2013

Privacy Self-Management and the Consent Dilemma

Daniel J. Solove
George Washington University Law School, dsolove@law.gwu.edu

Recommended Citation
Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880 (2013).

INTRODUCTION: PRIVACY SELF-MANAGEMENT AND THE CONSENT DILEMMA

Daniel J. Solove[*]

INTRODUCTION

During the past decade, the problems involving information privacy — the ascendance of Big Data and fusion centers, the tsunami of data security breaches, the rise of Web 2.0, the growth of behavioral marketing, and the proliferation of tracking technologies — have become thornier. Policymakers have proposed and passed significant new regulation in the United States and abroad, yet the basic approach to protecting privacy has remained largely unchanged since the 1970s. Under the current approach, the law provides people with a set of rights to enable them to make decisions about how to manage their data. These rights consist primarily of rights to notice, access, and consent regarding the collection, use, and disclosure of personal data. The goal of this bundle of rights is to provide people with control over their personal data, and through this control people can decide for themselves how to weigh the costs and benefits of the collection, use, or disclosure of their information. I will refer to this approach to privacy regulation as "privacy self-management."

Privacy self-management takes refuge in consent. It attempts to be neutral about substance — whether certain forms of collecting, using, or disclosing personal data are good or bad — and instead focuses on whether people consent to various privacy practices. Consent legitimizes nearly any form of collection, use, or disclosure of personal data.

Although privacy self-management is certainly a laudable and necessary component of any regulatory regime, I contend that it is being tasked with doing work beyond its capabilities. Privacy self-management does not provide people with meaningful control over their data. First, empirical and social science research demonstrates that there are severe cognitive problems that undermine privacy self-management. These cognitive problems impair individuals' ability to

[*] John Marshall Harlan Research Professor of Law, George Washington University Law School. I would like to thank my research assistant, Rachel Kleinpeter, for her research on this Article. Thanks to Danielle Citron, Julie Cohen, Deven Desai, Woodrow Hartzog, Chris Hoofnagle, Orin Kerr, Harriet Pearson, and Paul M. Schwartz for comments on the manuscript.

make informed, rational choices about the costs and benefits of consenting to the collection, use, and disclosure of their personal data.

Second, and more troubling, even well-informed and rational individuals cannot appropriately self-manage their privacy due to several structural problems. There are too many entities collecting and using personal data to make it feasible for people to manage their privacy separately with each entity. Moreover, many privacy harms are the result of an aggregation of pieces of data over a period of time by different entities. It is virtually impossible for people to weigh the costs and benefits of revealing information or permitting its use or transfer without an understanding of the potential downstream uses, further limiting the effectiveness of the privacy self-management framework.

In addition, privacy self-management addresses privacy in a series of isolated transactions guided by particular individuals. Privacy costs and benefits, however, are more appropriately assessed cumulatively and holistically — not merely at the individual level. As several Articles in this Symposium demonstrate, privacy has an enormous social impact. Professor Neil Richards argues that privacy safeguards intellectual pursuits, and that there is a larger social value to ensuring robust and uninhibited reading, speaking, and exploration of ideas.[1] Professor Julie Cohen argues that innovation depends upon privacy, which is increasingly under threat as Big Data mines information about individuals and as media-content providers track people's consumption of ideas through technology.[2] Moreover, in a number of cases, as Professor Lior Strahilevitz contends, privacy protection has distributive effects; it benefits some people and harms other people.[3] Privacy thus does more than just protect individuals. It fosters a certain kind of society, since people's decisions about their own privacy affect society, not just themselves. Because individual decisions to consent to data collection, use, or disclosure might not collectively yield the most desirable social outcome, privacy self-management often fails to address these larger social values.

With each sign of failure of privacy self-management, however, the typical response by policymakers, scholars, and others is to call for more and improved privacy self-management. In this Article, I argue that in order to advance, privacy law and policy must face the problems with privacy self-management and start forging a new direction.

Any solution must confront a complex dilemma with consent. Consent to collection, use, and disclosure of personal data is often not meaningful, but the most apparent solution — paternalistic

---

[1] *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1945–52 (2013).

[2] *See* Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1918–27 (2013).

[3] *See* Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010 (2013).

measures — even more directly denies people the freedom to make consensual choices about their data. Paternalism would be easy to justify if many uses of data had little benefit or were primarily detrimental to the individual or society. But many uses of data have benefits in addition to costs, and individuals could rationally reach opposite conclusions regarding whether the benefits outweigh the costs. Making the choice for individuals restrains their ability to consent. Thus, to the extent that legal solutions follow a path away from privacy self-management and toward paternalism, they are likely to limit consent. A way out of this dilemma remains elusive.

Until privacy law recognizes the true depth of the difficulties of privacy self-management and confronts the consent dilemma, privacy law will not be able to progress much further. In this Article, I will propose several ways privacy law can grapple with the consent dilemma and move beyond relying too heavily on privacy self-management.

I. PRIVACY SELF-MANAGEMENT

Privacy self-management has its origins in the Fair Information Practices, which are also commonly referred to as the Fair Information Practice Principles (FIPPs).[4] The FIPPs officially appeared in a 1973 report by the U.S. Department of Health, Education, and Welfare (HEW) to address concerns about the increasing digitization of data. The principles included (1) transparency of record systems of personal data, (2) the right to notice about such record systems, (3) the right to prevent personal data from being used for new purposes without consent, (4) the right to correct or amend one's records, and (5) responsibilities on the holders of data to prevent its misuse.[5] These principles were embodied selectively in various statutes in the United States, and they helped shape the OECD Privacy Guidelines of 1980 and the APEC Privacy Framework of 2004.[6]

Nearly all instantiations of the FIPPs fail to specify what data may be collected or how it may be used. Instead, most forms of data collection, use, and disclosure are permissible under the FIPPs if individuals have the ability to self-manage their privacy — that is, if they are notified and provide consent.

---

[4] *See* Robert Gellman, *Fair Information Practices: A Basic History*, BOB GELLMAN 9–10 (Nov. 12, 2012), http://bobgellman.com/rg-docs/rg-FIPPShistory.pdf.

[5] SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS 41–42 (1973).

[6] ORG. FOR ECON. CO-OPERATION AND DEV., OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980); ASIA-PAC. ECON. COOPERATION, APEC PRIVACY FRAMEWORK (2004); Gellman, *supra* note 4, at 7.

Privacy self-management is so widely accepted that even deep disputes about privacy protection turn on different interpretations and applications of it. In 2012, for example, both the Federal Trade Commission (FTC) and the White House, dissatisfied with the current regulatory approach, issued major new frameworks for protecting privacy. At the foundation of both, however, is the same old privacy self-management model. The FTC framework aims to "[m]ake information collection and use practices transparent" and to provide people with "the ability to make decisions about their data at a relevant time and context."[7] A centerpiece of the White House's proposed Consumer Bill of Rights is the right of consumers to exercise "appropriate control" over their personal data and to have "clear and simple choices, presented at times and in ways that enable consumers to make meaningful decisions about personal data collection, use, and disclosure."[8]

As I will argue in this Part, however, privacy self-management faces several problems that together demonstrate that this paradigm alone cannot serve as the centerpiece of a viable privacy regulatory regime. I will discuss two broad types of problems: (1) cognitive problems, which concern challenges caused by the way humans make decisions, and (2) structural problems, which concern challenges arising from how privacy decisions are designed.

A. Cognitive Problems

A number of cognitive problems plague privacy self-management. Privacy self-management envisions an informed and rational person who makes appropriate decisions about whether to consent to various forms of collection, use, and disclosure of personal data. But empirical evidence and social science literature demonstrate that people's actual ability to make such informed and rational decisions does not even come close to the vision contemplated by privacy self-management.

1. The Problem of the Uninformed Individual. — Two of the most important components of privacy self-management are informing individuals about the data collected and used about them (notice) and allowing them to decide whether they accept such collection and uses (choice). These components of the FIPPs are widely embraced in the United States,[9] an approach termed "notice and choice." Entities have normalized the practice of providing notice and choice by offering pri-

---

[7] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, at i (2012), *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf.

[8] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD 47 (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[9] *See* Julie Brill, Comm'r, Fed. Trade Comm'n, Remarks at Conference of Western Attorneys General Annual Meeting, Privacy 3.0 Panel (July 20, 2010).

vacy notices and a choice to opt out of some of the forms of data collection and use described in the notices.

The FTC has stepped in to serve as an enforcer of privacy notices. Since 1998, the FTC has maintained that breaking promises made in a privacy notice constitutes "unfair or deceptive acts or practices in or affecting commerce" in violation of the Federal Trade Commission Act.[10] When it finds such a violation, the FTC can bring civil actions and seek injunctive remedies.[11] The notice and choice approach has also been a centerpiece of privacy legislation. The Gramm-Leach-Bliley Act (GLBA),[12] for example, requires financial institutions to provide customers with privacy notices and to allow customers to opt out of data sharing with third parties.[13]

Despite the embrace of notice and choice, people do not seem to be engaging in much privacy self-management. Most people do not read privacy notices on a regular basis.[14] As for other types of notices, such as end-user license agreements and contract boilerplate terms, studies show only a miniscule percentage of people read them.[15] Moreover, few people opt out of the collection, use, or disclosure of their data when presented with the choice to do so.[16] Most people do not even bother to change the default privacy settings on websites.[17] As FTC

---

[10] 15 U.S.C. § 45(a)(1) (2006). For background about the FTC's enforcement regarding privacy, see DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 820–31 (4th ed. 2011).

[11] 15 U.S.C. § 45(l)–(m).

[12] Pub. L. No. 106-102, 113 Stat. 1338 (codified in scattered sections of 12 and 15 U.S.C).

[13] 15 U.S.C. § 6802(a)–(b) (2006).

[14] *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT 105 (2010) (discussing a 2006 study showing that only 20% of people read privacy notices "most of the time" (quoting TRUSTe & TNS, *Consumers Have a False Sense of Security About Online Privacy: Actions Inconsistent with Attitudes*, PR NEWSWIRE, http://www.prnewswire.com/news-releases/consumers-have-false-sense-of-security-about-online-privacy---actions-inconsistent-with-attitudes-55969467.html (last visited Mar. 30, 2013) (internal quotation marks omitted))); Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 343, 361–62 (Jane K. Winn ed., 2006); George R. Milne & Mary J. Culnan, *Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices*, 18 J. INTERACTIVE MARKETING 15, 20–21 (2004) (finding that only 4.5% of respondents said they always read website privacy notices and 14.1% frequently read them).

[15] *See, e.g.*, Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 665–78 (2011); Florencia Marotta-Wurgler, *Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's "Principles of the Law of Software Contracts,"* 78 U. CHI. L. REV. 165, 178 (2011) (discussing a study that revealed that people accessed contract boilerplate terms far less than 1% of the time).

[16] *See* Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1230 (2002) (stating that according to one survey, "only 0.5% of banking customers had exercised their opt-out rights").

[17] *See* Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, *in* DIGITAL PRIVACY 363, 369 (Alessandro Acquisti, Stefanos Gritzalis, Costas Lambrinoudakis & Sabrina De Capitani di Vimercati eds., 2008).

Chairman Jon Leibowitz has concluded: "Initially, privacy policies seemed like a good idea. But in practice, they often leave a lot to be desired. In many cases, consumers don't notice, read, or understand the privacy policies."[18]

Why are so few people engaging in privacy self-management? One possible explanation is that privacy notices are long and difficult to comprehend.[19] There have been many proposals to shorten and simplify privacy policies, though these types of measures have not been shown to significantly improve comprehension.[20] For example, Professor M. Ryan Calo suggests that "visceral notice" may resuscitate the notice approach by attempting to make people experience notice more directly and emotionally.[21] As an example, Calo references the FDA's effort to require graphic warnings, including images of death, on cigarettes.[22] While smoking warnings may be effective because cancer and death are such concrete and terrible consequences, privacy warnings are more difficult to translate into visceral terms because the consequences are much more abstract.

There is a more difficult problem with proposals for improved notice, whether simplified or more visceral. Such proposals neglect a fundamental dilemma of notice: making it simple and easy to understand conflicts with fully informing people about the consequences of giving up data, which are quite complex if explained in sufficient detail to be meaningful. People need a deeper understanding and background to make informed choices. Many privacy notices, however, are vague about future uses of data.

Moreover, as Strahilevitz notes in this Symposium, privacy choices are often binary, such as with the Do Not Call Registry that allows people to choose whether to opt out of telemarketing solutions.[23] Many people might desire more granularity in their choices, but additional granularity adds complexity and creates greater risks of confusion.

---

[18] Jon Leibowitz, Comm'r, Fed. Trade Comm'n, So Private, So Public: Individuals, the Internet & the Paradox of Behavioral Marketing, Remarks at the FTC Town Hall Meeting on Behavioral Advertising: Tracking, Targeting, & Technology (Nov. 1, 2007), *available at* http://www.ftc.gov/speeches/leibowitz/071031ehavior.pdf.

[19] *See* Annie I. Anton et al., *Financial Privacy Policies and the Need for Standardization*, 2 IEEE SECURITY & PRIVACY 36, 42–44 (2004); Janger & Schwartz, *supra* note 16, at 1230–32; Erik Sherman, *Privacy Policies Are Great — For PhDs*, CBS NEWS (Sept. 4, 2008, 5:31 AM), http://industry.bnet.com/technology/1000391/privacypolicies-are-great-for-phds.

[20] *See* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1033 (2012) ("Studies show only marginal improvement in consumer understanding where privacy policies get expressed as tables, icons, or labels, assuming the consumer even reads them.").

[21] *See id.* at 1034–35.

[22] *Id.* at 1069–70.

[23] *See* Strahilevitz, *supra* note 3, at 2038.

Compounding the difficulties in providing notice and choice is the fact that people operate under woefully incorrect assumptions about how their privacy is protected. One study found that people correctly answered only 30% of questions regarding the privacy of their online transactions.[24] Another study found that "64% [of the people surveyed] do not know that a supermarket is allowed to sell other companies information about what they buy" and that 75% falsely believe that when "a website has a privacy policy, it means the site will not share my information with other websites and companies."[25]

Thus far, in most situations, people do not engage in privacy self-management. The evidence suggests that people are not well informed about privacy. Efforts to improve education are certainly laudable, as are attempts to make privacy notices more understandable. But such efforts fail to address a deeper problem — privacy is quite complicated. This fact leads to a tradeoff between providing a meaningful notice and providing a short and simple one.

2. The Problem of Skewed Decisionmaking. — Even if most people were to read privacy policies routinely, people often lack enough expertise to adequately assess the consequences of agreeing to certain present uses or disclosures of their data. People routinely turn over their data for very small benefits.[26] Some conclude from this fact that consumers do not value privacy highly.[27] Some have suggested that there might be a generational shift in privacy norms, where young people do not care about privacy.[28] But in surveys, people routinely declare how much they care about privacy, and attitudes about privacy among the young and old are, surprisingly, quite similar.[29]

There is a clear disconnect between people's expressed high value of privacy and their behavior, which indicates a very low value of privacy. Does this mean people actually do not care about privacy? Social science literature indicates that this disconnect stems from certain impediments to rational decisionmaking.

---

[24] Joseph Turow et al., Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It 20–21 (Sept. 29, 2009) (unpublished manuscript), *available at* http://ssrn.com/paper=1478214.

[25] Joseph Turow, Lauren Feldman & Kimberly Meltzer, OPEN TO EXPLOITATION: AMERICAN SHOPPERS ONLINE AND OFFLINE (Univ. of Pa., Annenberg Pub. Policy Ctr. 2005), *available at* http://www.annenbergpublicpolicycenter.org/downloads/information_and_society/turow_appc_report_web_final.pdf.

[26] *See* Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality: A Survey*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY 15, 16 (Katherine J. Strandburg & Daniela Stan Raicu eds., 2006).

[27] *See* Eric Goldman, *The Privacy Hoax*, FORBES, Oct. 14, 2002, at 42.

[28] *See* Emily Nussbaum, *My So-Called Blog*, N.Y. TIMES, Jan. 11, 2004 § 6 (Magazine), at 32, 34.

[29] *See* Chris Jay Hoofnagle et al., How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes & Policies? (Aug. 14, 2010) (unpublished manuscript) *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864.

Work in social science — which I will define broadly to encompass behavioral economics, psychology, and empirical studies in other fields — shows that so many of our cherished assumptions about the way people make decisions regarding privacy are false. As Professors Richard Thaler and Cass Sunstein note, the "false assumption is that almost all people, almost all of the time, make choices that are in their best interest or at the very least are better than the choices that would be made by someone else."[30] Studies by Professor Daniel Kahneman, Professor Amos Tversky, and others demonstrate the falsity of the traditional rational agent model of human decisionmaking, as people often decide based on heuristics and the way choices are framed.[31]

People have "bounded rationality" — they struggle to apply their knowledge to complex situations — with regard to privacy.[32] As Professors Alessandro Acquisti and Jens Grossklags observe, "our innate bounded rationality limits our ability to acquire, memorize, and process all relevant information, and it makes us rely on simplified mental models, approximate strategies, and heuristics."[33] Risk assessment is also skewed by the "availability heuristic," where people assess familiar dangers as riskier than unfamiliar ones.[34]

Social science also reveals that privacy preferences are not developed in the abstract but in context. The way choices are framed, and many other factors, shape — and tend to skew — privacy preferences.[35] People are also more willing to share personal data when they feel in control, regardless of whether that control is real or illusory. More generally, "people are more willing to take risks, and judge those risks as less severe, when they feel in control."[36]

People may also tend to make certain mistakes in judgment consistently.[37] At this point in time, companies, politicians, and others seeking to influence choices are only beginning to tap into the insights from social science literature, and they primarily still use rather anecdotal and unscientific means of persuasion. When those seeking to

---

[30] RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE 9 (2008).

[31] DANIEL KAHNEMAN, THINKING, FAST AND SLOW 411 (2011). *See generally* CHOICES, VALUES, AND FRAMES (Daniel Kahneman & Amos Tversky eds., 2000); JUDGMENT UNDER UNCERTAINTY: HEURISTICS AND BIASES (Daniel Kahneman, Paul Slovic & Amos Tversky eds., 1982).

[32] Acquisti & Grossklags, *supra* note 26, at 25–26.

[33] Acquisti & Grossklags, *supra* note 17, at 369.

[34] THALER & SUNSTEIN, *supra* note 30, at 25.

[35] Leslie K. John et al., The Best of Strangers: Context Dependent Willingness to Divulge Personal Information (July 6, 2009) (unpublished manuscript), *available at* http://ssrn.com/abstract=1430482.

[36] Laura Brandimarte, Alessandro Acquisti & George Loewenstein, *Misplaced Confidences: Privacy and the Control Paradox*, SOC. PSYCHOL. & PERSONALITY SCI. (forthcoming) (manuscript at 3), *available at* http://www.heinz.cmu.edu/~acquisti/papers/acquisti-SPPS.pdf.

[37] *See* DAN ARIELY, PREDICTABLY IRRATIONAL 240–41 (2008).

shape decisions hone their techniques based on these social science insights (ironically enabled by access to ever-increasing amounts of data about individuals and their behavior), people's choices may be more controlled than ever before (and also ironically, such choices can be structured to make people believe that they are in control).

The upshot of this problem is that privacy decisions are particularly susceptible to problems such as bounded rationality, the availability heuristic, and framing effects because privacy is so complex, contextual, and difficult to conceptualize.

* * *

The cognitive problems above thus present numerous hurdles for privacy self-management: (1) people do not read privacy policies; (2) if people read them, they do not understand them; (3) if people read and understand them, they often lack enough background knowledge to make an informed choice; and (4) if people read them, understand them, and can make an informed choice, their choice might be skewed by various decisionmaking difficulties. The situation nearly approaches that faced by the protagonist in Franz Kafka's parable *Before the Law* where the gateway was guarded by an infinite set of doorkeepers, each more powerful than the next.[38]

B. Structural Problems

Even assuming that people are fully informed and rational, that there is a way to protect their decisions from being skewed, and that there is a way to capture their preferences accurately, privacy self-management also faces serious structural problems. These structural problems involve impediments to one's ability to adequately assess the costs and benefits of consenting to various forms of collection, use, and disclosure of personal data. Structuring meaningful privacy decisions proves to be an immensely difficult endeavor.

1. The Problem of Scale. — A person may be able to manage her privacy with a few entities, but privacy self-management does not scale well. Even if every entity provided people with an easy and clear way to manage their privacy, there are simply too many entities that collect, use, and disclose people's data for the rational person to handle. In particular, the average American visits nearly a hundred websites per month and does business online and offline with countless companies (merchant, utility, insurance, technology, travel, financial,

[38] FRANZ KAFKA, THE TRIAL 215 (Breon Mitchell trans., Schocken Books 1998) (1925).

etc.).[39] Not only will people struggle to manage privacy with the entities they know about, but there are also scores of entities that traffic in personal data without people ever being aware. People cannot manage their privacy with regard to these extensive "reservoirs" of data unless they know these reservoirs exist and can identify the various entities that maintain them.[40]

The problem is reminiscent of the beleaguered student whose professors collectively assign too much reading each night. From the perspective of each professor, the reading is a reasonable amount for an evening. But when five or six simultaneously assign a night's worth of reading, the amount collectively becomes far too much. Thus, even if all companies provided notice and adequate choices, this data management problem would persist; the average person just does not have enough time or resources to manage all the entities that hold her data. One study estimated it would cost $781 billion in lost productivity if everyone were to read every privacy policy at websites they visited in a one-year period.[41] And many entities frequently modify their privacy policies, so reading them all just once is not enough. The problem exists with opt-out policies as well as with opt-in policies.

Many entities want to do the right thing and be open about their privacy practices and how people's data will be used. However, even with simple, conspicuous, and understandable privacy policies, the problem of scale persists.

2. The Problem of Aggregation. — Another problem is that even if people made rational decisions about sharing individual pieces of data in isolation, they greatly struggle to factor in how their data might be aggregated in the future. Suppose a person gives out an innocuous piece of data at one point in time, thinking that he or she is not revealing anything sensitive. At other points in time, the person reveals equally nonsensitive data. Unexpectedly, this data might be combined and analyzed to reveal sensitive facts about the person. The person never disclosed these facts nor anticipated that they would be uncovered. The problem was that the person gave away too many clues. Modern data analytics, which is also loosely referred to as data mining or "Big Data," can deduce extensive information about a person from

---

[39] *See August 2011 — Top US Web Brands*, NIELSEN WIRE (Sept. 30, 2011), http://blog.nielsen.com/nielsenwire/online_mobile/august-2011-top-us-web-brands/.

[40] *See* Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 243–51 (2007).

[41] Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL'Y FOR INFO. SOC'Y 543, 564 (2008).

these clues. In other words, little bits of innocuous data can say a lot in combination.[42] I have referred to this as the "aggregation effect."[43]

The difficulty with the aggregation effect is that it makes it nearly impossible to manage data. The types of new information that can be gleaned from analyzing existing information and the kinds of predictions that can be made from this data are far too vast and complex, and are evolving too quickly, for people to fully assess the risks and benefits involved. This state of affairs makes it very hard to assess whether revealing any piece of information will sometime later on, when combined with other data, reveal something sensitive.

The costs and benefits of each situation depend on the collective set of previous disclosure decisions. At Time 1, it might make sense for a person to reveal Fact 1. At Time 2, the person might decide to reveal Fact 2. What is hard to determine is whether at Time 3 Facts 1 and 2 might be combined to reveal Fact 3, and whether the person would be harmed by the knowledge or use of Fact 3. But at the time of revealing Fact 1 and Fact 2, the person might have no idea that Fact 1 plus Fact 2 would yield Fact 3.

In the real world, we do not have just a few facts, but thousands of pieces of data. Suppose that over the course of the past decade, a person gives out 50,000 pieces of data. The person has not been negatively affected by revealing these pieces of data. One day, the person reveals Fact 50,001, a relatively innocuous fact that gets combined with some of the other facts the person provided many years ago to reveal Fact 50,002. Deduced via a newly created algorithm, this fact proves harmful to the person.

Of course, Fact 50,002 could turn out to be beneficial to the person or to society as a whole — perhaps it reveals that the person is at risk for contracting a highly contagious and lethal disease. The point is that it is virtually impossible for a person to make meaningful judgments about the costs and benefits of revealing certain data. Therefore, in many situations, too much is unknown to make a meaningful decision about costs and benefits at the time that people are asked to manage their privacy.

To enable a person to make a rational decision about sharing data, that person would need to have an understanding of the range of possible harms and benefits so as to do a cost-benefit analysis. Of course, people make decisions in the face of uncertainty all the time, but they often do so quite badly. As psychologist Daniel Gilbert has noted,

---

[42] In addition to learning new information by combining bits and pieces of old information, data analytics can make predictions about future behavior. Big Data might know something about people even before they know it themselves.

[43] DANIEL J. SOLOVE, THE DIGITAL PERSON 44–47 (2004).

people's predictions about how various events will affect their future happiness are remarkably inaccurate.[44]

Another challenge is that aggregation alters the identifiability of other data. Privacy regulation is typically triggered by the presence of "personally identifiable information" (PII) — defined roughly as information that is identifiable to an individual. Privacy laws typically regulate only when PII is involved.[45] One problem with PII is that, as discussed above, it is not static: the identifiability of data depends upon context.[46] A search query, for example, is often not inherently identifiable. Its identifiability depends upon the existing data available online. Such was the case with the famous anonymized search results AOL released, leading to a reporter's identifying a person based on her search queries.[47] As data gets aggregated, information that is not identifiable can become identified.

3. The Problem of Assessing Harm. — Compounding these problems is the fact that people often favor immediate benefits even when there may be future detriments.[48] The aggregation effect shows that privacy is an issue of long-term information management, while most decisions to consent to the collection, use, or disclosure of data are tied to a short-term benefit.

Privacy self-management asks people to assess the potential harm to themselves early on, typically when the data is initially collected. However, for a number of reasons, people will find it immensely challenging to engage in this cost-benefit analysis. First, as already discussed, many privacy harms are cumulative in nature: people may agree to many forms of data collection, use, and disclosure over a long period of time, and the harmful effects may only emerge from the downstream uses of the combination of the data.

Individual privacy harms, meanwhile, are often small and dispersed. Of course, revealing nude photographs or highly embarrassing or discreditable facts can generate substantial emotional distress. But many privacy violations are akin to a bee sting. Despite this fact, it would be wrong to conclude that they ought to be ignored. One bee sting can be shrugged off, but a hundred or a thousand can be lethal. Harm from privacy violations can develop gradually over time, but decisions about privacy must be made individually, in isolation, and far in advance.

---

[44] *See* DANIEL GILBERT, STUMBLING ON HAPPINESS 24–25 (2006).

[45] *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1816 (2011).

[46] *See supra* p. 1890.

[47] Michael Barbaro & Tom Zeller, Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, at A1.

[48] *See* Acquisti & Grossklags, *supra* note 17, at 372.

Additionally, privacy self-management fails to account for the social impacts of individual privacy decisions. Individual privacy has a variety of social functions. Several scholars have recognized that privacy is "constitutive" of society.[49] Professor Priscilla Regan demonstrates the need for understanding privacy in terms of its social benefits.[50] Professor Joel Reidenberg contends that "[s]ociety as a whole has an important stake in the contours of the protection of personal information."[51] Professor Spiros Simitis recognizes that "privacy considerations no longer arise out of particular individual problems; rather, they express conflicts affecting everyone."[52] Then-Professor Robert Post asserts that privacy protection "safeguards rules of civility that in some significant measure constitute both individuals and community."[53] Professor Paul Schwartz has further developed the theory of constitutive privacy in arguing for privacy's importance to civil society.[54] Schwartz focuses on how the protection of information privacy will further self-governance and democracy on the Internet.[55]

According to Cohen, privacy protection "preserves a zone of informational autonomy for individuals."[56] Privacy is essential not just to our individual development but also to our cultural development. Our intellectual development depends upon the creativity of others, and our creativity in turn shapes their intellectual growth. These forces interact to develop a rich culture. Stunting individual creativity and intellectual development impoverishes society at large.[57]

Richards's concept of "intellectual privacy" also recognizes the broader social importance of privacy.[58] Richards contends that "new ideas often develop best away from the intense scrutiny of public exposure" and that privacy is essential to promoting intellectual freedom.[59] He also argues that intellectual privacy "should be preserved against

---

[49] *E.g.*, Janger & Schwartz, *supra* note 16, at 1247.

[50] *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY 212–14 (1995).

[51] Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 882–83 (2003).

[52] Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 709 (1987).

[53] Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 959 (1989).

[54] *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1613 (1999).

[55] *Id.* at 1613–14.

[56] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1428 (2000).

[57] *See* Cohen, *supra* note 2, at 1918.

[58] Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008).

[59] Richards, *supra* note 1, at 1946.

private actors as well as against the state" because "[w]e are constrained in our actions by peer pressure at least as much as by the state."[60]

Privacy self-management cedes substantial responsibility for preserving privacy to individuals, and it assumes that the primary harm to be redressed is nonconsensual data collection, use, or disclosure. Although impinging upon consent constitutes harm worthy of redress, the collective actions of people regarding privacy can implicate larger social values. Privacy self-management does not prevent, redress, or even consider infringements on those social values.

There is a countervailing social value in certain uses of data, such as research uses, which might justify overriding individual decisions. As Schwartz and I document elsewhere, data analytics have led to new and improved medical treatments, as well as more effective responses to data security breaches.[61] There are thus social values both in favor of and against privacy that are not adequately reflected in privacy self-management, which focuses too exclusively on individual choice.

* * *

Privacy self-management often asks people to make decisions at an early point in time (when information is collected) and at a series of isolated instances. But the true consequences of information use for individuals cannot be known when they make these decisions. Furthermore, the consequences are cumulative, and they cannot be adequately assessed in a series of isolated transactions. Privacy self-management's very structure impedes its ability to achieve its goal of giving people meaningful control over their data. Moreover, its narrow focus on individuals neglects the larger social dimensions of privacy.

II. BEYOND PRIVACY SELF-MANAGEMENT

Where should privacy law go from here? Clinging more tightly to privacy self-management is not the answer. Nor is abandoning privacy self-management or embracing paternalistic regulation. In this Part, I propose some guidance for privacy law's future direction. Although I am far from ready to propose a complete solution, I can with reasonable confidence point out paths that will prove fruitful and paths that will not.

---

[60] *Id.* at 1951.

[61] Schwartz & Solove, *supra* note 45, at 1866–68.

A. Navigating the Consent Dilemma

Through privacy self-management, the law aims to give people control over their data. The core of this control involves people's choices about whether to consent to data collection, use, and disclosure. As I demonstrated above, people are not able to provide meaningful consent in many situations.

The most obvious alternative would be for the law to regulate and compel certain privacy choices. Privacy regulation, however, risks becoming too paternalistic. Regulation that sidesteps consent denies people the freedom to make choices. The end result is that either people have choices that are not meaningful or people are denied choices altogether. Ironically, paternalistic regulation might limit people's freedom to choose in the name of enhancing their autonomy. I term this problem the "consent dilemma." Privacy scholars must identify a conception of consent that both protects privacy and avoids paternalism.

1. Rethinking Consent and Paternalism. — Consent is an undertheorized concept that is crucial for privacy and many other areas of law. Consent performs an enormous amount of work. Activities that would otherwise be illegitimate are made legitimate by consent. For example, a person can agree to maintain confidentiality of data as a condition of employment. The person would ordinarily be free to speak about the data under the First Amendment right to free speech but has consented to waive this right.[62] Indeed, many constitutional rights can be waived with consent, including rights that implicate privacy, such as First Amendment rights to freedom of speech and association, the Fourth Amendment right to protection against unreasonable searches and seizures, the Fifth Amendment right to protection against compelled self-incrimination,[63] and the right to information privacy.[64] In addition to waiving their constitutional rights, people can consent to a wide array of other incursions on their privacy, such as monitoring of their communications and drug testing.[65]

As I demonstrated earlier, individuals cannot adequately self-manage their privacy, and consent is not meaningful in many contexts involving privacy. The primary regulatory alternative, endorsed by several scholars, is that the law should regulate privacy in a more pa-

---

[62] *See* Daniel J. Solove & Neil M. Richards, *Rethinking Free Speech and Civil Liability*, 109 COLUM. L. REV. 1650, 1676 (2009).

[63] *See* Jason Mazzone, *The Waiver Paradox*, 97 NW. U. L. REV. 801, 801–02 (2003). Some rights, however, cannot be relinquished with consent, such as the right to vote.

[64] Solove & Richards, *supra* note 62, at 1653.

[65] Jennings v. Minco Tech. Labs, Inc., 765 S.W.2d 497, 502 (Tex. App. 1989) (holding that giving employees a choice between taking a drug test or being fired was sufficient to make the drug tests consensual).

ternalistic manner. For example, Professor Anita Allen contends that privacy is a "'foundational' human good[]," one that is essential for a free and democratic society.[66] She argues that in certain instances, privacy must be mandated: "[F]or the sake of foundational human goods, liberal societies properly constrain both government coercion and individual choice . . . ."[67]

Cohen criticizes viewing privacy as something that can always be "traded off against other goods."[68] Under her view, individuals should not be able to waive privacy in a number of circumstances. Waiving privacy can lead to less creativity and impinge upon the development of selfhood. In her contribution to this Symposium, Cohen contends that privacy "is an indispensable structural feature of liberal democratic political systems."[69] The implication is that the law must override individual consent in certain instances.

The call for increased paternalism stems in part from the fact that people appear to be sharing data with increasing frequency and magnitude. Most people are not opting out as companies gather and use data. They are exposing the intimate minutiae of their lives on sites like Facebook and Twitter. This increased sharing of data is not the result of people's pure preferences. Their exposure is, in part, a result of the fact that many websites are designed to encourage exposure while minimizing awareness of the risks. This problem is made even more acute by the fact that many of the users of these sites are teenagers, whose ability to make decisions is not fully mature.

More broadly, because of the cognitive and structural problems with privacy self-management, people consent to the collection, use, and disclosure of their personal data when it is not in their self-interest to do so. This tendency lends support to those arguing for paternalistic regulation.

Despite the manifold problems with privacy self-management, there are two arguments that counsel against paternalism. First, the correct choices regarding privacy and data use are not always clear. For example, although extensive self-exposure can have disastrous consequences, many people use social media successfully and productively. Suppose a person suffering from bulimia wants to share her experiences and medical information with the world. She is willing to suffer the loss of privacy because she finds sharing her experiences to be cathartic and empowering. She also desires to help other people suffering from the disorder, and doing so gives her a rewarding sense of purpose. She writes passionately about herself, exposing details that

---

66 ANITA L. ALLEN, UNPOPULAR PRIVACY 13 (2011).

67 *Id.*

68 JULIE E. COHEN, CONFIGURING THE NETWORKED SELF 148 (2012).

69 Cohen, *supra* note 2, at 1905.

could later be seen by employers or others, potentially resulting in a loss of employment opportunities. Should the law forbid her from sharing her story? If the law were to put restrictions on her disclosure, then it would be limiting her freedom and autonomy — ironically in the name of preserving her freedom and autonomy. A further problem with the paternalistic approach is that the cost-benefit analysis, at least in this hypothetical, does not clearly counsel against disclosure. In fact, the benefits might far outweigh the costs. She might, for example, use her exposure to write a book launching a successful career as a writer and as a crusader against bulimia.

Similarly, some people want targeted marketing. They want their data shared. They want catalogs to be mailed to their homes. They want to be tracked. They want to be profiled. They want companies to use their personal information to recommend products and services. These people should not be dismissed as uninformed or foolish, as it is far from clear that the costs to these people outweigh the benefits.

Second, and more broadly, there are social benefits to data analysis. As Professor Omer Tene and Jules Polonetsky note, the collection, use, and disclosure of personal data — even without consent — can lead to great benefits for individuals and society.[70] For example, many Internet companies that offer free web content use the analysis or sale of personal data as the main source of revenue.[71] If many people refuse to consent to the use of the data, these business models will fail. Thus, structurally, one of the benefits of data collection, use, and disclosure is that it pays for online content. There are deep problems with this state of affairs, as people are often not fully aware that they are paying for online content with their personal data,[72] but legal restrictions on this business model would strike many as overly paternalistic.

In general, the law overrides people's ability to consent when the individual or social harms of what they might consent to clearly outweigh the benefits. The total social costs and benefits of an individual's waiver of privacy rights are often complicated to weigh. As Strahilevitz notes in this Symposium, various restrictions on the collection, use, and disclosure of personal data lead to benefits for some people and detriments to others.[73] Privacy has distributive effects, and

---

[70] Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. (forthcoming 2013) (manuscript at 6–12). Schwartz and I raise additional examples elsewhere. Schwartz & Solove, *supra* note 45, at 1866–68.

[71] Jan Whittington & Chris Jay Hoofnagle, *Unpacking Privacy's Price*, 90 N.C. L. REV. 1327, 1328–29 (2012).

[72] *See id.*

[73] Strahilevitz, *supra* note 3, at 2022.

this fact makes it more complicated to determine which choice is the right one to make.[74]

The law generally does not override consent, even with potentially dangerous activities. Individuals can consent to smoking cigarettes and drinking alcohol, even though those activities are dangerous. The same is true for playing football or engaging in careers such as coal mining or firefighting. Other consensual activities are prohibited, such as prostitution and certain drug use; these activities are seen as having little social value. While these activities may not be distinguishable from legal ones for more than historical and moral reasons, they are among the small number of consensual activities that are forbidden by law. The choice to surrender one's privacy does not seem burdened by the extreme moral or safety considerations inherent in the small group of forbidden consensual activities.

As a general matter, the law refrains from restricting transactions that appear on the surface to be consensual, and the law will tolerate a substantial amount of manipulation and even coercion before it deems a transaction to be nonconsensual. Contract law does not second-guess every agreement, even lopsided ones where one party did not fare very well. People make decisions all the time that are not in their best interests. People relinquish rights and take bad risks, and the law often does not stop them.

The EU has a more paternalistic approach to data processing, as Schwartz documents in this Symposium.[75] EU privacy law has a self-management component, but it requires a much more stringent and explicit form of consent than U.S. privacy law.[76] Moreover, EU law is more restrictive of data collection, use, and disclosure — it requires a legal basis before personal data can be processed, whereas in the U.S. data can generally be processed "unless a law specifically forbids the activity."[77]

Despite these differences, the EU's more explicit consent requirements do not necessarily lead to people engaging in more meaningful cost-benefit analyses regarding the collection and uses of their data. In the EU, consent is certainly more difficult and costly to obtain, sometimes so much so that it can impede beneficial information flow. Moreover, EU regulation can be formalistic, and it often provides restrictions without any connection to harm. The regulation can thus

---

[74] *See id.* at 2027.

[75] *See* Paul M. Schwartz, *The EU–U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1971–76, 1992–2001 (2013).

[76] Professor Fred Cate notes that although some EU officials downplay the extent to which the EU Data Protection Directive relies upon notice and consent, the Directive "plainly" does so, as "[m]any of its substantive protections can be waived without consent." Cate, *supra* note 14, at 360.

[77] Schwartz, *supra* note 75, at 1976.

hinder processing that does not cause harm and even might be beneficial. U.S. law, in contrast, generally allows the processing of data unless it causes a problem.[78] The difficulty with the EU approach is that data collection, use, and disclosure are rarely inherently good or bad. The costs and benefits depend upon the consequences. Paternalism is much easier to justify when the consequences are clearly bad.

2. The Failure of Opt-in Consent. — Some argue that the answer to the many problems of consent is to move to a more explicit and affirmative method of procuring consent: an opt-in rather than opt-out regime. As stated by FTC Commissioner Jon Leibowitz, companies should move to a model where consumers "'opt in' when it comes to collecting information — especially when it comes to sharing consumer information with third parties and sharing it across various web-based services."[79]

Despite my early optimism about opt-in, I now believe it will fail. One reason is that many organizations will have the sophistication and motivation to find ways to generate high opt-in rates. They can do so simply by conditioning products, services, or access on opting in. As Schwartz has aptly noted, "many data-processing institutions are likely to be good at obtaining consent on their terms regardless of whether the default requires consumers to authorize or preclude information-sharing."[80]

Moreover, "consumers are likely to be far more sensitive to price terms, such as the cost of a checking account, than to nonprice terms like the financial institution's privacy policies and practices."[81] Indeed, agreeing to clickwrap contracts and end-user license agreements is often a prerequisite for obtaining access to a website or to use a product or service. Consider the end-user license agreement to Apple's iTunes Store.[82] Periodically, this agreement pops up and people are required to agree. On an iPhone, the text of this agreement often extends to more than fifty screens. If people want to download apps from the store, they have no choice but to agree. This requirement is akin to an opt-in system — affirmative consent is being sought. But hardly any bargaining or choosing occurs in this process. Thus, despite regulators' best intentions, an opt-in system or a requirement of affirmative consent for most new uses of data will likely lead to more

---

[78] *Id.*

[79] Leibowitz, *supra* note 18, at 6.

[80] Paul M. Schwartz, *Privacy Inalienability and the Regulation of Spyware*, 20 BERKELEY TECH. L.J. 1269, 1274 (2005); *see also* Cate, *supra* note 14, at 366–67 ("[If] consent is required as a condition for opening an account or obtaining a service, a high response rate can always be obtained." *Id.* at 366.).

[81] Schwartz, *supra* note 80, at 1274.

[82] *See iTunes Store — Terms and Conditions*, APPLE, http://www.apple.com/legal/itunes/us/terms.html (last visited Mar. 30, 2013).

buttons to click and more forms to sign, but not to more meaningful privacy protection.

Requiring companies to obtain affirmative consent for many new uses of data might also be unnecessarily costly and impede socially beneficial uses.[83] Making consent cumbersome and costly to procure can have the de facto effect of restricting certain uses not because people will withhold consent, but because the costs of procuring consent might prevent entities from engaging in those uses. The result might be to restrict uses of data in a formalistic manner that fails to distinguish beneficial from harmful uses. Some might say that less data collection, use, and disclosure is always a victory, but should privacy win out when the benefits of data uses outweigh the privacy costs? Or when individuals would desire a use but are not asked because asking would be too costly?

Some might support opt-in because consumers would be forced to pay attention to notifications about how their data will be used and disclosed, which people are less likely to know with an opt-out system. Despite the knowledge benefit of opt-in, there is a cost. In opt-in regimes, people affirmatively indicate their consent to data collection and sharing. With this clearer and more legitimate consent, companies might feel more entitled to use and disclose data more widely. In contrast, with opt-out the consent procured is less legitimate than with opt-in regimes. This disparity does not make opt-out consent illegitimate, but it is certainly ambiguous, as opt-out consent might be the product of mere inertia or lack of awareness of the option to opt out.

In the long run, opting in may not even lead to fewer people sharing data. If companies must obtain opt-in consent, they might also be more aggressive about the amount of data that they ask for.[84] Data collectors may attempt to define potential future uses more broadly and vaguely in order to avoid having to obtain new consent in the future. In the end, opt-in is just another version of privacy self-management, and it suffers from the same underlying problems.

3. Should Privacy Self-Management Be Abandoned? — For all its flaws, privacy self-management should not be abandoned. Providing people with notice, access, and the ability to control their data is key to facilitating some autonomy in a world where decisions are increasingly being made about them with the use of personal data, automated processes, and clandestine rationales, and where people have minimal abilities to do anything about such decisions. A world without privacy self-management would clearly be troublesome, as people should have

---

[83] Cate, *supra* note 14, at 364–65.

[84] Nicklas Lundblad & Betsy Masiello, *Opt-in Dystopias*, 7 SCRIPTED 155, 162 (2010), http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.pdf.

rights to know about how their data is being used and to make decisions about those uses.

Moreover, efforts to improve privacy self-management through more consumer education, more salient notices, and more choices are certainly laudable and important. Such efforts have been a major legal and policy goal. In essence, this work is doubling down on self-management.

Ironically, perhaps the greatest practical impact of privacy self-management is not in informing individuals and improving their privacy management, but in informing the companies that are collecting and using the data and in improving the companies' management of privacy.[85] The process of creating privacy notices forces internal changes within a company, raising self-awareness about data collection and use. Chief Privacy Officers (CPOs) educate personnel to be mindful of privacy and influence software, product, and service design to be more privacy friendly. Privacy self-management thus has the salutary effect of creating beneficial structural privacy protections and accountability inside institutions.[86]

Privacy self-management should also not be abandoned because there are times when people want to manage their privacy, and denying people this ability can disempower them and constrain their freedom. For example, some people take great care with the privacy settings on their social media profile pages. Some want their profiles exposed to the world. Some want their profiles exposed only to their friends. People in each group might care a lot about their social media privacy settings on one particular site yet not bother to look at the privacy policies at other sites they use.

Thus, privacy self-management should not be abandoned, and paternalistic solutions are troubling. There is no silver bullet, and so we must continue to engage in an elaborate dance with the tension between self-management and paternalism.

B. Future Directions

Although we should not reject privacy self-management, it is currently asked to bear far more weight than it can support. So what can be done?

---

[85] *See* Peter P. Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 MINN. L. REV. 1263, 1316 (2002) ("[A] principal effect of the notices has been to require financial institutions to inspect their own practices. . . . In order to draft the notice, many financial institutions undertook an extensive process, often for the first time, to learn just how data is and is not shared between different parts of the organization and with third parties.").

[86] *See generally* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011).

1. Rethinking Consent and Employing Nudges. — In order for privacy regulation to make headway, the law needs a better and more coherent approach to consent with respect to privacy. Indeed, in many areas of law, consent plays a critical role, yet what constitutes valid consent varies greatly across different areas of law. Thus far, few have attempted to analyze systematically what consent entails and to develop a more coherent approach toward consent.

Currently, the law has not sufficiently grappled with the social science literature that has been teaching us about the complexities and challenges involved in human decisionmaking. What does consenting to something really mean? What should the law recognize as valid consent? Many transactions occur with some kind of inequality in knowledge and power. When are these asymmetries so substantial as to be coercive? The law's current view of consent is incoherent, and the law treats consent as a simple binary (that is, it either exists or it does not). Consent is far more nuanced, and privacy law needs a new approach that accounts for the nuances without getting too complex to be workable.

There are also promising ways to mix consent with paternalism. For example, Thaler and Sunstein propose forms of "libertarian paternalism," which they refer to as "nudges," that seek to architect choices so as to change "people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives."[87] Nudges are paternalistic, but not as restrictive and absolute as more traditional paternalistic regulation. In some cases, nudges might be a workable middle ground between privacy self-management and paternalism.

2. Developing Partial Privacy Self-Management. — In essence, what many people want when it comes to privacy is for their data to be collected, used, and disclosed in ways that benefit them or that benefit society without harming them individually. If people have an objection to certain uses of data, they want a right to say no. But many people do not want to micromanage their privacy. They want to know that someone is looking out for their privacy and that they will be protected from harmful uses.

With the food we eat and the cars we drive, we have much choice in the products we buy, and we trust that these products will fall within certain reasonable parameters of safety. We do not have to become experts on cars or milk, and people do not necessarily want to become experts on privacy either. Sometimes people want to manage their privacy in a particular situation, and they should be able to do so. But globally across all entities that gather data, people will likely find self-

---

[87] THALER & SUNSTEIN, *supra* note 30, at 5–6.

management to be a nearly impossible task. People want some privacy self-management, just not too much. Privacy law needs to find a way to deliver partial privacy self-management.

One possible answer might be to find ways for people to manage their privacy globally for all entities rather than one at a time. But unifying such management can be challenging because it will be difficult to find a uniform set of privacy options that makes sense for all entities, and the consequences of data collection, use, or disclosure might differ depending upon which entities are involved.

3. Adjusting Privacy's Timing and Focus. — Privacy law's timing needs to be adjusted. Privacy self-management and the law focus heavily on the time of the initial collection of data — and often on each individual transaction where data is exchanged. But it is very difficult at the time of data collection for a person to make a sensible judgment about the future privacy implications because the implications are often unknown.

Therefore, the focus should be more on downstream uses rather than on the time of the initial collection of data. In many cases, benefits might not be apparent at the time the data is collected. New ideas for combining data, new discoveries in data aggregation and analysis, and new techniques and technologies of data analysis might change the benefits side of the equation. They might change the costs side as well. Rules that require renewed consent for new uses of data might be too prohibitively costly and serve as a de facto bar on these uses. Such an outcome might not be socially desirable, and it might not be the outcome preferred by most people whose data is involved. On the other hand, blanket consent that allows for a virtually unlimited array of new uses of data can be just as undesirable, as data can potentially be used in harmful ways that people might not be able to anticipate or understand.

Moreover, measuring the costs of certain forms of collection, use, and disclosure of personal data is extremely difficult because privacy harms are so elusive to define. Ultimately, because of the dynamism of this area, assessing costs and benefits requires a fair degree of speculation about the future. Individuals are likely not able to make such decisions very well in advance, but neither is the law.

Such decisions would be better made at the time of particular uses of data. What is needed is for the law to weigh in and provide guidance about the types of new uses at the time they are proposed. Perhaps some ought to be restricted outright, some ought to be limited, some ought to require new consent, some ought to be permitted but with a right to revoke consent, and some ought to be permitted without new consent. Perhaps an agency should review proposals for new uses as they arise.

4. Moving Toward Substance over Neutrality. — Any way forward will require the law to make difficult substantive decisions. Privacy

self-management attempts to remain neutral about the merits of particular forms of data collection, use, or disclosure and looks merely to whether or not there is consent. Under privacy self-management, most forms of data collection, use, or disclosure are acceptable if consensual. Consent often becomes a convenient way to reach outcomes without confronting the central values at stake. To move forward, this kind of neutrality cannot be sustained.

The law should develop and codify basic privacy norms. Such codification need not be overly paternalistic — it can be in a form like the Uniform Commercial Code (UCC), where certain default rules can be waived. The norms of the UCC have become well entrenched and oft followed. Deviations from these norms are quite salient. Privacy law has said far too little about the appropriate forms of collection, use, and disclosure of data. I am not suggesting a paternalistic regime where the law rigidly prohibits a wide array of data collection, use, or disclosure; only on the outer boundaries should the law do so. But the law must take a stronger stance about substance.

More substantive rules about data collection, use, and disclosure could consist of hard boundaries that block particularly troublesome practices as well as softer default rules that can be bargained around. Default rules can be crafted in a manner that modulates the ease with which parties can bargain around them. More substantive rules that establish a basic set of norms about privacy will make it easier for people to understand how their privacy is being protected. Deviations from these norms will be more conspicuous. The cacophony of different approaches to privacy will be lessened.

CONCLUSION

For far too long, privacy law has been relying too heavily upon privacy self-management. Privacy self-management cannot achieve the goals demanded of it, and it has been pushed beyond its limits. But privacy self-management should not be abandoned, and alternatives risk becoming too paternalistic.

At the core of many privacy issues is the consent dilemma, and too often, law, policy, and scholarship ignore it. The way forward involves (1) developing a coherent approach to consent, one that accounts for the social science discoveries about how people make decisions about personal data; (2) recognizing that people can engage in privacy self-management only selectively; (3) adjusting privacy law's timing to focus on downstream uses; and (4) developing more substantive privacy rules. These are enormous challenges, but they must be tackled. Otherwise, privacy law will remain stunted while the problems it must deal with grow larger and more out of control.