expand our reach, they are capable of monitoring our reading, thinking, and private communications in ways that would be impossible for paper-based technologies. Whenever we shop, read, speak, and think, we now do so using computers that create records of these activities.[94]

Our ISPs, for example, have records of every web site we visit—a virtual transcript of our intellectual explorations, of our reading and thinking. Consider further all the searches you may have entered into Google's search box, or everything

---

90. Aaron Smith, *The Internet's Role in Campaign 2008*, Pew Research Center, Apr. 15, 2009, http://www.pewinternet.org/2009/04/15/the-internets-role-in-campaign-2008 [http://perma.cc/MZT5-FPPE].

91. Amy Mitchell et al., *Political Polarization and Media Habits*, Pew Research Center, Oct. 21, 2014, http://www.journalism.org/2014/10/21/political-polarization-media-habits [http://perma.cc/H78D-MDH8]; Amy Mitchell, *State of the News Media 2014*, , Pew Research Center, March 26, 2014, http://www.journalism.org/2014/03/26/state-of-the-news-media-2014-overview [http://perma.cc/37ZU-XGAS].

92. Yochai Benkler et al., *Social Mobilization and the Networked Public Sphere: Mapping the SOPA-PIPA Debate*, Berkman Center Research Paper No. 2013-16 (July 19, 2013).

93. Hurwitz, *supra* note 62, at 1580 ("From its inception in the 1960s through commercialization in 1993, the Internet was a relatively simple network that was designed, constructed, and used by a relatively small community of research and governmental institutions with broadly aligned incentives . . . [E]ven as these institutions gave way to diverse commercial interests, trust remained an organizing principle").

94. RICHARDS, *supra* note 3, at 1.

you have said on the phone. Many powerful but shadowy entities, from data brokers to the National Security Agency, have shown an interest in our intellectual records—our reading habits, surfing habits, and private communications. Such activities threaten our intellectual privacy, the protection from surveillance or interference when we are engaged in the processes of generating ideas—thinking, reading, and speaking with confidantes before our ideas are ready for public consumption.

Surveillance or interference of our reading and thinking can drive our beliefs to the average, the mainstream, and the boring. Many studies document the often substantial deterrent effects of surveillance on criminal activity, from employee theft[95] to misbehavior by police.[96] But in a free society surveillance can have a substantial chilling effect on thought, reading habits, and private speech. Recent studies, for example, demonstrate that the Snowden revelations produced a chilling effect on Google searches, in areas not merely related to national security, but also things that were unrelated to the NSA's dragnet, like divorce lawyers, mental illness, and weight loss.[97] Another study suggested that surveillance makes writers and journalists more likely to self-censor.[98]

As a society, we say frequently that we care about individuality, diversity, eccentricity, and the vibrant weirdness that freedom makes possible. If we don't have intellectual privacy, all of these important values that make life worth living are threatened. But rules protecting intellectual privacy can safeguard the trust in our digital tools to enable fearless and unfettered intellectual exploration and private communication. This is a reality that librarians recognized decades ago, when they established both professional duties and legal requirements protecting the privacy and confidentiality of patron records.[99] Today librarians remain among the most trusted information professionals.[100]

Intellectual privacy rules produce the trust in digital systems that enables engagement with ideas, political association, and truly free speech to flourish. From this perspective, trust-promoting privacy rules serve not merely economic values, but those of a constitutional magnitude as well. Trust is essential for the kind of society we want to live in. To review, trust drives commerce and it creates the conditions for intimacy and free expression. If we want to flourish as humans, we must be able to trust each other.

---

95. Lamar Pierce et al., *Cleaning House: The Impact of Information Technology Monitoring on Employee Theft and Productivity,* MIT Sloan Research Paper No. 5029-13 (Oct. 15, 2014).

96. *See generally*, Richards, *supra* note 23 (collecting examples).

97. Alex Marthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior*, SSRN (Apr. 29, 2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564.

98. *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*, PEN America (Nov. 12, 2013), http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf [http://perma.cc/S27M-7R3U].

99. Neil M. Richards, *The Perils of Social Reading*, 101 GEO. L. J. 689 (2013).

100. Maureen Sullivan et al., *Librarians Working Together*, American Libraries Magazine, (June 25, 2013), http://americanlibrariesmagazine.org/2013/06/25/librarians-working-together [http://perma.cc/PE6E-3435].

IV. REJUVENATING PRIVACY LAW THROUGH TRUST

Privacy law's legacy of harm and control has left our privacy torts useless and the FIPs threadbare. Privacy law is not just pessimistic. It is worn out. In this Part, we show how trust can rejuvenate privacy law and policy.

First, trust can add nuance and force to foundational privacy concepts such as confidentiality, transparency and security by reimagining them as discretion, honesty, and protection. In addition to rejuvenating old privacy concepts, we introduce loyalty as a foundational concept in privacy law. We argue that entrustees have a duty to avoid unreasonable and dangerous self-dealing. These concepts are not new. They are foundations of one of the most established legal concepts involving trust in relationships: the law of fiduciaries.

A. *Relying on Fiduciaries*

The best place to look for wisdom on how to secure trust is from relationships that are defined by trust—fiduciaries. Fiduciaries are an ancient concept in the common law, and the central goal of fiduciary law is to protect against the exploitation of a vulnerability created by trust in another.[101] From this perspective, fiduciary relationships are the paradigm case for law enabling trust by imposing duties such as care, loyalty, and confidentiality. It should thus be no surprise that most if not all fiduciary relationships also fit within the larger category we have been calling "information relationships."

A few prominent privacy and cyberlaw scholars have also suggested that privacy law might take cues from the law of fiduciaries. Jack Balkin has proposed looking to the law of fiduciaries in the privacy context, explaining that "[t]he concept of an information fiduciary helps us understand how we might protect digital privacy while not running afoul of the First Amendment. . . . Traditionally, a fiduciary is a person who has a relationship of trust with a party (the beneficiary), and who is authorized to hold something valuable—for example—the beneficiary's

101. Leib, *supra* note 79, at 732; J.C. SHEPHERD, THE LAW OF FIDUCIARIES (1981); Robert C. Clark, *Agency Costs Versus Fiduciary Duties*, in PRINCIPALS AND AGENTS 55 (John W. Pratt & Richard J. Zeckhauser eds., 1985); Robert Cooter & Bradley J. Freedman, *The Fiduciary Relationship: Its Economic Character and Legal Consequences*, 66 N.Y.U. L. REV. 1045 (1991); Kenneth B. Davis, Jr., *Judicial Review of Fiduciary Decisionmaking—Some Theoretical Perspectives*, 80 NW. U. L. REV. 1 (1985); Deborah A. DeMott, *Beyond Metaphor: An Analysis of Fiduciary Obligation*, 37 DUKE L.J. 879 (1988); Scott FitzGibbon, *Fiduciary Relationships Are Not Contracts*, 82 MARQ. L. REV. 303 (1999); Robert Flannigan, *The Economics of Fiduciary Accountability*, 32 DEL. J. CORP. L. 393 (2007); Robert Flannigan, *The Fiduciary Obligation*, 9 OX. J. LEGAL STUD. 285 (1989) [hereinafter Flannigan, *The Fiduciary Obligation*]; Tamar Frankel, *Fiduciary Law*, 71 CAL. L. REV. 795 (1983); Lawrence E. Mitchell, *The Death of Fiduciary Duty in Close Corporations*, 138 U. PA. L. REV. 1675 (1990); Eileen A. Scallen, *Promises Broken vs. Promised Betrayed: Metaphor, Analogy, and the New Fiduciary Principle*, 1993 U. ILL. L. REV. 897; L.S. Sealy, *Fiduciary Relationships*, 1962 CAMBRIDGE L.J. 69; J.C. Shepherd, *Towards a Unified Concept of Fiduciary Relationships*, 97 L. Q. REV. 51 (1981); D. Gordon Smith, *The Critical Resource Theory of Fiduciary Duty*, 55 VAND. L. REV. 1399 (2002); Ernest J. Weinrib, *The Fiduciary Obligation*, 25 U. TORONTO L.J. 1 (1975).

assets or other property—and manage them on the beneficiary's behalf."[102] Daniel Solove has also suggested looking to the law of fiduciaries as a way to guide sound policy in the age of data brokers who collect an overwhelming amount of personal information.[103]

We agree with Balkin and Solove that the concept of fiduciaries helpfully reorients privacy and crystalizes the concept of trust in information relationships. To be clear, though, we are not recommending that all relationships of trust should automatically be considered as fiduciary in nature. Imposition of the full panoply of fiduciary duties is a serious and burdensome decision. But the law need not face the binary choice of treating information relationships as either "fiduciary" or "unprotected." Surely some middle ground exists between these two extremes. Accordingly, we recommend that duties inspired by fiduciary law can apply in a flexible and variable way across the full spectrum of information relationships.

In relationships where vulnerabilities are minimized because there is only a small amount of trust, these remedies should be applied sparingly or lightly. Where there is greater trust (or greater potential for exposure), entrustees should be held to higher duties of care and loyalty. Rather than relying on a rigid fiduciary/nonfiduciary distinction, we propose a more flexible approach that recognizes the role of trust is *all* information relationships. Yet our fundamental point is that the law of fiduciary relationship can helpfully shed light on the specific duties and actions that promote and erode trust.

B. *Improving the Existing FIPs*

Although the FIPs are worn out, they remain the foundational structure for the regulation of personal data, not only in the United States, but throughout the world.[104] Replacing the FIPs entirely would be a daunting task. But fortunately, what is needed is not the replacement of the FIPs, but rather their rejuvenation from a procedural means of manufacturing consent into a substantive system of regulating the processing of personal data in the interests of all. Trust can provide the source of that rejuvenation, allowing us to rethink the FIPs in ways that are positive, substantive, and inspiring, rather than pessimistic, procedural, and depressing. When viewed through the lens of trust-building the existing FIPs of Confidentiality, Transparency, and Security become the substantive obligations of Discretion, Honesty, and Protection. Even more importantly, when we thinking about privacy in terms of trust suggests the adoption of a new Fair Information Practice: Loyalty.

---

102. Jack Balkin, *Information Fiduciaries in the Digital Age,* BALKINIZATION, http://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html [http://perma.cc/T65R-MNZB]. Jack M. Balkin, Information Fiduciaries and the First Amendment, 49 U.C. DAVIS. L. REV. 1183 (2016).

103. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2006).

104. *See* Gellman, *supra* note 4.

Our proposed modifications are not merely word games. Discretion, Honesty, Protection, and Loyalty offer an alternative vision of privacy protection that escapes the Harm Principle and the Control Illusion. They identify the substantive values that privacy law should embrace if it is to promote the trust that is essential for sustainable information relationships. But critically, when we argue that privacy law should promote trust, this requires a meaningful, substantive level of trust rather than trickery. By contrast, our vision for a rejuvenated, positive theory of privacy protection requires real trust; trust that is accountable. It is for this reason that the substantive principle of loyalty must be understood as essential to the information privacy law project.

1. *Confidentiality as Discretion*

The concept of confidentiality is perhaps the earliest and most foundational in all of privacy law.[105] Despite its entrenched and robust presence in the doctrine, confidentiality is a surprisingly under-developed concept. In most forms of existing regulation, confidentiality is conceptualized merely as nondisclosure. For example, the limited tort of breach of confidentiality prohibited those within confidential relationships from divulging confidential information to any unauthorized parties.[106] As a FIP, confidentiality is articulated as a mere limit on disclosure. This can either take a vague form like "there shall be limits on the external disclosures of information about an individual a record-keeping organization may make,"[107] or be tethered to the purpose of collection and contingent upon the consent of the data subject.[108]

Conceptualizing confidentiality solely in terms of nondisclosure obligations has limited this otherwise dependable, bedrock concept. In many ways, characterizing confidentiality solely in terms of nondisclosure is like characterizing safe sexual practices solely in terms of abstinence—it's effective, but risks overkill and is often too costly. Because confidentiality is so restricting, most people in information relationships are not confidants. They are free to share the information with whomever they wish. The law is rightfully reluctant to make most recipients of information bound by a legal obligation of confidentiality. People need to be able to share most of the information they receive, whether they are businesses and intermediaries or friends and acquaintances.

---

105. Richards & Solove, *supra* note 67, at 135.

106. *Id.*

107. Privacy Protection Study Commission (PPSC) report, Personal Privacy in an Information Society at 501-502 (1977), http://epic.org/privacy/ppsc1977report [http://perma.cc/L4MG-VMUK].

108. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [http://perma.cc/98M6-3BBX] ("Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: a) with the consent of the data subject; or b) by the authority of law.").

Yet people still trust recipients of personal information who are not confidants not to hurt them with that personal information. Is there a middle ground between confidentiality and "every man for himself"? We argue that there is. There are ways other than rigid nondisclosure that entrustees can protect trustors. They can limit to whom they disclose information, they can limit what they share with others, and they can control how they share information to make sure they preserve the trust placed in them. We argue that entrustees can combine all of these strategies: nondisclosure, limited disclosure, trustworthy recipients, and obfuscation to be discreet.

Perhaps the most basic assumption people make when disclosing personal information is that the recipient will be discreet. Discretion, defined as "the quality of behaving or speaking in such a way as to avoid causing offense or revealing private information,"[109] is an implicit part of most information relationships.[110] We trust doctors not to reveal information about our health and mental state; we trust lovers not to kiss and tell; and we trust ISPs and search engines not to reveal our search history. In information relationships, the quickest way to betray a trust is indiscretion: revealing personal information to the wrong person or in the wrong way.

The most robust form of discretion is confidentiality, which we have elsewhere characterized as an obligation of nondisclosure in relationships.[111] Discretion is a broader concept than confidentiality, as it recognizes that trust can be preserved even when the trustee shares information in limited ways. Our disclosures on social media demonstrate this notion of discretion as "appropriate disclosure."

Most disclosures on social network sites like Facebook, Twitter, and Instagram are not confidential. Yet there is an expectation that they are less than "public"—that they will not be read by most people, just by our friends or perhaps our "friends" in the Facebook sense. Professor Lior Strahilevitz has observed this phenomenon and argued that privacy law should take a lesson from the way we expect our disclosures to travel through our offline social networks.[112] Strahilevitz explains that "given the . . . ease with which juicy secrets can spread among people, one might expect that we would play our cards close to our vests, refusing to reveal these embarrassing details to anyone. Yet it is likely that most of us have

---

109. *Discretion*, OXFORD ENGLISH DICTIONARIES, http://www.oxforddictionaries.com/us/definition/american_english/discretion [http://perma.cc/U5EP-T6DZ].

110. Lee Rainie et al., *Anonymity, Privacy, and Security Online*, PEW RESEARCH CENTER (Sept. 5, 2013), http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online [http://perma.cc/MSP9-27Q3], (detailing the importance of control over information and importance of authorization of recipients); Susannah Fox, *Trust and Privacy Online*, PEW RESEARCH CENTER (Aug. 20, 2000), http://www.pewinternet.org/2000/08/20/trust-and-privacy-online [http://perma.cc/2EDC-THU2].

111. Richards & Solove, *supra* note 67.

112. Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005).

shared our most embarrassing details with other people: spouses, siblings, parents, best friends, clergy, psychiatrists, coworkers, or perhaps even strangers on transatlantic flights . . . . By common parlance, we still consider these facts to be "secrets" even after we have revealed them to a handful of people."[113] Strahilevitz draws from sociology, network theory, and related disciplines to argue that people make risk calculations when sharing information. They often assume that their disclosures will stay within certain social networks even if it doesn't remain completely confidential.[114] Such calculations rely not merely on notions of practical obscurity, but on discretion as well.[115]

So trust is preserved when entrustees exercise sound discretion in choosing what and to whom personal information is revealed. It can also be preserved when individuals refrain from becoming entrustees. But at its core, discretion protects against wrongful disclosure, and nondisclosure enables our ability to make friendships, communicate with other people, and participate in society.[116] As Daniel Solove explains, "social judgment and social norms can impede these practices . . . . Protection against disclosure shields us from the harshness of social judgment, which, if left unregulated, could become too powerful and oppressive."[117]

When people are confident that their entrustees will be discreet with their personal information, they become free to engage in commercial and social activities that form the basis of modern society.[118] We gossip, we love, we shop, and we seek help. This has benefits not just for the individual, but also for society as a whole. Commercial activity keeps the lights on. Seeking help from medical professionals benefits public health. The exploration of political beliefs leads to a better-informed electorate, better political decisions, and potentially better leaders. All because entrustees remain discreet.

Privacy law should embrace discretion, which reflects the blurry and contextual lines between "public" and "private." Regulators, legislators, and judges should create some kind of obligation on entrustees to obfuscate disclosures such that the general public or specifically unauthorized parties are unlikely to find or understand entrusted information, even when the information relationship is not

---

113. *Id.*

114. *Id.*

115. *See generally* Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1 (2013); Lauren Gellman, *Privacy, Free Speech, and 'Blurry-Edged' Social Networks*, 50 B.C. L. REV. 1315 (2009).

116. Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 1064 (2003).

117. *Id.* ("People's lives in the public sphere are precarious, for they are constantly subject to the judgment of others and to the sting of social sanctions. It is because people care so much about their public lives, about how others in society regard and treat them, that protection against disclosure is important.").

118. Obligations of nondisclosure also allow people to disclose information that might be used against them, such as credit card numbers, health conditions, and any number of other kinds of personal information that can lead to lost employment, identity theft, and reputational harm.

strictly confidential. The tort of breach of confidentiality could be enhanced by taking discretion into account. The Federal Trade Commission could find a lack of discretion in some instances to be an unfair or deceptive trade practice. Such laws could look to whether entrustees made sure that recipients of data were trustworthy or whether they ensured that certain kinds of information were not publicly available through search engines like Google.

2. *Transparency as Honesty*

One of the bedrock notions of privacy law is that companies should be transparent about their data collection, use, and disclosure practices so that individuals will be on notice of any potentially worrisome practices and can tailor their disclosures accordingly.[119] The FIPs refer to this as the "Openness," that "[t]here should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available to establish the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller."[120] The law and regulations built upon the FIPs often refer to this as "notice and choice," which we discussed above.

In a notice and choice regime, mere disclosure and transparency is usually sufficient to relieve a company of its legal obligations. As long as the data collector is putting its practices out there, it often does not matter whether the data subject reads or even knows about an entrustee's data practices. This is the Choice Illusion in practice. But if trust is to be kept, it is not sufficient to be merely "open" or "transparent." Trust in information relationships requires an affirmative obligation of honesty to correct misinterpretations and to actively dispel notions of mistaken trust.

At a minimum, entrustees must be honest and open with those who disclose personal information to them. The duty of candor and disclosure is a significant one for fiduciaries.[121] Generally speaking, fiduciary trustees should keep those to

---

119. *See* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1049 (2012) (citing Paula J. Dalley, *The Use and Misuse of Disclosure as a Regulatory System*, 34 FLA. ST. U. L. REV. 1089, 1093 (2007) ("[D]isclosure schemes comport with the prevailing political philosophy in that disclosure preserves individual choice while avoiding direct governmental interference.")); Joel Reidenberg, et al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 I/S: A J. OF L. & POL'Y FOR THE INFO. SOC'Y 485 (2015).

120. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [http://perma.cc/GWP4-8YNY].

121. Ethan J. Leib, *Friends As Fiduciaries*, 86 WASH. U. L. REV. 665, 675 (2009) ("This may take the form of requiring doctors to reveal their personal financial interests to their patients (even when those interests are "unrelated to the patient's health") or it may take the form of a general "accounting" requirement, necessitating accurate bookkeeping subject to inspection by the beneficiary as well as the disclosure of all relevant information pertaining to the relationship."); Balkin, *supra* note 102 ("The fiduciary's duty of loyalty may also create a duty of honesty to disclose to the beneficiary how the fiduciary is handling the assets or property.").

whom they are accountable informed. This means accommodating requests for inspection and either affirmatively disclosing or making information available upon request.[122] One rationale for this obligation is that trustees must have the information necessary in order for them to be able to enforce the obligations of the trustee.[123] Obligations of transparency and honestly also help ensure that the trustees are complying with their duty of care and duty of loyalty.

Beyond the narrow category of legal fiduciaries such as trustees, principles of honesty are essential to information relationships more generally. Earlier in our argument, we explained that while the Control Illusion is part of Privacy Pessimism, the problem is one of excessive weight placed on individuals to manage their own privacy from complex, generalized, and often hidden notices. Honesty, by contrast, requires more affirmative steps than passive notice, and includes an obligation to make sure that trusters are actually aware of things that matter to them.[124] It takes the fiction out of constructive notice to require actual notice. Honesty also serves the additional function of forcing companies to take stock of their information practices in order to be accurate when keeping individuals informed.[125]

A focus on honesty can also drive particularized remedies designed to build and maintain trust. California has already mandated privacy policies for mobile apps. GLB and COPPA also require notice. FTC Commissioner Julie Brill's "Reclaim Your Name" campaign, which is designed to increase data broker transparency, is a promising approach for building consumer trust in disclosing personal information.[126]

To be sure, there are many obstacles to ever fully "informing" individuals about a certain practice or risk.[127] Information can be too vast or complex to convey, and the audiences can be too diverse. The goal should not be more notice, but *better* notice. But the goal of honesty-based disclosure in these sorts of cases is broader than just informing. While notice rules are horrible at informing people,

---

122. *Id.*

123. This guiding principle can be seen in the law of irrevocable trusts. *See, e.g.*, Lauren Z. Curry, *Agents in Secrecy: The Use of Information Surrogates in Trust Administration*, 64 VAND. L. REV. 925, 929 (2011) ("Under the most basic principle, a beneficiary of an irrevocable trust is always entitled to information about the trust that is reasonably necessary to allow the beneficiary to enforce the trust, even if the terms of the trust restrict disclosure.").

124. Calo, *supra* note 119.

125. Peter P. Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 MINN. L. REV. 1263, 1264-65 (2002) ("[C]ritics have largely overlooked . . . important benefits from these notices. Perhaps most significantly, publication of the notices and the new legal obligation to comply with them have forced financial institutions to engage in considerable self-scrutiny as to their data handling practices.").

126. Julie Brill, *Demanding Transparency From Data Brokers*, WASH. POST (Aug. 15, 2013), http://www.washingtonpost.com/opinions/demanding-transparency-from-data-brokers/2013/08/15/00609680-0382-11e3-9259-e2aafe5a5f84_story.html [http://perma.cc/2LMD-ZLPV].

127. *See generally* OMRI BEN-SHAHAR & CARL E. SCHNEIDER, THE FAILURE OF MANDATED DISCLOSURE (2014).

they can be very good at generating the skepticism necessary to avoid a misplaced trust. Information practices that are secret or shrouded in secrecy are inherently untrustworthy. Faced with such practices, skeptics act more judiciously or refrain entirely from accepting risk, even if they aren't entirely sure of what they are avoiding or how likely an undesired action or effect is.

"*If I had only known*" is a common response by victims of alleged wrongdoing by others. This refrain is based upon the theory that if certain information had been presented, the would-be victim could have acted differently, or at least knowingly accepted her fate. The idea of notice as savior is the foundation for many disclosure-based regulatory regimes such as privacy policies, Miranda warnings, informed consent, and health warnings on unhealthy products.[128] However, the discussion surrounding notice too often misses the fact that individuals need not fully appreciate risk in order to avoid it. They only need to become skeptical enough to avoid a misplaced trust. If companies or government entities want to avoid creating skeptics, they must embrace and protect the trust users place in them and be honest and transparent.

There are several ways the law might implement honesty requirements. Mandated disclosure regimes might be leveraged to help build trust or, in the least, encourage the kind of skepticism we have mentioned above. Mandated disclosure regimes such as privacy policies, nutrition labels, or informed consent are popular because they are relatively cheap and use a soft regulatory touch. But they are also seen as ineffective, particularly with respect to privacy policies.[129] No one reads the fine print on websites and mobile apps, nor should they be expected to.

A focus on trust might remedy the problems with privacy policies as a tool for consumers. While it is one thing for a company to be forced to list in the fine print the ways in which it collects and shares people's information, it is something else entirely for a company to be forced to admit, "You cannot trust us to be discreet, honest, loyal, or protective." Indications of trust are more intuitive and useful to consumers than dry recitations of what types of information are collected and vague assurances that personal information will only be disclosed to "third party affiliates."

Another way privacy law could better encourage and protect trust is to better situate the concept within the existing law of deception and fraud. Courts and policymakers could find that when people and companies invite or encourage trust, they are making a representation that they must keep. Under this notion, to breach a trust is to deceive. Equating a breached trust with deception will empower the Federal Trade Commission to declare certain breached trusts a deceptive trade practice under Section 5.[130]

Betrayed trusters could also look to the tort of fraud or the law of contracts. This approach would be similar to the finding of an implied confidence, where

---

128. *Id.*

129. *Id.*

130. 15 U.S.C § 45; Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

even though no explicit promise of privacy was made, the surrounding norms and context make it clear a trust was invited and a reasonable person would expect it to be maintained.[131]

Trust need not be exclusively a matter of government policy. Companies can also voluntarily adopt trust-enhancing internal policies, safeguards, and organizational schemes. As with data security, companies can segment entrusted information from less critical data and limit the accessibility of the information. Company executives can make trust a priority by requiring employee training, enshrining trustworthy practices in employee manuals and regularly enforcing these obligations. Companies can delete data when it is no longer needed and collect no more information than is necessary for the information relationship. Even if a company accidentally fails to be discreet or protective, it can help maintain trust by creating and implementing a response plan for when a trust is breached.

Because trust is good for business, companies should be competing to be the most trustworthy. Companies that earn the trust of their users will get more information and sales. Consumers that trust companies will have less reason to flee to competitors who might be less trustworthy. The end result is that the information economy can flourish while still protecting consumers. Everyone wins, except the untrustworthy.

3. *Security as Protection*

Attackers have always sought unauthorized access to personal information. This is why file cabinets have long contained locks and even the earliest databases were protected by passwords. Such stores of information were maintained by "secretaries," a profession dating to medieval times as "one who is entrusted with private or secret matters; a confidant; one privy to a secret."[132]

Tort law has been slow to recognize data security obligations because harms from data breaches can be very difficult to prove.[133] (This is of course but another manifestation of the harm fixation). By contrast, the FIPs have always required data security, with language usually along the lines of "personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data."[134] Policymakers have tended to interpret security requirements in terms of the process data holders must take to protect against attackers.[135] This mainly consists of regularly auditing data assets and risk, minimizing data, implementing technical, physical, and

131. Woodrow Hartzog, *Reviving Implied Confidentiality*, 89 IND. L.J. 763, 764 (2014).

132. *Secretary*, OXFORD ENGLISH DICTIONARY (2015).

133. *See infra* Part II.

134. OECD PRIVACY GUIDELINES, *supra* note 120, at § 5.

135. *See* FEDERAL TRADE COMMISSION, *Commission Statement Marking the FTC's 50th Data Security Settlement* (Jan. 31, 2014), http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf [http://perma.cc/WH5U-66AF]; 45 C.F.R. § 164.306(a) (2015); 15 U.S.C.A. §§ 6801-6809.

administrative safeguards, and creating and following a data breach response plan.[136]

New threats to data require a more holistic approach to data security than just protecting held data. Entrustees must adopt a mentality of data stewardship, which includes protecting information passed on to others. Put simply, in order to preserve a trust, entrustees must protect data, not just secure databases. This requires going beyond firewalls and passwords and affirmatively acting in the interest of data holders. This is the obligation of Protection.

While there are antecedents to Protection from common law duties owed by bodyguards (for physical protection) and banks and lawyers (for protection of secrets and money), Protection has taken on particular importance in the digital age.

In the early 2000s it became clear that personal data was a critical component of our national infrastructure and that external threats to personal data were mounting. The Privacy Rights Clearinghouse has reported that since 2005 there have been over 4,400 data breaches made public with a total of over 932 million records breached.[137] Such estimates are even more startling given that they fail to include the vast number of data breaches that companies have not reported and the unknown number of breaches occurred without companies realizing that they have happened. Data protection is largely hidden from consumers, who typically have no way of knowing how securely their data is being held, or even if databases containing their personal information have been compromised. People in this situation (which is to say, all of us) can only hope that companies will reasonably protect the data that has been entrusted to them.[138]

That data is constantly under attack is no secret. Almost every week a national story breaks detailing the latest data breach, leading 2014 to be dubbed by some as "the year of the breach."[139] Most individuals likely anticipate that trustees will keep information reasonably safe.[140] This was highlighted by the recent massive Office of Personnel Management data breach, where a number of commenters

---

136. *Id.*

137. *Chronology of Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/data-breach [http://perma.cc/T2F9-BFF8].

138. BRUCE SCHNEIER, LIARS AND OUTLIERS: ENABLING THE TRUST THAT SOCIETY NEEDS TO THRIVE (2012).

139. *See, e.g.*, P.J. Smith, *Lessons Learned from 2014: The Year of the Breach*, WIRED INNOVATION INSIGHTS (Dec. 26, 2014, 10:41 AM), http://insights.wired.com/profiles/blogs/lessons-learned-from-2014-the-year-of-the-breach [http://perma.cc/U8U3-FZB9]; Tara Seals, *2014 So Far: The Year of the Data Breach*, INFORMATION SECURITY (Aug. 12, 2014), http://www.infosecurity-magazine.com/news/2014-the-year-of-the-data-breach [http://perma.cc/NLR7-2RSA]; Daniel Fisher, *If 2014 Was the Year of the Data Breach, Brace for More*, FORBES (Jan. 2, 2015), http://www.forbes.com/sites/danielfisher/2015/01/02/if-2014-was-the-year-of-the-data-breach-brace-for-more [http://perma.cc/Q9X3-B7GF].

140. HELEN NISSENBAUM, *Will Security Enhance Trust, or Supplant It?*, *in* TRUST AND DISTRUST WITHIN ORGANIZATIONS: EMERGING PERSPECTIVES, ENDURING QUESTIONS 155 (Roderick Kramer & Karen Cook eds., 2004).

stated a betrayal of their trust in the government to protect their highly sensitive personal information.[141]

People need to be able to trust that entities will protect their data against attackers. Computer company Lenovo breached its users' trust when it surreptitiously installed malware on its new laptops. This code altered users' search results to show them different ads than they would otherwise have seen.[142] The secret deployment of the malware also weakened the laptops' security settings, exposing the computer's browsing history to hackers with the ability to use a particular exploit against the software. In addition to being dishonest and disloyal, this weakening of the computers' security settings violated the duty of Protection.[143]

Protection means more than just setting up a few technical safeguards like firewalls, user authentication requirements, and encryption. It requires a more complete commitment to data protection that includes having procedures to regularly audit the stores of personal information and continuously assess risk using updated threat models, minimizing data collection and storage, instituting procedural and physical safeguards, and preparing a response plan in case of a breach.

Data protection also involves more than just data security. It involves protecting the identity and sensitive attributes of those in stored and released data sets. This means as a practical matter that Discretion will often be essential to protect security as well. The government of New York City betrayed the trust of its tourists and citizens when it released data on 173 million individual taxi trips that were improperly deidentified, inadvertently making it trivial to identify people in the data set.[144] Data sets (big or small) that are shared with others must also be properly scrubbed and protected to minimize the risk that any particular individual will be re-identified. Requirements of this sort are particularly important now that data science is getting better at reidentifying allegedly "anonymized" data sets.[145] More robust techniques of deidentification are being developed, such as k-anonymity and differential privacy, and Protection requires that entrustees (es-

---

141. Jamie Winterton, How OPM Betrayed Me, SLATE (July 16, 2015), http://www.slate.com/articles/technology/future_tense/2015/07/opm_security_clearance_hack_i_trusted_the_government_it_betrayed_me.html?wpsrc=sh_all_dt_tw_top [http://perma.cc/79FT-VEW2].

142. Rosenblat, *Lenovo's Superfish Security Snafu Blows Up in Its Face*, *supra* note 55.

143. *Id.*

144. Alex Hern, *New York Taxi Details Can Be Extracted from Anonymized Data, Researchers* Say, THE GUARDIAN (June 27, 2014, 10:57 AM), http://www.theguardian.com/technology/2014/jun/27/new-york-taxi-details-anonymised-data-researchers-warn [http://perma.cc/PKV3-A4F4].

145. *See generally* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010); Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1, 2 (2011); Felix T. Wu, *Defining Privacy and Utility in Data Sets*, 84 U. COLO. L. REV. 1117 (2013); Daniel Barth-Jones, *The 'Re-Identification' of Governor William Weld's Medical Information: A Critical Re-Examination of Health Data Identification Risks and Privacy Protections, Then and Now* (June 18, 2012), http://fpf.org/wp-content/uploads/The-Re-identification-of-Governor-Welds-Medical-Information-Daniel-Barth-Jones.pdf [http://perma.cc/4BLU-FF6T].

pecially sophisticated commercial ones) stay abreast of such Protection innovations.[146]

Just as our physical security is a combination of technologies like door locks and legal prohibitions on burglary and assault, so too must data Protection rely on law as well as technologies and marked protections. Such legal protections can include contracts prohibiting recipients from reidentification attempts and obligating them to mandate their duties as entrustees to all downstream holders of the data.[147] For example, the Department of Health and Human Services (HHS) and the FTC recently suggested that those who receive anonymized data, whether it be researchers or companies, must promise in advance (preferably via contract) not to attempt to reidentify it.[148] The data security threats our digital society faces are complex, and we should not shirk from sophisticated, multilayered solutions along these lines. Protection of personal data demands no less.

C. *Introducing Loyalty as a Foundational Privacy Value*

One of the foundational obligations of a fiduciary is loyalty, which is an obligation to avoid in self-dealing at the expense of the entrustee.[149] Yet the concept of loyalty is completely missing from privacy law that regulates those who accept information in a fiduciary-like context. We propose that trust in information relationships can be promoted by establishing loyalty as a foundational concept in privacy law.

Personal information is valuable. In the technology industry, it is commonplace to state that "data is the new oil," meaning a fundamental source of value in the information economy.[150] People are becoming wise to the fact that "free" services are only free in the sense that companies do not charge money for them. Their cost is frequently an implicit or unwitting transaction of the customer's personal information and mental attention to advertisements targeted on the basis of

---

146. *See generally* Felix T. Wu, *Defining Privacy and Utility in Data Sets*, 84 U. COLO. L. REV. 1117 (2013).

147. *See generally* Robert Gellman, *The Deidentification Dilemma: A Legislative and Contractual Proposal*, 21 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 33 (2010); Woodrow Hartzog, *Chain-Link Confidentiality*, 46 GA. L. REV. 657 (2012).

148. *Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators*, 76 FED. REG. 44,512, 44,519-20 (July 26, 2011); FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 2 (2012), http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf , William McGeveran et al., *Deidentification and Reidentification in Returning Individual Findings from Biobank and Secondary Research: Regulatory Challenges and Models for Management*, 13 MINN. J. L. SCI. & TECH 485 (2012); Robert Gellman, *supra* note 147.

149. *See* RESTATEMENT (SECOND) OF TRUSTS § 170 cmt. a ("A trustee . . . is under a duty not to profit at the expense of the beneficiary . . . unless authorized to do so by the terms of the trust."); Ethan J. Leib, *supra* note 79.

150. ANGWIN, supra note 7, at 32.

that data.[151] Given the commercial value of personal data, it is not surprising that entrustees in information relationships are tempted to use personal information they receive for their own benefit.

The duty of loyalty is a bedrock principle of the law of fiduciaries. A trustee, for example, cannot lend entrusted funds to herself; nor can trust property be bought by a trustee unless explicitly authorized by the trust instrument.[152] The rationale behind the obligation to avoid self-dealing is to cut off avenues for fraud. As one court put it, "The rule is founded in the highest wisdom. It recognizes the infirmity of human nature, and interposes a barrier against the operation of selfishness and greed. It discourages fraud by taking away motive for its perpetration."[153] Formal trustees are bound to act in the interest of the principal.

Outside the formal context of fiduciary law, not all self-dealing will betray trust. Companies can legitimately use entrusted personal information to their benefit in many different ways. Data can be mined to offer and improve services, effectively anonymized for public research, and even shared with others also willing to preserve a trust. Facebook leverages the personal information of its users to create a precise advertising service. One of Amazon's most valuable features is its recommendation system, which relies upon user data.[154] Websites routinely share deidentified data with others for profit and to simply fine-tune their services.[155]

Such activities are loyal only up to a point, as personal information can quite easily be used to the detriment of trusters. Recall that when we trust others by disclosing our personal information, we expose our vulnerabilities. We regularly expose our preferences, our weaknesses, our desires, and our tendencies to act in a certain way. Disclosure creates power in trustees who can exploit our personal information for their own gain.

The law of consumer protection, for example, is littered with examples of disloyal companies that have misused personal information entrusted to them, for example by using credit card information or other financial data to engage in un-

---

151. Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606 (2014); Jan Whittington & Chris Jay Hoofnagle, *Unpacking Privacy's Price*, 90 N.C. L. REV. 1327 (2012).

152. *See In re* Noonan's Estate, 63 A.2d 80, 83 (Pa. 1949) (holding the executor liable for self-dealing in selling the trust property where he had a personal interest in the transaction that might affect his judgment); RESTATEMENT (SECOND) OF TRUSTS § 170(1) cmt. b (1959) ("A trustee with power to sell trust property is under a duty not to sell to himself . . . [even if he] acts in good faith . . . [and] pays a fair consideration.").

153. *In re* Ryan's Will, 52 N.E.2d 909, 923-24 (N.Y. 1943) (quoting Justice Kent in Bergen v. Bennett, 1 Caines, Cas., 19); *see also* Charles Bryan Baron, *Self-Dealing Trustees and the Exoneration Clause: Can Trustees Ever Profit from Transactions Involving Trust Property?*, 72 ST. JOHN'S L. REV. 43 (2012).

154. Richards, *Social Reading*, *supra* note 99.

155. *See, e.g.*, Ricardo Alonso-Zaldivar & Jack Gillum, *HealthCare.gov Quietly Sharing Personal Data*, WASH. TIMES (Jan. 20, 2015), http://www.washingtontimes.com/news/2015/jan/20/healthcaregov-quietly-sharing-personal-data/?page=all [perma.cc/PLG4-ADUA].

authorized transactions. In *FTC v. Hill*, the FTC alleged that defendant used consumers' financial and credit card data to "pay for goods or services without the consumers' consent."[156] Less nefarious, but equally disloyal, was Orbitz's tactic of showing pricier hotel rooms to users it knew were using Apple computers, based upon the assumption that these users were used to paying more for goods and services.[157]

Disloyalty can take a variety of forms, many of which are not merely financial. Consider the Facebook emotional contagion experiment, in which researchers manipulated Facebook's news feed by, among other things, showing fewer positive posts to some users to see if they would lead to greater user expressions of sadness.[158] Exploiting the power to make trusters unwittingly sad (or angry, or hungry, or aroused) is the definition of disloyalty.

Consider also Uber, the app-based transportation network and taxi company. Uber is entrusted with incredibly sensitive data beyond financial information, including where its users currently are, where they have been, and where they are going. The company created an interface it ominously called "God View," which let administrators see all of the cars in a city as well as the users who are waiting for cars.[159] When "God Mode" was used to entertain corporate party-goers by pointing out one-night stands, this was not loyal. (It had many other issues, of course, including not being discreet). More infamously, Uber was disloyal when it contemplated mining its database to find information to smear journalists who were critical of its business.[160] In such cases, the threat of exposure has ramifications not just for the journalists who used Uber, but political and free expression ones from its chilling of public debate.

Ryan Calo has helpfully coined the term "digital market manipulation" to describe this practice of leveraging personal information against consumers in mediated environments.[161] Calo argues that some manipulations of users which exploit vulnerabilities should be legally actionable.[162] Our theory of privacy as trust

---

156. Complaint for Permanent Injunction and Other Equitable Relief, FTC v. Sitesearch (D.Ariz., Dec. 22, 2014), http://www.ftc.gov/system/files/documents/cases/141223leaplabcmpt.pdf [http://perma.cc/4U7C-DQ6K].

157. Dana Mattioli, *On Orbitz, Mac Users Steered to Pricier Hotels*, WALL ST. J. (Aug. 23, 2012, 6:07 PM), http://www.wsj.com/articles/SB10001424052702304458604577488822667325882 [perma.cc/X23K-TJDJ].

158. Dewey, *9 Answers About Facebook's Creepy Emotional-Manipulation Experiment*, *supra* note 8.

159. Kashmir Hill, *'God View': Uber Allegedly Stalked Users For Party-Goers Viewing Pleasure*, FORBES (Oct. 3, 2014, 11:32 AM), http://www.forbes.com/sites/kashmirhill/2014/10/03/god-view-uber-allegedly-stalked-users-for-party-goers-viewing-pleasure [perma.cc/MXV5-68P7].

160. Ben Smith, *Uber Executive Suggests Digging Up Dirt on Journalists*, BUZZFEED (Nov. 17, 2014, 6:57 PM), http://www.buzzfeed.com/bensmith/uber-executive-suggests-digging-up-dirt-on-journalists#.guwMYyV65 [perma.cc/RH8R-XFJE].

161. Calo, *Digital Market Manipulation*, *supra* note 75.

162. *Id.*

helps to explain why this should be the case, by better capturing the essence of the wrongdoing (here, as trust-destroying disloyalty).

More broadly, many of our deep-seeded fears about "big data," genetic information, and discrimination are at base fears about disloyalty.[163] After a recent public investigation of big data's discriminatory potential,[164] the FTC expressed its serious concerns about the use of big data analytics to unfairly exclude lower-income consumers.[165] Similar fears of digital "redlining" undergird the White House's study of big data.[166] Companies could use big data to exclude disadvantaged populations from the marketplace. Much of this exclusion could be justified as fair competition. However, the law should prohibit unreasonable self-dealing and regulate disloyal entrustees of information. This could be done through presumptions of trust created via tort law by expanding the breach of confidentiality tort or through regulatory mechanisms like a consumer privacy bill of rights or Section 5 of the FTC Act, which prohibits unfair and deceptive trade practices. But regardless of how it is implemented, loyalty is essential to any theory of privacy that meaningfully safeguards trust.

V. CONCLUSION

We have thought about privacy in pessimistic and outdated terms for too long. Uses of personal information can certainly cause anxiety and stimulate feelings of creepiness, they can absolutely cause harm, and individual choice certainly will have an appropriate role to play in our digital future. But Privacy Pessimism is a limited and incomplete way of conceptualizing questions of personal information and new technologies. It looks only to the costs of privacy rules rather than their benefits, and in so doing blinkers our vision, preventing us from imagining ways in which privacy rules can create value rather than impose costs and inefficiencies.

Understanding privacy in terms of its ability to promote trust solves the problem of Privacy Pessimism. Information relationships have long been essential to our lives, and the growth of digital networked technologies has only deepened their importance. Our venerable information relationships with doctors, lawyers, and merchants recognized the importance of information rules, and how those rules could produce the trust necessary for the kinds of long-term relationships that served the interests of trusters, entrustees, and society as a whole. Yet these understandings were perhaps so obviously correct as to be implicit and rarely re-

163. Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671 (2016).

164. *See* FTC, *Big Data: A Tool for Inclusion or Exclusion?: Event Webpage*, FTC (Sept. 15, 2014), http://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion [perma.cc/74CF-6DRF].

165. *Id.* ("For example, high-income consumers may receive offers for 'gold level' credit cards and low-income consumers may receive offers for subprime credit cards.").

166. EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 46 (May 2014).

marked upon.

As we embark on the creation of new information relationships involving new entrustees and new kinds of personal information, we must ensure that the essential elements of social trust are built into them so that our new relationships can be as sustainable as our older ones. This observation is, we believe, the most important contribution this Article makes. Trust is necessary for a sustainable digital future, and trust-promoting privacy rules can create individual and social value. If trust becomes a major part of the privacy conversation; if we look beyond Privacy Pessimism towards a kind of Privacy Optimism that can guide social norms and legal rules, we believe that our intervention will have been a success.