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 *1881 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. **

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 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). [FN4] 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. [FN5] 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. [FN6]

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. * * *

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, [FN9] an approach termed “notice and choice.” Entities have normalized the practice of providing notice and choice by offering privacy*1884 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. [FN10] When it finds such
a violation, the FTC can bring civil actions and seek injunctive remedies. [FN11] The notice and choice approach has also been a centerpiece of privacy legislation. The Gramm-Leach-Bliley Act (GLBA), [FN12] for example, requires financial institutions to provide customers with privacy notices and to allow customers to opt out of data sharing with third parties. [FN13]

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. [FN14] 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. [FN15] Moreover, few people opt out of the collection, use, or disclosure of their data when presented with the choice to do so. [FN16] Most people do not even bother to change the default privacy settings on websites. [FN17] As FTC *1885 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.” [FN18]

Why are so few people engaging in privacy self-management? One possible explanation is that privacy notices are long and difficult to comprehend. [FN19] There have been many proposals to shorten and simplify privacy policies, though these types of measures have not been shown to significantly improve comprehension. [FN20] * * *

There is a more difficult problem with proposals for improved notice * * *. 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. * * *

*1886 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. [FN24] 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.” [FN25] * * *

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. [FN26] Some conclude from this fact that consumers do not value privacy highly. [FN27] Some have suggested that there might be a generational shift in privacy norms, where young people do not care about privacy. [FN28] 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. [FN29]

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.

*1887 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.” [FN30] 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. [FN31]

People have “bounded rationality”--they struggle to apply their knowledge to complex situations--with regard to privacy. [FN32] 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.” [FN33] Risk assessment is also skewed by the “availability heuristic,” where people assess familiar dangers as riskier than unfamiliar ones. [FN34]

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. [FN35] 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.” [FN36] * * *

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.

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, etc.). 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.

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.
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 these clues. In other words, little bits of innocuous data can say a lot in combination. I have referred to this as the “aggregation effect.”

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.

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

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. 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.

*1892 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. [FN49] [Quotes from Regan, Schwartz, Cohen, Richards, etc.]

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. [FN61] 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

* * *

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?

*1901 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.” [FN87] 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-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 scholar-
ship 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.

[FN1]. 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.


[FN9]. See Julie Brill, Comm'r, Fed. Trade Comm'n, Remarks at Conference of Western Attorneys Gen-
eral Annual Meeting, Privacy 3.0 Panel (July 20, 2010).


[FN20]. 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.”).

[FN21]. See id. at 1034-35.

[FN22]. Id. at 1069-70.

[FN23]. See Strahilevitz, supra note 3, at 2038.


[FN28]. See Emily Nussbaum, My So-Called Blog, N.Y. Times, Jan. 11, 2004 § 6 (Magazine), at 32, 34.


[FN33]. Acquisti & Grossklags, supra note 17, at 369.

[FN34]. Thaler & Sunstein, supra note 30, at 25.


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.


See supra p. 1890.


See Acquisti & Grossklags, supra note 17, at 372.

E.g., Janger & Schwartz, supra note 16, at 1247.


Id. at 1613-14.

[FN57]. See Cohen, supra note 2, at 1918.


[FN59]. Richards, supra note 1, at 1946.

[FN60]. Id. at 1951.

[FN61]. Schwartz & Solove, supra note 45, at 1866-68.


[FN63]. 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.

[FN64]. Solove & Richards, supra note 62, at 1653.

[FN65]. 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).


[FN67]. Id.


[FN69]. Cohen, supra note 2, at 1905.


[FN72]. See id.

[FN73]. Strahilevitz, supra note 3, at 2022.

[FN74]. See id. at 2027.


[FN76]. 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.

[FN77]. Schwartz, supra note 75, at 1976.

[FN78]. Id.

[FN79]. Leibowitz, supra note 18, at 6.

[FN80]. 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.).

[FN81]. Schwartz, supra note 80, at 1274.


[FN83]. Cate, supra note 14, at 364-65.

[FN85]. 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.”).


[FN87]. Thaler & Sunstein, supra note 30, at 5-6.

126 Harv. L. Rev. 1879

END OF DOCUMENT